ISSN: 2704-8012

SUOR ORSOLA
BENINCASA
UNIVERSITÀ EDITRICE

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

www.ejplt.tatodpr.eu



2022/2

EJPLT
ISSN: 2704-8012

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

Directed by Lucilla Gatt

2022/2

SUOR ORSOLA BENINCASA
UNIVERSITÀ EDITRICE

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



With the support of the
Erasmus+ Programme
of 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.

Editing
Luciana Trama

Design
Flavia Soprani

Development
Emanuele Garzia

© Copyright 2022 by Suor Orsola Benincasa Università Editrice, published in December 2022
ISSN: 2704-8012
The Issue is 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*
The intellectual property of the individual contributions remain with the authors.

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. Valeria Falce – Università Europea di Roma, Italy
Prof. Pim Haselager – Radboud University, Netherlands
Prof. Toni M. Jaeger-Fine – Fordham University, United States
Prof. Indranath Gupta – O.P. Jindal Global University, India
Prof. Antonios Karaiskos – Kyoto University, Japan
Prof. Roberto Montanari – Università degli Studi Suor Orsola Benincasa di Napoli, 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
Prof. Alex Nunn – University of Derby, 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. Anna 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. Paola Manes – Alma Mater Studiorum Uiversità di Bologna, Italy
Prof. Giovanni Martini – Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Michala Meiselles – University of Derby, United Kingdom
Prof. Alessia Mignozzi – Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Salvatore Monticelli – Università di Foggia, Italy
Prof. Cinzia Motti – Università di Foggia, Italy
Prof. Nora Ni Loideain – Institute of Advanced Legal Studies of London, United Kingdom

EJPLT
ISSN: 2704-8012

European Journal of Privacy Law & Technologies

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

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, Russia
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. Hans Steege – Gottfried Wilhelm Leibniz Universität Hannover, 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 degli Studi 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 degli Studi Suor Orsola Benincasa di Napoli, Italy
Ph.D. (c) Avv. Chiara Vitagliano – Università degli Studi di Napoli l'Orientale, Italy

pp.

Editorial

Lucilla GATT AND ILARIA AMELIA CAGGIANO – *Consumers and digital environments as a structural vulnerability relationship.* *8*

Section I: **Articles**

GIOVANNA D'ALFONSO – *Danni algoritmici e sviluppi normativi europei tra "liability" e "permittance rules".* | *Algorithmic damages and European regulatory developments between liability and permittance rules.* *18*

ALESSIA MIGNOZZI – *Digital divide ed enti del terzo settore nella società del terzo millennio.* | *Digital divide and third sector entities in the third millennium society.* *67*

FRANCESCA DI LELLA – *Identità e destino degli embrioni soprannumerari. Ipotesi* de iure condendo. | *Identity and fate of supernumerary embryos.* De iure condendo hypothesis. *84*

ANNA ANITA MOLLO, DOMENICO NAPOLITANO AND LUIGI MARIA SICCA – *Il formalismo testamentario e le tecnologie assistive per le persone con disabilità: profili giuridici e organizzativi.* | *Testamentary formalism and assistive technologies for people with disabilities: legal and organizational profiles.* *99*

ANDREA DEL FORNO – *L'intelligenza artificiale nei processi gestori dell'impresa.* | *Artificial intelligence in business processes management.* *119*

FABIO ZAMBARDINO – *La* blockchain *e la protezione dei dati personali: una tecnologia* privacy compliant by design*?* | *Blockchain and the protection of personal data: a privacy compliant by design technology?* *136*

CHIARA IORIO – *Legal issues concerning the circulation and processing of data in the digital age.* *153*

SIMONE FABIO DICORATO AND MATTEO DE PAMPHILIS – *'Stretching the rules': how racing design may drive the evolution of the technological and legal environment.* *169*

Luigi Izzo – Il difficile rapporto tra diritto alla privacy e dovere di contribuzione alla spesa pubblica. | The difficult relationship between the right to privacy and the duty to contribute to public expenditure. 187

Ranieri Razzante – L'attribuzione degli attacchi informatici. | The attribution of cyberattacks. 215

Elena Quarta – Applicazione I.A. della pena pecuniaria nel sistema penale peruviano: una proposta di ricerca per dare un futuro al "presente novecentesco" del sistema carcerario italiano. | I.A. application to pecuniary penalties in the Peruvian penal system: a research proposal to give a future to the "twentieth-century present" of the Italian prison system. *242*

Section II: **Review**

MASSIMO DE FELICE – *Su* Privacy and Consent. *Cinque osservazioni.* | *On Privacy and Consent. Five observations.* (Recensione a GATT L., MONTANARI R., CAGGIANO I.A. (eds.), P*rivacy and Consent. A Legal and UX&HMI Approach*, University Suor Orsola Benincasa Press, Naples, 2021). 265

Section III: **Focus papers**

ROBERTA MARINO AND SEYED MILAD MAHMOOD KASHANI – *The mechanism of smart contract conclusion in the Italian and Iranian legal systems.* 273

ANTONELLA DI CERBO – *L'inquadramento giuridico dei dati personali ceduti per la fruizione dei servizi digitali. | The legal framework of personal data transferred for the use of digital services.* 293

FRANCESCO RIBEZZO – *Le nuove vie della giuridificazione del corpo.* | *The new ways of body juridification.* 305

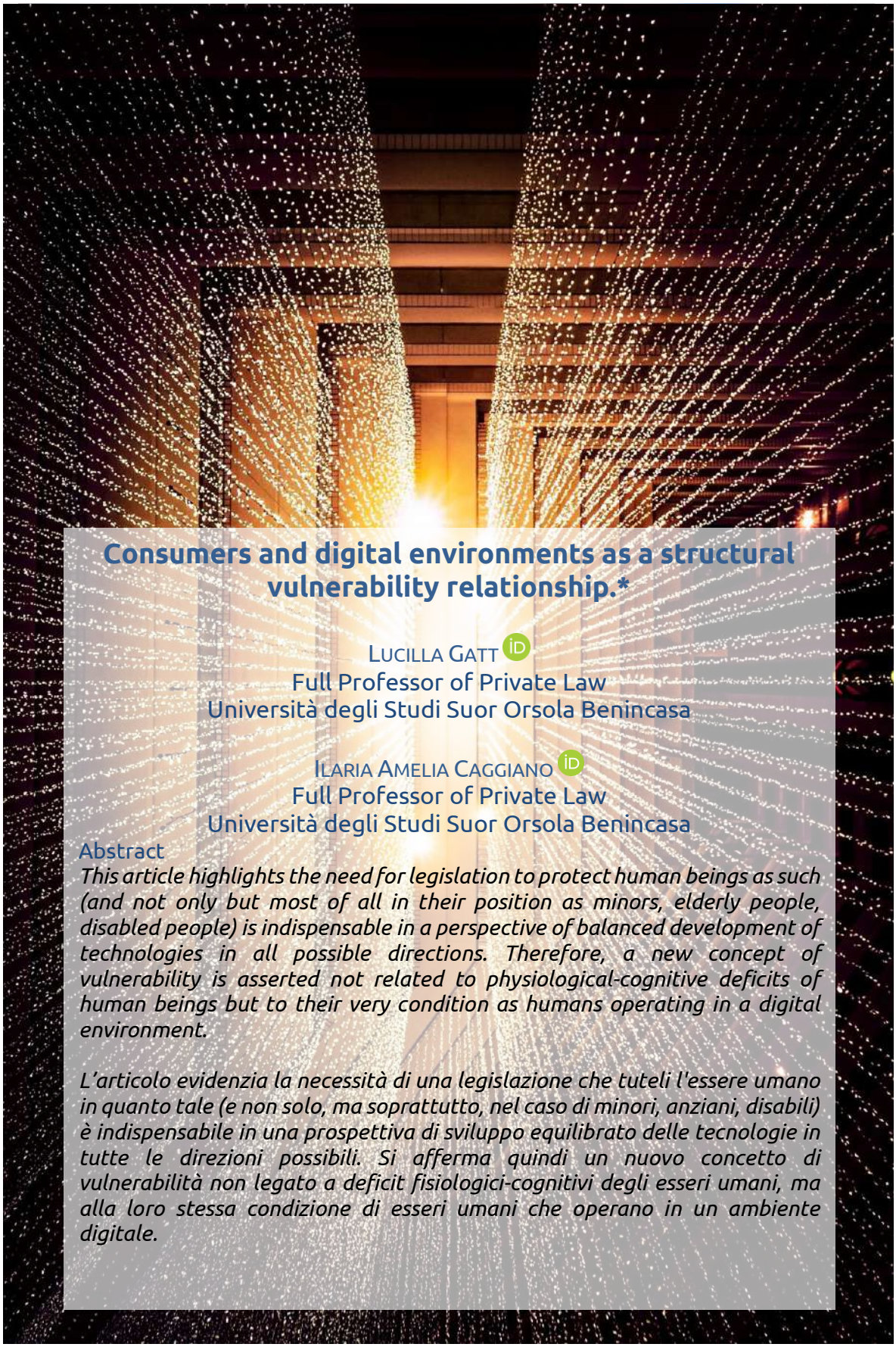
SERGIO GUIDA – *Golem* vs. Transhuman*: l'uomo del futuro tra biologia, nuove tecnologie, etica e sostenibilità.* | *Golem vs. Transhuman: the man of the future between biology, new technology, ethic and sustainability.* 313

SABIRE SANEM YILMAZ AND HABIBE DENIZ SEVAL – *Mind over matter: Examining the implications of machine brain interfaces on privacy and data protection under the GDPR.* 347

List of authors 362

Gatt L, Caggiano I, 'Consumers and Digital Environments as a Structural Vulnerability Relationship ' (2022) 2 EJPLT, 8-16.
DOI: https://doi.org/10.57230/EJPLT222LGIAC

EJPLT
ISSN 2704-8012



Consumers and digital environments as a structural vulnerability relationship.*

Lucilla Gatt
Full Professor of Private Law
Università degli Studi Suor Orsola Benincasa

Ilaria Amelia Caggiano
Full Professor of Private Law
Università degli Studi Suor Orsola Benincasa

Abstract

This article highlights the need for legislation to protect human beings as such (and not only but most of all in their position as minors, elderly people, disabled people) is indispensable in a perspective of balanced development of technologies in all possible directions. Therefore, a new concept of vulnerability is asserted not related to physiological-cognitive deficits of human beings but to their very condition as humans operating in a digital environment.

L'articolo evidenzia la necessità di una legislazione che tuteli l'essere umano in quanto tale (e non solo, ma soprattutto, nel caso di minori, anziani, disabili) è indispensabile in una prospettiva di sviluppo equilibrato delle tecnologie in tutte le direzioni possibili. Si afferma quindi un nuovo concetto di vulnerabilità non legato a deficit fisiologici-cognitivi degli esseri umani, ma alla loro stessa condizione di esseri umani che operano in un ambiente digitale.

* The author of paragraphs 1 to 5 is Lucilla Gatt, Full Professor of Private Law and Director of the Research Centre of European Private Law; the author of paragraphs 6 and 7 is Ilaria Amelia Caggiano, Full Professor of Private Law and Vice-Director of the Research Centre of European Private Law.

© The author(s) 2022, published by Suor Orsola University Press. 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: human being; new technologies; new vulnerabilities; minors; ethical space; education.

Summary: 1. The concept of relational vulnerability with special regard to the technological environment – 2. The role of law in the vulnerability context – 3. The phases of relational vulnerability discovery – 4. The technological vulnerability – 5. The ethical space as an intermediation tool in the relationship of vulnerability – 6. A special category of vulnerable individuals: Minors, and the case of data protection – 7. Some considerations on the current regulation of minors' vulnerability in the digital environment

1. The concept of relational vulnerability with special regard to the technological environment.

In the legal field, vulnerability is a relational concept.

It is a multidimensional and correlated condition, no longer a status linked to old age, minor age, female gender or disability conditions. In the current legal framework at national and international level, vulnerability can be considered to have acquired a broader meaning.

It includes all living entities – from humans to animals or plants (although this aspect is not considered in this document) – when they operate in contexts where other actors are more powerful for various reasons: social, economic or cultural, physical strength, possession of weapons and, last but not least, technological gap.

This means an imbalance in starting positions, which determine someone's vulnerability to someone else. This condition, in turn, means that someone is capable of profiting someone else or, more dramatically, causing them pain or death.

Having identified the condition of vulnerability in these terms, it seems plausible to state that:

1) the abuse of a person in a position of greater power/strength to the detriment of another person is unjust.

2) the subject who is in a weak position – i.e., the vulnerable subject – must be protected from any abuse of power/strength by the other subject.

2. The role of law in the vulnerability context.

Assuming a historical perspective with Europe and neighboring countries at the center, it can be seen how these conclusions, although currently (apparently) shared when it comes to national and international Western charters on fundamental rights, have not always been applied in economic practice and legal. In other words, for a relatively short time the idea has penetrated Western culture that being holders of greater physical, intellectual, cultural, and economic strength does not authorize behaviors of oppression of various kinds on who or what cannot react with of equal importance and

intensity.

The word 'vulnerability' (from the Latin 'vulnerare', to wound) literally means 'likely to be injured'. Figuratively, it refers to the precariousness of a condition marked by the possibility of violation and limitation, often defined by different degrees of weakness, dependence, lack of protection. Cicero spoke of three realities susceptible to being injured: life, reputation and health. Similarly, contemporary philosophy emphasizes different meanings of vulnerability: physical, psychological, spiritual, political and legal. The «Declaration of Barcelona» of 1998 represents an important event in the promotion of the category of vulnerability, in view of its possible public legitimization, so to speak, in the field of bioethics. The Declaration was signed by a group of twenty-two European scholars and represents the result of three years of study promoted by the European Commission. [1] It is structured around four new principles, of which the principle of vulnerability is the innovative principle. In fact, the Barcelona principles represent, taken together, a critique and a rather conspicuous alternative to the four principles of North American bioethics: autonomy, non-maleficence, beneficence and justice (W. T. Reich, 2001).[2]

Conversely, the position of greater strength translates into greater responsibility to who or what is in a different position. This trend can be seen in European and not only European policies of the green deal and human-centered artificial intelligence.

This attests to an evolution in the European culture of the concept of vulnerability in the sense of a transition of the vulnerable entity (that is to say: weaker) from an object of oppression to a subject to be protected. That said, the tools that can be used to counter the abuse and to protect the vulnerable subject from abuse are of a preventive or repressive nature. In both cases, the law comes into play, i.e., a mandatory regulatory apparatus with adequate prescriptions and corrective tools. These norms make illegal the abuse to the detriment of the vulnerable, which otherwise would only possibly be ethically unacceptable (unjust, in fact).

Because of this possible prospect, it was decided to develop a research and teaching project on the vulnerability of human beings in relation to digital technology[3]. This is one of the areas in which the relationship of vulnerability has developed, understood as a relationship of fragility of one subject with

[1] The «Declaration of Barcelona» of 1998 has been developed within the Bio-Med II research project (1995-1998), founded by the EU Commission. The results of the Bio-Med II EU research project have been published: P Kemp, J Rendtorff, NM Johansen, Bioethics and biolaw. Vol. I-II. (Rhodos international Publishers 2000).

[2] W T Reich, 'Prendersi cura dei vulnerabili: il punto di incontro tra etica secolare ed etica religiosa nel mondo pluralistico' (2002) 3, Annali di Studi Religiosi, 71-86.

About the basic principles for European bioethics: P Kemp JD Rendtorff, 'The Barcelona Declaration – Towards an Integrated Approach to Basic ethical principles' (2008) 2, Synthesis Philosophica, 239 – 251; JD Rendtorff, 'Basic ethical principles in European bioethics and biolaw: autonomy, dignity, integrity and vulnerability - Towards a foundation of bioethics and biolaw' (2002) 5, Med Health Care Philos; P Kemp, 'Four ethical principles in biolaw' (2000) 2 Bioethics and Biolaw, 13-22.

About the principles of North American bioethics: TL Beauchamp, JF Childress, Principles of biomedical ethics (Oxford University Press 1979).

[3] The research and teaching project has been developed within the activities of the Jean Monnet Chair 'European Protection Law of Individuals in Relation to New Technologies – PROTECH', held at the University Suor Orsola Benincasa of Naples, faculty of law.

Project website is available at https://www.protech-jeanmonnet.eu

respect to another: (e.g., consumer natural person, on the one hand, platforms – e-commerce or social-network – from the other one). Compared to this relationship, minor age or advanced age or computer illiteracy or single disability are not the cause of vulnerability but can represent an aggravating factor.

3. The phases of relational vulnerability discovery.

The analysis started from the focus on vulnerability as a concept that can be elaborated, following the following phases:

a) to map and analyze with a multidisciplinary method the most evident cases of vulnerability aka 'difference of positions' in the various sectors such as, for example, human rights violations in dictatorial governments; the forced occupation of territories; unfair terms in consumer contract law; the abuse of power in private and public relations; the determination of the will of others through the undeclared and unauthorized use of technological tools; the abusive treatment of personal data and the like.

b) extrapolate the recurring weaknesses from these scenarios.

Considering each element of weakness as a value to be protected, we can highlight the values to be included in the mandatory regulatory frameworks to ensure that protection against vulnerabilities is guaranteed at the macro level.

In summary, vulnerability is an indicator of greater weakness on one side of the relationship. This weakness must be considered a value, i.e. an asset to be protected through the adoption of adequate regulations.

4. The technological vulnerability.

This scenario and the consequent need for protective legislation occurs above all in the relationship between human beings and the digital environment in all its possible articulations.

In the technological habitat (for example: e-commerce platforms) a subject can act in an unfamiliar context that can be known or simply more comfortable or familiar to others for various reasons (digital divide, minor/old age, asymmetry of bargaining or information power). But in this large category of vulnerable subjects we also include human embryos, which are a crucial example of exposure to the risk of harm (alias vulnerability) because they do not act but are created aborigine in a technological and highly manipulated environment without their consent.

Ultimately, in digital habitats the subjects that can be qualified as more vulnerable are:

– Those concerned with particular regard to Minors and the Elderly;

– Consumers with particular regard to Minors and the Elderly;

– Embryos, unborn children, new life forms created in the laboratory.

It is necessary to highlight or, better, to promote a protective approach in existing national and international legislation (data protection, consumer protection, embryo protection), which regulates the relationship between

individuals and technologies.

Finally, also to increase students' awareness of vulnerability as a value to be protected, we also consider their condition as vulnerable subjects, in relation to teaching staff. This assumption can be the basis of a new integrated educational model (online and offline) with a high level of accessibility and usability in a global scenario.

The crucial point lies in the determination of a concept of vulnerability that is not linked to specific physical or psychological disabilities but is identified in the relationship between the physical person and the technological environment in which he/she operates (Gatt L., 2022)[4].

5. The ethical space as an intermediation tool in the relationship of vulnerability.

Having taken note of the ontological vulnerability of human beings – in general – with respect to digital technology structures, it should be emphasized that the law alone is not sufficient to reconcile the interests at stake and to achieve objectives of effective protection.

The rules must express a direction, choosing to protect weakness as a value but they must also prepare concrete tools by foreseeing them. Among these, a very valid tool is that of the Ethical Space which translates into an entity of various kinds, adaptable to the context in which it is called to operate.

With regard to the 'educational fact', i.e., the teacher-student training relationship, it is important that it takes place in suitable places and with suitable means to guarantee the weak subject of the relationship total and equal access to the educational path.

The physical space where training takes place must be built and designed to compensate for this disparity of positions (for example: digital training requires adequate tools and equal accessibility to them as well as human resources dedicated to training and the required support).

This principle of the organization and structuring of physical and digital space according to the maximum usability, accessibility and effective utility for the weak subject is also valid in the relationship between student and teacher as well as consumer and entrepreneur and, above all, between citizen and State.

Think of the issue of the digital identity needed to access many if not all public services. Also, this relationship between natural person and public subject requires the adoption and construction of ethical spaces (e.g., intermediation stations with dedicated human resources; chats with human operators; clear and transparent information; loyal behavior on the part of the public administration).

The conscious use of places, of real and virtual spaces together with the involvement of human resources prepared to guarantee represents the real

[4] L Gatt, 'Legal anthropocentrism between nature and technology: the new vulnerability of human beings' (2022) 1 EJPLT, 15-26. DOI: https://doi.org/10.57230/EJPLT221LG

challenge for a real transition to digital for all those who find themselves in a position of vulnerability.

6. A special category of vulnerable individuals: Minors, and the case of data protection.

When looking at the existing law, one might consider if it protects technological vulnerability. To analyze this aspect, we will consider European data protection regulation (GDPR, EU Reg. 2016/679), which is a case where vulnerability towards technology, although not being qualified in such a manner, is taken into consideration for regulating personal data of children.

Minors are legally vulnerable individuals, as already foreseen in other areas of law (ex. Family, Contract, Immigration Law).

In the digital world, they become, indeed, doubly vulnerable: they are not fully aware of themselves and the perceivable world and for this reason they are already legally protected in various context (subjective vulnerability); in addition, they are more exposed to unknown or not perceivable risks arising from the digital environment (technological vulnerability).

Probably for this reason, minors are the only category of vulnerable subjects expressly foreseen by the GDPR, in various provisions, either only as subjective vulnerable persons or as also technologically vulnerable ones.

Whereas (38) of the GDPR identifies reasons why children are considered vulnerable persons and therefore merit specific protection, as well as the principal areas where processing of personal data needs to be under attention: *« […] they may be less aware of the risks, consequences and safeguards concerned and their rights […]. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. [..]».* The reference made in whereas 38 to creation of personality or using profiles implicitly refers to the digital world. More specifically, the EDPB Guidelines on the targeting of social media users[5] focuses on the potential adverse impact of targeting, which « […] *can influence the shaping of children's personal preferences and interests, ultimately affecting their autonomy and their right to development*».

The Guidelines refer to risks which are known in social studies as the *filter Bubble* phenomenon, where during the web navigation algorithms select information that a profiled user would like to see, based on past information about him/her, and past click-behavior and search history. As a result, users are not used to information that disagrees with their viewpoints, effectively isolating them in cultural or ideological bubbles. For minors, this means that they do not have the chance to develop critical viewpoints based on diverse, even conflicting, information.

For protecting vulnerability, the GDPR adopts a regulatory technique based on the general principles and the general obligations already in charge of the

[5] Guideline 8/2020 on the targeting of social media users, adopted on 13 April 2021. Available online at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en

data controllers, which they must implement, through decisions and processes in their business or institutional activity (*e.g.*, Data protection by design and by default). Except spare cases, one would not find specific rules addressing vulnerability, whilist not-binding recommendations are variously provided for.

The GDPR reinforces what is already foreseen on a general basis as for rights and interests of minors: in terms of recommendation regarding the Right to erasure ('right to be forgotten') (art. 17), Whereas 65 recommends guaranteeing in any case the right to erasure if the consent has been given when the subject was minor.

The balancing test that the data controller must undertake between legitimate interest and rights and freedom of the data subject must be particularly cautious when he/she is a minor (art. 6, §1, *f)* GDPR).

More specifically, protection of minors as technologically vulnerable subjects is devised through the general obligations of the data controller, and recommendations to him/her.

Consideration of minors as technologically vulnerable subjects can specify the Data-protection-by-design-principle, which is referred to data processing in general (Art. 25). Whereas 71, states: *Profiling ... should not concern a child*. According to *soft law* (WP 29, Guidelines on Automated individual decision-making and Profiling) [6] this prohibition must be considered only as a recommendation, as well as the one regarding apps on smart devices (WP 29, Opinion 02/2013) [7] : App developers must '[…] refrain from processing children's data for behavioral advertising purposes, either directly or indirectly […]'.

If the data processing concerns vulnerable data subjects and/ or the digital environments, the data controller may be obliged to conduct a Data Processing Impact Assessment before starting or to continue the processing. Soft law (WP29 Guidelines) identifies some specific criteria in this regard, including evaluation or scoring, profiling; Automated-decision making with legal or similar significant effect; Data processed on a large scale; Data concerning vulnerable data subjects (minors, mentally ill persons, asylum seekers, or the elderly, patients, etc.).[8]

The DPIA is required if at least two of these criteria are met, but – taking into account the circumstances – the data controller can decide to conduct a DPIA even if only one of the above criteria is met.

Binding provisions regulate minors' decision, both as for the information to be provided (art. 12), and for the consent itself (art. 8). In this last case, GDPR takes into consideration technological vulnerability of minors in the information society services, as a context within which the minor operates

[6] WP 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP251rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018. Available online at https://ec.europa.eu/newsroom/article29/items/612053

[7] WP29, Opinion 02/2013 on apps on smart devices, 00461/13/EN WP 202, adopted on 27 February 2013. Available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[8] WP 29 Guidelines on Data Protection Impact Assessment (DPIA) 17/EN, WP 248 rev.01, Adopted on 4 April 2017. Available online at https://ec.europa.eu/newsroom/article29/items/611236/en

more widely and freely and fixes an age threshold (16 years) to give consent to the data processing as a legal basis.

Following the waiver allowed by GDPR, a number of Member States, among which there is Italy, has lowered this threshold age, thus altering in principle the harmonization of markets.

7. Some considerations on the current regulation of minors' vulnerability in the digital environment.

The regulatory framework depicted on the regulation minors' data takes into account their technological vulnerability by charging the data controller with evaluations to carry out and decision to take, or by fixing more specific rules.

At this point, some considerations on the state of the art may be done.

As for the privacy consent of minors in the digital environment, in our view, diversification of the age threshold among Member States is a collateral issue in terms of relevance if one regards the role of the rule of consent in the operating practice.

One must recognize that the impact of the rule on minors' consent in the digital environment is sensibly weak for a number of reasons:

(1) The scope of the rule is the consent as a legal basis for data processing, which means that it is relevant for those processing of data not included in the performance of the contracts and in the legitimate interest (e.g., only behavioural advertising, and, profiling, according to the evaluations of the controller);

(2) Therefore, access to platforms is regulated by contract rules. The social networks more desirable by minors fix low threshold ages for contracting, adopting same rules in different countries (12 years), probably relying on the overall validity of the contract, since subscription to social networks has to be considered as a means for expressing freedom and personality;

(3) On the privacy by design perspective, social networks (*e.g.,* Tik-tok, privacy policy) provide for different age groups (13-15; 16-17) for the share and third parties access functions.

As for the consent profile, wherever it is contractual consent or privacy consent (regulated by art. 8 GDPR), the crucial point for protecting children acting in the digital world is to verify their age. Given the absence of expressed rules, as well as the flawless of verification mechanisms currently activated (*e.g.*, one-choice option) and traditionally considered (*e.g.*, id card, parents' payment card), nowadays it is more than easy for a child to create a fake profile, declaring an older age. This expedient can make the law virtually ineffective, if not supported by different technologies enabling verification (id recognition, blockchain and / or smart contracts), which, however, bring other data protection issues, or written-alike mechanisms of contract conclusion (*e.g.*, qualified electronic signature), which has been historically an instrument of protection of vulnerable parties.

On the side of the obligations and the compliance processes in charge of controllers, here *ex post* remedies, Supervisor's activities and deterrence of

sanctions are the institutional tools, even if not capillary, to control data processing of minors and protect their vulnerability.

SECTION I
ARTICLES

D'Alfonso G, 'Danni algoritmici e sviluppi normativi europei tra "liability" e "permittance" rules' (2022) 2 EJPLT, 18-66.
DOI: https://doi.org/10.57230/ejplt222GDA

EJPLT
ISSN 2704-8012



Danni algoritmici e sviluppi normativi europei tra "liability" e "permittance" rules.

Algorithmic damages and European regulatory developments between liability and permittance rules.

GIOVANNA D'ALFONSO
Associate Professor of Private Law
Università degli Studi della Campania Luigi Vanvitelli

Abstract

Le nuove forme di tecnologia intelligente, più o meno automatizzata, applicata ai processi di produzione di beni e di erogazione di servizi, possono dar luogo ad una pluralità di scenari dannosi completamente diversi rispetto a quelli tradizionalmente affrontati a livello giurisprudenziale, aprendosi nuove problematiche di responsabilità civile. L'articolo analizza criticamente le soluzioni offerte dai più rilevanti provvedimenti europei in fieri, dettati in materia di responsabilità civile "algoritmica" extracontrattuale, e i capisaldi della disciplina introdotta dalla proposta di regolamento, la c.d. legge sull'intelligenza artificiale. Si evidenzia il rapporto di complementarietà tra le "liability" rules, attinenti alle tematiche di natura prettamente civilistica, e le "permittance" rules, concernenti le esigenze di regolamentazione pubblicistica del settore.

The new types of intelligent technology, more or less automated, applied to the processes of production of goods and delivery of services can give rise to a multitude of damage scenarios completely different from those traditionally approached, at a jurisprudential level, opening up new issues of civil liability. The article critically analyses the solutions offered by the most relevant European regulations in progress, laid down on the subject of tort "algorithmic" liability, and the fundamentals of the discipline introduced by the proposal for a regulation, the so-called Artificial Intelligence Act. The complementary relationship between the "liability" rules, relating to issues of a strictly civil nature, and the "permittance" rules, concerning the requirements of public regulation of the sector, is highlighted.

© The author(s) 2022, 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: algorithmic damages; civil liability models; multi-layered system of responsibility; "liability" rules; "permittance" rules; European regulatory perspectives; critical remarks.

Summary: Introduzione. – 1. I "nuovi" danni algoritmici: quali modelli di responsabilità civile? – 2.1. Le questioni affrontate dal legislatore europeo. L'individuazione del soggetto responsabile nell'ambito della "catena di valore" del sistema digitale. – 2.2. (*segue*) La probatio "diabolica" del nesso di causalità tra l'operato del sistema intelligente e l'evento dannoso. – 2.3. (*segue*) Principio di accountability e "sistema multilivello" di responsabilità. – 3.1.1. Scenari normativi. Le "*permittance" rule*s e la proposta della c.d. legge sull'intelligenza artificiale. – 3.1.2. (*segue*) Punti di forza e profili critici della disciplina. – 3.2.1. (*segue*) Le "*liability rules*". La Risoluzione del Parlamento europeo «recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale». – 3.2.2. (*segue*) La proposta di revisione della direttiva sulla responsabilità per danni da prodotto difettoso. – 3.2.3.(*segue*) La proposta c.d. *AI Liability Directive*. – Conclusioni.

Introduzione.[1]

Le nuove forme di tecnologia intelligente, più o meno automatizzata, applicata ai processi di produzione di beni ed erogazione di servizi, possono dar luogo ad una pluralità di scenari dannosi completamente diversi rispetto a quelli tradizionalmente affrontati a livello giurisprudenziale, aprendosi nuove problematiche di responsabilità civile[2].

[1] Questo lavoro è il risultato del Progetto di Ricerca finanziato "Diritto e Intelligenza Artificiale: nuovi orizzonti giuridici della personalità e responsabilità robotica" (PID2019-108669RBI00 /AEI/ 10.13039/501100011033), di cui la Prof.ssa Margarita Castilla Barea è la principale ricercatrice

[2] Cfr. A. Amidei, *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in *Giur.it*. 2021, p. 100. Numerosi sono i contributi della letteratura giuridica che si è interrogata sulle problematiche sollevate dallo sviluppo esponenziale delle intelligenze artificiali, sulle complessità dell'adattamento della normativa vigente alle nuove esigenze del mondo digitale e che ha approfondito i capisaldi dei provvedimenti *in fieri*, elaborati in ambito europeo. E*x multis*, cfr. G. Alpa (a cura di), *Diritto e intelligenza artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile,* Pisa, 2020, *passim*; M. Castilla Barea, *La universidad ante los desafíos éticos de la inteligencia artificial. Reflexiones a propósito del nuevo «marco europeo de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas»*, in Edunovatic 2020, Conference Proceedings: 5th Virtual International Conference on Education, Innovation and ICT, December 10 - 11, 2020, pp. 630 ss.; S. Faro, T.E. Frosini, G. Peruginelli (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020, *passim*; P. Perlingieri, S. Giova, I. Prisco (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Napoli, 2020, *passim*; ID. (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto e economia*, Napoli, 2020, *passim*; U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Torino, 2020, *passim*; A. Santosuosso, *Intelligenza e diritto. Perché le nuove tecnologie sono una grande opportunità per il diritto,* Milano, 2020, *passim*; I. Zurita Martín, *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Reus, Madrid, 2020, *passim*, recensito da F. J. Jiménez Muñoz, in *Actualidad Jurídica Iberoamericana*, Nº 14, febrero 2021, pp. 1141 ss.; U. Ruffolo (a cura di), *XXVI Lezioni di Diritto dell'intelligenza artificiale*, Torino, 2021, *passim*; D. Buzzelli, M. Palazzo (a cura di), *Intelligenza artificiale e diritti della persona*, Pisa, 2022, *passim*; A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?, Volume 1., Diritti fondamentali, dati personali e regolazione*, Bologna, 2022, *passim*; ID. (a cura di), *Intelligenza*

La portata dei "nuovi danni" è strettamente correlata alle modalità operative delle tecnologie digitali 'emergenti'[3].

Quando le regole comportamentali e relazionali della macchina sono predeterminate, al momento della programmazione, la stessa indirizzerà le proprie scelte, azioni e risoluzioni, sulla base delle prescrizioni e dei dati forniti dal programmatore e, di conseguenza, i danni cagionati ai destinatari delle stesse potranno essere generati da un difetto di progettazione o di programmazione[4].

Diversamente, nei sistemi di intelligenza artificiale "di ultima generazione" [5], dotati di capacità di autoapprendimento, l'operato della macchina nel mondo esterno non discende da regole predeterminate, dal momento che le scelte sono assunte, in base all'elaborazione di algoritmi di *machine learning*[6], in maniera autonoma dal controllo e dall'intervento umano. Il sistema digitale, oltre a basarsi sul *training* ricevuto, si confronta con la realtà e si trasforma, in base alle interazioni con l'ambiente esterno in cui opera, dal quale può ricevere *input*; per, poi, adottare comportamenti e decisioni coerentemente con i dati esperienziali acquisiti nel tempo[7]. In tal caso, i danni possono discendere dai meccanismi di *self-learning* che elaborino opzioni difformi da quanto previsto in fase di programmazione[8].

Nel variegato panorama dei cc.dd. danni "algoritmici", viene in rilievo l'ipotesi che un sistema informatico, debitamente programmato, finisca col ledere il diritto di determinati soggetti a non essere discriminati e ad avere un

---

artificiale e diritto: una rivoluzione?, Volume 2. *Amministrazione, responsabilità e giurisdizione*, Bologna, 2022, *passim*; M. TAMPERI, *Intelligenza artificiale e le sue evoluzioni. Prospettive civilistiche,* Padova, 2022, *passim*; G. SARTOR, *L'intelligenza artificiale e il diritto*, Torino, 2022, *passim*; L. DI DONNA, *Intelligenza artificiale e rimedi risarcitori*, 2022, Padova, *passim*.

[3] Le tecnologie digitali sono riconducibili alla categoria delle c.dd. tecnologie emergenti, in ragione della velocità con la quale vengono sviluppate e del loro impatto "rivoluzionario" nei settori economici, sociali ed ambientali in cui sono impiegate. Cfr. R. MONTINARO, *Responsabilità da prodotto difettoso. Tecnologie digitali tra soft law e hard law*, in *Pers.merc.*, 2020, p. 351.

[4] Cfr. A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, *Robot e diritto: una prima ricognizione*, in *Nuova giur. comm.*, 2012, p. 494 ss.

[5] L'art. 3, proposta della c.d. Legge sull'intelligenza artificiale (Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione, Bruxelles, 21.4.2021 COM(2021) 206 final, 2021/0106(COD)), definisce «sistema di intelligenza artificiale» un *software*, sviluppato con una o più delle tecniche e degli approcci (elencati nell'allegato I), che può generare, per una determinata serie di obiettivi definiti dall'uomo, «*output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono». Può, dunque, affermarsi che l'intelligenza artificiale consiste in una famiglia di tecnologie, in grado di generare *output*. Occorre precisare che non si può parlare di un'unica intelligenza artificiale, ma bisogna parlare di intelligenze artificiali al plurale, poiché possono differenziarsi, a seconda dei tipi di *machine learning* e di agenti di *software*, più o meno autonomi. Cfr. L. COPPINI, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Politica del diritto*, 2018, p. 720.

[6] Stimata dottrina puntualizza che la caratteristica essenziale dell'intelligenza artificiale è di poter dar luogo ad un processo di autoapprendimento ed essere *self-learning,* chiarendo che il *machine learning* ed il suo molteplice atteggiarsi si caratterizza per la capacità di apprendimento della "macchina", sia che si tratti di entità robotica, sia che sia un'entità meramente immateriale. Nell'ambito dei sistemi di *machine learning*, si erge lo specifico settore applicativo del *deep learning*, che solleva ulteriori problemi, a causa della complessità dei modelli matematici usati (cd. "reti neurali" artificiali). Cfr. U. RUFFOLO, *La responsabilità da produzione e gestione dell'intelligenza artificiale self learning*, in ID. (a cura di), *XXVI Lezioni*, *op.cit.*, p. 132, s.

[7] Cfr. U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della Commissione Europea*, in *Riv.dir.civ.*, 2020, p. 1247.

[8] Cfr. V. DI GREGORIO, *Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?,* in *Danno e resp.*, 2022, p. 53.

libero ed equo accesso a beni e servizi[9]. I meccanismi di '*scoring*', ampiamente impiegati nella prassi digitale, per selezionare gli aspiranti ad una posizione lavorativa, possono condurre all'inammissibilità ad un colloquio, oltre che alla mancata assegnazione di un posto di lavoro[10]. I medesimi, utilizzati nel vaglio della potenziale solvibilità di chi miri ad ottenere un fido bancario[11] oppure nella valutazione delle caratteristiche dei clienti con cui stipulare polizze assicurative[12], possono portare ad esiti negativi della pratica bancaria o assicurativa.

Il ricorso all'algoritmo può determinare la compromissione delle libertà e dei diritti fondamentali della persona, quali la sicurezza degli individui, la loro salute, la vita privata e la protezione dei dati personali, l'integrità, la dignità, l'autodeterminazione[13].

Si pensi alle conseguenze negative che possano provenire ad una persona, sul piano economico, reputazionale ed emotivo, dal trattamento algoritmico e dalla circolazione dei suoi dati personali[14], nonché ai possibili incidenti dovuti dalla loro perdita[15]; ai danni cagionati, nel settore sanitario, alla salute del paziente dall'uso di sistemi di supporto alla diagnosi medica che, a causa della scarsa rappresentatività o del mancato aggiornamento dei dati che siano stati loro forniti, segnalino, come urgente, un erroneo trattamento curativo o farmacologico ovvero erroneamente non ne indichino uno necessario[16].

Si consideri che un algoritmo incorporato in un prodotto può cagionare un pregiudizio alla salute di chi lo adoperi o di terzi: possono verificarsi incidenti causati da un veicolo *self-driving*, il cui programma sbagli, nel valutare gli *input* che provengano dall'ambiente circostante[17]; errori commessi dai *robot* chirurgici, a danno dei pazienti[18] oppure dai *robot* industriali, a danno dei lavoratori.

---

[9] Cfr. G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, consultabile on line sul sito *www.federalismi.it*, 2020, n. 16, p. 285.

[10] Si veda la pronuncia del Cons. St., 8 aprile 2019, n. 2270, in *Foro it.*, 2019, 11, III, c. 606, riguardo agli esiti della procedura dell'assegnazione delle sedi al personale docente scolastico (l. 107/2015), compiuta sulla base di un algoritmo appositamente introdotto dal Miur.

[11] Cfr. G. BIFERALI, *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, in *Dir.inf e informatica*, 2018, p. 487 ss.

[12] Cfr. D. PORRINI, *Big data, personalizzazione delle polizze ed effetti nel mercato assicurativo*, in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2018, p. 319 ss.

[13] Sul punto cfr. M. GAMBINI, *Responsabilità civile e controlli del trattamento algoritmico*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico, op.cit.*, p. 314.

[14] Cfr. M. INFANTINO, *La responsabilità per danni algoritmici: prospettive europeo-continentali*, in *Resp. civ. e prev.*, 2019, pp. 1762 ss., par. 2, consultabile *online*, sul sito http://dejure.it

[15] Cfr. V. ZENO-ZENKOVICH, *Liability for Data Loss*, in Mak-Tjin Tai Berlee (eds.), *Research Handbook*, in *Data Science and Law*, Cheltenham, 2018, pp. 39 ss.

[16] Cfr. G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability: il carattere trasformativo dell'IA e il problema della responsabilità*, in *Anal.giur.econ.*, 2019, p. 182.

[17] Tra i contributi sul tema, cfr., *ex multis*, M. C. GAETA, *Liability rules and self-driving cars. The evolution of tort law in the light of new technologies*, Napoli, 2019, *passim*; F.P. PATTI, *The European Road to Autonomous Vehicles,* 43 FORDHAM INT'L L.J. 125 (2019), p. 125 ss.; L. GATT, I. CAGGIANO, M.C. GAETA, *Italian Tort Law and Self-Driving Cars: State of art and Open Issues,* in B.H. OPPERMANN, J. STENDER-VORWACHS (a cura di), *Autonomes Fahren. Technische Grundlagen, Rechtsprobleme, Rechtsfolgen*, München, 2020, p. 239 ss.

[18] Per un'attenta disamina della tematica della responsabilità civile nel campo della robotica medica, cfr. C. PERLINGIERI, *Responsabilità civile e robotica medica*, in *Tecnologie e diritto*, 2020 p. 165 ss. Con precipuo riguardo alla chirurgia plastica, cfr. M. MIGLIARDI, *La chirurgia plastica nell'era dell'intelligenza artificiale. Tutela della salute, privacy e consenso informato*, Padova, 2022, p. 125 ss.

L'impiego dell'algoritmo può produrre ingenti perdite agli investitori, ad esempio, per effetto di un *bug* oppure di un comportamento anomalo del programma che animi un *robo-advisor* finanziario[19].

Sorge allora il quesito di quale sia il modello di responsabilità civile più adeguato a tutelare i soggetti lesi dai sistemi digitali e a garantire loro la corretta ed equa riparazione dei danni subiti[20].

La questione assume particolare rilevanza, quando tali sistemi sono capaci di apprendimento e in grado di assumere decisioni autonome, giacché la complessità delle tecnologie incide negativamente sulla comprensione dei meccanismi, in base ai quali è stata presa una determinata risoluzione. I processi decisionali automatizzati, ideati per rispondere, oltre che a stimoli predeterminati, a nuovi impulsi, identificati autonomamente dagli algoritmi, finiscono con l'essere incontrollabili ed imprevedibili, *ex ante*, da parte di chi li progetta, li programma, li sviluppa e li utilizza; opachi *ex post*[21] e, pertanto, difficilmente spiegabili, imperscrutabili ed indecifrabili da parte dei loro destinatari, in quanto nascosti dentro una scatola nera (il c.d. effetto *black box*)[22], con conseguenti difficoltà di contestazione in sede giudiziaria[23].

Tali peculiarità rendono la soluzione non facile.

Primariamente, è difficile rispondere all'interrogativo di portata giuridica, oltre che etica, di chi e a quale titolo sia il soggetto responsabile delle condotte autonome dei sistemi tecnologici e dei danni dalle medesime provocati. Se coloro che progettano, programmano, sviluppano ed usano gli algoritmi non saranno in grado di prevederne le reazioni e, di riflesso, i pregiudizi conseguenti, in quale modo dovranno essere allocate le responsabilità[24]?

Si dovrà individuare il danneggiante, tra i soggetti che intervengono nel "ciclo di vita" dei sistemi di intelligenza artificiale, creandoli, eseguendone la manutenzione o controllandone i rischi associati[25], quali: l'ideatore-autore-progettista dell'algoritmo, veicolante l'apprendimento; l'"addestratore", figura identificabile in colui che "addestri" un'entità artificiale intelligente o comunque la esponga ad esperienze che siano congrue ad indirizzarlo ovvero ad istruirlo; colui che lo utilizzi o lo "produca" o lo incorpori in un prodotto oppure in una componente dello stesso; il programmatore del *software*; il fornitore di sistemi intelligenti ed, in alcuni casi, l'utilizzatore (*user*) o il "titolare" (a vario titolo) ovvero il "custode" della macchina[26].

Tra l'altro, tali figure possono coincidere, soprattutto nelle imprese di grandi dimensioni che, invece di affidarsi a terzi, scelgano l'internalizzazione della produzione delle componenti del prodotto digitale: si immagini un'impresa automobilistica che, nel costruire un'auto a guida autonoma, produca

---

[19] Sul tema, cfr. E. CORAPI, *Robo advice*, in G. ALPA (a cura di), *Diritto, op. cit.*, p. 401 ss.
[20] Cfr. M. GAMBINI, *op.cit.*, p. 330.
[21] Sul punto, cfr. U. SALANITRO, *op.loc.ult.cit.*
[22] Cfr. A. AMIDEI, *La responsabilità da intelligenza artificiale tra product liability e sicurezza del prodotto*, in U. RUFFOLO (a cura di), *XXVI Lezioni*, *op.cit.*, p. 150, il quale parla del «dilemma del "*black box*"».
[23] Cfr. E. TROISI, AI e *GDPR*: l'*Automated Decision Making*, *la protezione dei dati e il diritto alla 'intellegibilità' dell'algoritmo*, consultabile *online* in *EJPLT*, 2019, p. 47 ss.
[24] Cfr. M. GAMBINI, *op.cit.*, p. 330.
[25] Cfr. G. CAPILLI, *I criteri di interpretazione della responsabilità*, in G. ALPA, (a cura di), *Diritto, op.cit,* p. 477.
[26] Cfr. U. RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo,* in *Giur.it.*, 2019, p. 1698; G. CAPILLI, *op.cit.*, p. 477.

l'*hardware* e provveda all'ideazione, alla progettazione ed alla programmazione del *software* di guida intelligente.

1. I "nuovi" danni algoritmici: quali modelli di responsabilità civile?

Una volta identificati i soggetti potenzialmente responsabili, secondo le circostanze del caso concreto, è d'uopo definire il regime di imputazione e la natura della responsabilità[27].

Molte delle situazioni descritte possono involvere rapporti contrattuali, come quello di vendita di prodotti, di lavoro, di assicurazione, di banca, di intermediazione finanziaria, di opera professionale e i soggetti lesi sono legittimati ad azionare rimedi contrattuali, per ottenere la riparazione dei danni algoritmici[28].

L'Unione europea è intervenuta in sede di contratti di fornitura di contenuti o servizi digitali, con la direttiva 2019/770/UE, recepita in Italia dal d.lg. 4 novembre 2021, n. 173 (artt. 135 *octies* ss., c.cons.), riconoscendo innovativamente al consumatore la legittimazione ad azionare i rimedi contrattuali che gli spettino, in caso di difetto di conformità o di mancata fornitura del servizio o del contenuto digitale, anche laddove il trasferimento dei propri dati personali rappresenti il "corrispettivo contrattuale" della prestazione fornita dall'operatore economico. In coordinamento con tale provvedimento, la direttiva 2019/771/UE[29], recepita dal d.lg., 4 novembre 2021, n. 170 (artt. 135 *bis* ss., c.cons.), detta la disciplina della vendita dei beni di consumo, da un lato, escludendone l'applicazione ai contratti di fornitura di un contenuto o di un servizio digitale, dall'altro, disponendone l'attuazione ai contenuti digitali o ai i servizi incorporati o interconnessi con i beni e che siano forniti con gli stessi, ai sensi del contratto di vendita, indipendentemente dal fatto che detti contenuti o servizi digitali siano somministrati dal venditore o da terzi (art. 3, 3° co.) [30]. La normativa prevede la responsabilità del

[27] Cfr. I. GIUFFRIDA, *Liability for AI Decision-Making: Some Legal and Ethical Considerations*, in *Fordham Law Review*, 2019, 88, 2, p. 443.

[28] Cfr. M. INFANTINO, *op.cit.*, par. 3. Nel caso, ad esempio, di un malfunzionamento di un prodotto intelligente, come un veicolo a guida autonoma, o di un macchinario industriale, il venditore del bene sarà contrattualmente responsabile nei confronti del suo acquirente e il datore di lavoro verso il lavoratore danneggiato. Nelle ipotesi di errori provocati, nell'elaborazione dei dati personali, da parte della banca o della società assicurativa che ledano la posizione dei loro clienti, costoro potranno agire in giudizio, ai fini del conseguimento del risarcimento del danno, in forza del contratto bancario oppure assicurativo. Alla stessa stregua, il paziente potrà citare in giudizio il medico che sbagli la diagnosi o il trattamento medico o farmacologico, affidandosi all'utilizzo dell'intelligenza artificiale, facendo valere l'inadempimento dell'obbligazione di prestazione d'opera professionale. Sulla responsabilità contrattuale, connessa all'uso dell'intelligenza artificiale, cfr. M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 333 ss.; A. MASSOLO, *Responsabilità civile e IA*, *ivi*, p. 373 ss.

[29] La direttiva modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE e abroga la direttiva 1999/44/CE.

[30] Le due direttive, nell'ambito della strategia per il mercato unico digitale, mirano al bilanciamento tra l'esigenza di promozione della competitività delle imprese e la necessità di garantire un elevato livello di protezione dei consumatori. Per un'attenta analisi delle rilevanti novità introdotte, cfr., *ex multis*, A. DE FRANCESCHI, *La vendita di beni con elementi digitali,* Napoli, 2019, *passim*; R. TORINO, G. CAPILLI, *Codice del consumo: le novità per i contratti di vendita e fornitura di beni digitali,* Torino, 2022, *passim*. Per un commento al recepimento della direttiva 2019/771/UE in Spagna, cfr. M. CASTILLA BAREA, Prologuista García Vicente, José Ramón, *La nueva regulación europea de la venta de bienes muebles a consumidores. Studio de la Directiva*

professionista, per qualsiasi difetto di conformità, sussistente al momento della consegna del bene e che emerga entro due anni, stabilendo i requisiti soggettivi e oggettivi di conformità che il bene deve rispettare. Il difetto potrà concernere altresì gli elementi digitali contenuti nel bene e sussisterà, qualora gli aggiornamenti dovuti siano carenti, viziati o installati in modo imperfetto. Il venditore dovrà garantirli anche per la sicurezza dei terzi, al fine di assicurare che i beni digitali continuino ad essere conformi per il periodo previsto nel contratto oppure nell'arco temporale che il consumatore possa attendersi ragionevolmente. In ogni modo, la normativa ha una valenza distinta da quella della responsabilità del produttore che si attua al di fuori del rapporto tra le parti contrattuali; infatti, gli obblighi del venditore verso l'acquirente del bene, malgrado siano calibrati sulla sicurezza dei terzi, non si declinano in doveri verso gli altri consociati[31].

Inoltre, assume preminente interesse la questione della gamma dei rimedi applicabili, nelle ipotesi di disfunzioni degli *smart contracts*[32].

Sotto il profilo della responsabilità extracontrattuale, entrano in gioco la responsabilità per danni da prodotto difettoso ed altri modelli.

In tale contesto, assume rilevanza centrale la direttiva comunitaria 85/374/CEE sulla responsabilità per danno da prodotti difettosi, ormai confluita, in Italia, nel Codice del Consumo (negli artt. 114 ss.)[33].

(UE) 2019/771 y su transposición por el Real Decreto-ley 7/2021, de 27 de abril, Cizur Menor (Navarre), Spagna, 2021, *passim*.

[31] Per tali osservazioni, cfr. U. SALANITRO, *op.cit.*, p. 1258 s.

[32] Con tale locuzione, si fa, per lo più, riferimento a contratti in cui l'adozione della tecnologia determina procedimenti di formazione semplificati, grazie a "*software* intelligenti" ovvero protocolli informatici, per mezzo dei quali gli elementi di un rapporto contrattuale vengono formalizzati e tradotti in un codice crittografico. In sostanza, tali *software* sono in grado di eseguire autonomamente i termini dell'accordo contrattuale, codificati al loro interno, qualora siano soddisfatte le condizioni ivi definite *ex ante* (cfr. D. DI SABATO, *Diritto e new economy*, Napoli, 2020, p. 158). Il programma elettronico compie, cioè, in automatico, valutazioni relative alla sussistenza dei presupposti, delle circostanze ovvero delle condizioni per l'esecuzione del rapporto contrattuale, finendo, in tal guisa, con il sottrarre alle parti la scelta in ordine al 'se' ed al 'come' della stessa (cfr. F. DI GIOVANNI, *Attività contrattuale e intelligenza artificiale*, in *Giur.it.*, 2019, p.1697; D. DI SABATO, *op.cit.*, p. 158). Tali contratti sono ampiamente usati nel settore bancario, finanziario e assicurativo e rendono più agevole l'attuazione degli interessi delle parti contraenti, visto che costituiscono un regolamento contrattuale flessibile, idoneo ad incidere, in modo diretto, nelle vicende negoziali con programmi che, sostituendosi quasi del tutto ai contraenti umani, gestiscono la formazione, la fase esecutiva e le sopravvenienze del contratto. Cfr. D. DI SABATO, *op.cit.*, p. 156; I. MARTONE, Gli *smart contracts. Fenomenologia e funzioni*, Napoli, 2022, p. 27 ss. La letteratura sugli *smart contracts* è vastissima. *Ex multis*, cfr. M. MAUGERI, *Smart contracts e disciplina dei contratti*, Bologna 2021, *passim*. Per altro verso, tuttavia, la diffusione della contrattualizzazione algoritmica pone problematiche complesse, tra le quali, la sussistenza del rischio che l'algoritmo, nel tradurre in termini informatici la volontà delle parti che definiscono le regole del rapporto contrattuale, non ne operi una corretta trasposizione. In queste ipotesi, nasce il dubbio della conciliabilità di tale figura con i rimedi caducatori o conservativi tradizionali e ci si domanda sulla base di quali presupposti siano attivabili i rimedi restitutori e risarcitori. Cfr. I. MARTONE, *op.cit.*, p. 170 ss.

[33] La letteratura giuridica sulla disciplina della responsabilità per danno da prodotto difettoso è sconfinata. *Ex multis*, cfr. G. SALVI, *Responsabilità extracontrattuale*, in *Enc.dir.*, XXIX, Milano, 1988, p. 1229; A. GORASSINI, *Contributo per un sistema della responsabilità del produttore*, Milano, 1990, *passim*; G. ALPA, U. CARNEVALI, F. DI GIOVANNI, G. GHIDINI, U. RUFFOLO, C.M VERARDI (a cura di), *La responsabilità per danno da prodotti difettosi*, Milano, 1990, *passim*; G. PONZANELLI, *Responsabilità del produttore*, in *Riv.dir.civ.*, 1995, 2, p. 215 ss.; ID., *La responsabilità civile. Profili di diritto comparato*, Bologna, 1992, p. 112; G. ALPA, M. BIN, P. CENDON, *La responsabilità del produttore*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia* (diretto da F. GALGANO), XIII, Padova, 1989, *passim*; C. CASTRONOVO, *Danno da prodotti (dir. it. e straniero*), in *Enc.giur.*, X, Roma, 1995, 11; M. FRANZONI, *Dieci anni di responsabilità del produttore*, in *Danno e resp.*, 1998, p. 823; P.G. MONATERI, *Illecito e responsabilità civile*, in *Trattato di diritto privato* (diretto da M. BESSONE), Torino, X, 2, 2002, p. 257; L. CABELLA PISU, *Ombre e luci nella responsabilità del produttore*, in *Contratto e impresa Europa*, 2008, p. 617 ss.; A. CORDIANO, commento sub art. 114, in E. CAPOBIANCO, G. PERLINGIERI (a cura di) *Codice del consumo*

Si inizi col dire che la direttiva si apre con il principio generale, secondo il quale il "produttore" europeo è responsabile del danno cagionato dal difetto del prodotto.

Il "prodotto" è definito, nel Codice del Consumo, in maniera ampia, dall'art. 3, 1 °co., lett. d), e), (la cui definizione è ripresa dall'art. 103 c.cons., in tema di sicurezza generale dei prodotti); oltre che dall'art. 115 c.cons., che si trova in rapporto di specialità rispetto alla definizione più ampia e prevede che è "prodotto" "ogni bene mobile, anche se incorporato in altro bene mobile o immobile".

La nozione di "produttore" è estesa e include il fabbricante della componente ed il fornitore della materia prima. L'art. 121 c.cons. statuisce la responsabilità solidale di tutti gli operatori della linea di produzione, salvo il diritto di rivalsa esperibile, nell'ambito dei coobbligati.

La direttiva ha introdotto un regime di responsabilità oggettiva, dato che prescinde dall'accertamento della colpa; il danneggiato deve provare il danno effettivamente subito, il difetto del prodotto e il nesso di causalità tra difetto e danno[34].

Il criterio di imputazione si fonda sul rischio di immissione del prodotto nel mercato e sulla nozione di difetto[35].

L'art. 6 della direttiva e l'art. 117, c.cons., definiscono la "difettosità" del prodotto, con una clausola aperta alla molteplicità dei modi in cui può estrinsecarsi, in termini di mancanza di sicurezza, consistente nella difformità tra le condizioni di sicurezza concretamente offerte dal prodotto e quelle che, dallo stesso, è legittimo attendersi «tenendo conto delle circostanze», tra le quali: il modo in cui sia stato messo in circolazione, la sua presentazione, le sue caratteristiche palesi, le istruzioni o le avvertenze fornite; l'uso per il quale può essere ragionevolmente destinato e i comportamenti che, in relazione ad esso, si possono ragionevolmente prevedere; il tempo in cui è stato messo in circolazione[36]. La nozione di difetto non coincide con un vizio intrinseco del bene; ma consiste in un "giudizio di valore" che ha ad oggetto la corrispondenza del rischio attinente al prodotto (in base alle circostanze menzionate) alle legittime aspettative di sicurezza degli utenti[37]. In sostanza, sussiste la regola

---

annotato con la dottrina e la giurisprudenza, Napoli, 2009, p. 645; M. FRANZONI, *L'illecito*, in *Trattato della responsabilità civile*, seconda edizione, I, Milano, 2010, p 661 ss.; A. THIENE, *commento sub art. 114 cod. cons.*, in *Commentario breve al Diritto dei consumatori* (diretto da G. De Cristofaro, A. Zaccaria), Padova, 2010, p. 767; R. PARDOLESI, G. PONZANELLI, *Speciale 2012, "I 25 anni di products liability"*, *Danno e resp.*, 2012, *passim*.

[34] La direttiva si applica ai danni causati dalla morte o dalle lesioni personali oppure a quelli provocati alla proprietà.

[35] Cfr. G. CAPILLI, *op.cit.*, p. 471. La normativa si inserisce nell'ambito di uno spazio europeo di riferimento, nel quale rientrano provvedimenti che sono espressione dell'attuazione del principio di precauzione, quale strumento per gestire l'incertezza, facendo sì che la responsabilità sia traslata ai soggetti produttori. Cfr. U. IZZO, *La precauzione nella responsabilità civile. Analisi di un concetto sul tema del danno da contagio per via trasfusionale,* Padova, 2004, p. 1.

[36] Sul tema, *ex multis*, cfr. U. CARNEVALI, *La responsabilità del produttore*, Milano, 1974, p. 150 ss.; F. CAFAGGI, *La nozione di difetto e il ruolo dell'informazione. Per l'adozione di un modello dinamico-relazionale di difetto in una prospettiva di riforma*, in *Riv. critica dir.priv.*, 1995, p. 450 ss.; M. FRANZONI, *Responsabilità per colpa e responsabilità oggettiva*, in S. PAGLIANTINI, E. QUADRI e D. SINESIO (a cura di), *Scritti in onore di Marco Comporti,* Milano, 2008, p. 1322 ss.

[37] Sul punto, cfr. G. STELLA, *Causa ignota del danno derivante dall'uso del prodotto e responsabilità del produttore per prodotto difettoso*, in *Resp. civ. e prev.*, 2017, p. 1444 ss.; G.F. SIMONINI, *L'approccio olistico nel danno da prodotto*, in *Danno e resp.*, 2018, p. 137 ss.; G. PONZANELLI, *Responsabilità del produttore*, *op.cit.*, p. 220 ss. Tradizionalmente si distinguono quattro tipologie di difetti: i difetti di fabbricazione o di costruzione;

che non può essere superato "il livello accettabile di rischio" che il prodotto diffonde tra il pubblico, da individuarsi in riferimento al momento della sua immissione in commercio[38].

Ci domanda se tale normativa sia idonea a governare i "nuovi" rischi, derivanti dall'uso di sofisticati prodotti delle tecnologie digitali, che presentano caratteristiche molto diverse dai beni per i quali la direttiva è stata concepita negli anni Ottanta. Sorgono, difatti, difficoltà a collegare i concetti di "prodotto", di "produttore", oltre che quello di "difetto", con le questioni relative al suo accertamento, ad alcuni *smart devices*[39].

Anzitutto, si rilevi[40] che i nuovi beni delle tecnologie digitali, alle volte, sono composti da un insieme non distinguibile di cose materiali (manufatti, sensori, *hardware*) e di elementi immateriali (*software*, applicazioni, algoritmi, dati personali e non), oltre che da servizi (quali, ad esempio, la raccolta, l'elaborazione, l'analisi di dati, servizi di connettività, etc.). Invero, la componente immateriale e quella logico-informatica, che impiega e produce dati, assumono il maggior peso sia sotto il profilo economico-tecnologico, sia quanto ai rischi che possono provocare. Tali prodotti possono, poi, subire modificazioni, nel corso del loro utilizzo, a causa dell'aggiunta di *software*, di applicazioni oppure per via di estensioni e di aggiornamenti della componente digitale. Tali modifiche sono progettate dallo stesso produttore come essenziali per il funzionamento del prodotto e sono fornite da quest'ultimo e, più di frequente, da terzi per conto del primo, dopo l'immissione del bene in circolazione nel mercato.

Ancora, vi sono i prodotti intelligenti in grado di prendere decisioni autonome, come i veicoli autonomi e i *robot* chirurgici, e talvolta anche capaci di apprendimento, con le descritte conseguenze che ne derivano.

Ebbene, la questione della qualificabilità di tali beni come "prodotti" non ha rilevanza pratica, quando il contenuto digitale sia incorporato in un bene *hardware* più complesso, visto che, in tal caso, il suo fabbricante sarà certamente chiamato a rispondere verso il consumatore danneggiato, sebbene risulti difettosa la mera componente "*software*"[41]. Quesiti più complessi sorgono per i casi in cui un contenuto digitale venga venduto non insieme ad un *hardware* più articolato che lo incorpori, ma in via separata. Precipuamente per l'intelligenza artificiale, la problematica è aggravata, ancora di più, dalla rilevanza che gli algoritmi di *machine learning* ricoprono nel funzionamento del *software* (rispetto ai quali i primi sono ancora più immateriali), soprattutto

---

i difetti di progettazione, consistenti nella difformità di *design* dagli *standard* che possono esigersi, in concreto, dal produttore; la mancanza o la carenza di informazioni circa il corretto funzionamento del prodotto; i difetti da sviluppo, ossia i danni che, allo stato attuale della scienza e della tecnica, risultano del tutto imprevedibili.

[38] Cfr. R. MONTINARO, *op.cit.*, p. 360.

[39] Cfr. ID., *op.cit.*, p. 350; L. COPPINI, *op.cit.*, p. 727 ss. Per un'attenta disamina della questione dell'idoneità della disciplina vigente a regolamentare i danni causati dai *robot* intelligenti, cfr. I. ZURITA MARTÍN, *op.cit.*, *passim*; A. BERTOLINI, *Artificial Intelligence and Civil Liability,* in *Study Requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies*, Bruxelles, 2020, p. 56; U. RUFFOLO, *Responsabilità da produzione*, *op.cit.,* pp. 131 ss.; G. CAPILLI, *op.cit.*, pp. 471 ss.; A. AMIDEI, *op.ult.cit.*, p. 152 ss.

[40] Per le osservazioni che seguono, cfr. R. MONTINARO, *op.cit.*, pp. 350, 354.

[41] Sul punto e per le riflessioni che seguono, cfr. A. AMIDEI, *op.ult.cit.*, p. 153.

tenendo conto del fatto che sovente i loro autori sono diversi, rispetto a quelli che realizzano le altre componenti del prodotto.

Potrebbe, in verità, risultare difficile qualificare l'algoritmo come "prodotto", ai sensi della Direttiva, qualora, considerando che lo stesso è destinato, per sua natura, ad essere incorporato nel "prodotto" intelligente, lo si intenda come un mero progetto, una mera idea o formula, ovvero un'entità non ancora adeguata a divenire una "componente" fisica di un prodotto o di parte di esso (quali il *software* di cui sia munito). Potrebbe succedere che l'"autore" dell'algoritmo sia un soggetto diverso dal produttore dello *smart product*[42] e, secondo tale ricostruzione, il primo si configurerebbe come un semplice "fornitore" di idee o progetti e sarebbe problematico immaginare una sua responsabilità autonoma[43].

Sotto un diverso angolo di visuale, che si condivide, l'algoritmo può essere inteso quale creazione intellettuale, consistente «nella mera descrizione di un procedimento, in un pugno di *bit* o in una semplice formula matematica» e, quindi, come "componente" immateriale, caratterizzante il sistema intelligente[44].

In quest'ottica, si possono contemplare, quali produttori di una "componente" dell'entità artificiale intelligente, non solo il produttore del complessivo *software* che lo incorpori, ma anche l'ideatore-autore dei codici di programmazione, quello dell'algoritmo d'autoapprendimento o quello di altri apporti che condizionino i comportamenti del prodotto [45]. L'inventore dell'algoritmo dovrebbe, di conseguenza, essere responsabilizzato sia sul piano negoziale verso il suo committente, sia, sul piano aquiliano, verso i terzi danneggiati dal sistema tecnologico, al quale abbia attribuito il potere di apprendere e di indirizzare conseguentemente il proprio comportamento. Allora, quando l'intelligenza artificiale *self-learning*, nata ''buona'', traligni, in seguito, in *malware* (*malicious software*), potrebbe rinvenirsi la causa della distorsione della macchina, rispetto a quello che dovrebbe essere il risultato atteso, nella mancata introduzione nell'algoritmo di "blocchi", in grado di impedire le future "deviazioni" dell'intelligenza artificiale o, ad ogni modo, del *device* che la incorpori. In tale ipotesi, la "componente" algoritmo di apprendimento sarà "difettosa" e la responsabilità per il danno determinato dal difetto sarà imputabile all'inventore dell'algoritmo e sarà autonoma e distinta da quella del produttore del dispositivo che lo incorpori. La responsabilità del primo concorrerà con quella di quest'ultimo, in linea con l'approccio della direttiva europea che prevede la responsabilità cumulativa e non alternativa dei soggetti facenti parte della catena produttiva, con l'obiettivo di offrire effettiva tutela ai consumatori[46].

---

[42] Cfr. A. AMIDEI, *op.ult.cit.*, p. 150, il quale definisce l'algoritmo quale «mera linea di codice».

[43] In posizione critica verso tale impostazione cfr. U. RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, in *Giur.it.*, 2019, p. 1691.

[44] Di fatto, l'algoritmo, pur non comparendo quale componente distinta del prodotto finale, attribuisce "l'anima" al *software* di un'intelligenza artificiale complessa, incarnata o meno in entità robotica. Cfr. U. RUFFOLO, *op.loc.ult.cit.* Conformemente R. MONTINARO, *op.cit.*, p. 359.

[45] Cfr. U. RUFFOLO, *La responsabilità da produzione*, *op.cit.*, p. 134.

[46] È questa la ricostruzione di U. RUFFOLO, *Intelligenza Artificiale*, *machine learning*, *op.cit.*, p. 1691, il quale sottolinea che un ulteriore aspetto da valutare è che i danni provenienti dai sistemi di intelligenza artificiale *self-learning* potrebbero derivare da *bias*, imputabili agli "insegnamenti" ricevuti direttamente o indirettamente dall'"addestratore". In tale ipotesi, si dovrebbe considerare la responsabilità di quest'ultimo

Secondariamente, la direttiva presenta l'ulteriore criticità di "cristallizzare" il "difetto", al momento della messa in circolazione del prodotto.

L'applicazione rigorosa della disciplina attualmente vigente implicherebbe, *in primis*, che il "produttore" risponda per i difetti del prodotto o delle sue componenti, unicamente quando sussistano al tempo della messa in circolazione del bene, ancorché si manifestino successivamente. Costui potrebbe, quindi, invocare l'esimente del "difetto sopravvenuto", quando il danno sia dovuto ad una condotta anomala ed imprevedibile del prodotto, conseguente al processo di *self learning*, argomentando che la deviazione dovrebbe essere collegabile ad un difetto "iniziale", quale, ad esempio, una propensione anomala del meccanismo di autoapprendimento a determinare quel tipo di comportamenti dannosi.

In secondo luogo, il produttore potrebbe far valere l'esimente del c.d. rischio da sviluppo, attualmente opzionale a livello europeo e vigente nel nostro ordinamento, escludendo la qualificazione di "difetto" per l'anomalia dello *smart device* non prevedibile, allo stato delle oggettive conoscenze tecnico-scientifiche del tempo in cui abbia messo in circolazione il prodotto[47].

In aggiunta, la direttiva non precisa chi sia il responsabile, quando un'impresa modifichi un prodotto che sia già immesso sul mercato o qualora sia importato dal consumatore da un Paese che non sia uno Stato membro dell'Unione europea. Tale circostanza non garantisce la protezione dei consumatori e rende complesso alle imprese misurare i rischi della commercializzazione di prodotti innovativi[48].

Vieppiù, la complessità, l'autonomia, l'opacità e l'imprevedibilità dell'intelligenza artificiale si riverbera negativamente sulla posizione del danneggiato, sotto il profilo dell'onere della prova del nesso di causalità tra l'operato del prodotto digitale e l'evento dannoso.

Ordunque, le Istituzioni europee, nella consapevolezza che la direttiva ha dimostrato, per quasi quarant'anni, di essere uno strumento normativo efficace, hanno avanzato la necessità della sua modernizzazione, per adeguarla al mondo digitale[49]. Per tali ragioni, è da salutare con favore l'iniziativa della Commissione europea che, il 28 settembre 2022, ha presentato la proposta per una direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danni da prodotti difettosi[50], di revisione della disciplina attualmente vigente, che costituirà oggetto di analisi *infra*.

La proposta di revisione dovrà essere interpretata, in via sistematica, unitamente alle due proposte di regolamento, presentate, nel 2021, dalla

---

quantomeno concorrente con quella del produttore di un'entità artificiale intelligente e/o con quella dell'ideatore dell'algoritmo, se distinto da quest'ultimo. Cfr. U. RUFFOLO, *op.ult.cit.*, p. 1698 s.

[47] Per tali riflessioni, cfr. U. SALANITRO, *op.cit.*, p. 1261 s., il quale richiama le preoccupazioni della Commissione europea, esposte nella Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità, 19 febbraio 2020, (COM (2020), 64 final), p. 17.

[48] Cfr. D. MAISTO, *Nuove norme europee sulla responsabilità per danno da prodotti difettosi anche derivanti da AI*, consultabile *online*, sul sito in https://quifinanza.it/innovazione/

[49] Cfr. il punto 8 della Risoluzione del Parlamento europeo del 20 ottobre 2020 «recante raccomandazioni alla Commissione sul regime di responsabilità civile per intelligenza artificiale» (2020/2014(INL))) e la Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità, cit., pp. 15 ss.

[50] Bruxelles, 28.9.2022 COM(2022) 495 final 2022/0302 (COD).

Commissione europea, relative, l'una, alla sicurezza generale dei prodotti e l'altra alla sicurezza delle macchine. Si puntualizzi che la Direttiva 2001/95/CE sulla sicurezza generale dei prodotti si pone in termini complementari a quella sulla responsabilità per danno da prodotto difettoso, statuendo i requisiti da rispettare per la messa in commercio di beni**,** fissando la tipologia di informazioni da fornire ai consumatori e regolando l'apposizione del marchio CE. La Direttiva c.d. Macchine 2006/42/CE rappresenta la regolamentazione settoriale di riferimento, in merito alla produzione e alla messa in commercio di prodotti automatizzati, dato che definisce i requisiti essenziali, in ambito di sicurezza e di salute pubblica, ai quali devono rispondere le macchine, durante la fase di progettazione, fabbricazione e funzionamento, prima della loro immissione sul mercato. Entrambe le direttive sono state emanate in un momento in cui i nuovi prodotti tecnologici ed i dispositivi correlati erano rari e tecnicamente non avanzati, come allo stato attuale; per tale motivo, costituiscono oggetto di modernizzazione[51]. Il 21 aprile 2021 è stato pubblicato il testo della Proposta di Regolamento del Parlamento europeo e del Consiglio sui prodotti macchina che, nei prossimi mesi, una volta terminato l'*iter* di approvazione, andrà a sostituire la direttiva Macchine 2006/42/CE [52]. Il 30 giugno 2021 è stato pubblicato il testo della proposta di regolamento del Parlamento europeo e del Consiglio, relativo alla sicurezza generale dei prodotti che modifica il regolamento 1025/2012/UE e che abroga la direttiva 87/357/CEE e la direttiva 2001/95/CE[53].

Detto ciò, ci si interroga su quali siano i modelli di responsabilità civile, delineati dall'Unione Europea, per far fronte alle ipotesi in cui il paradigma della responsabilità da danno da prodotto difettoso non offra risposte esaurienti ai "nuovi danni" provocati dalle tecnologie digitali emergenti[54].

Si vaglieranno le soluzioni offerte dai provvedimenti europei *in fieri,* ponendo in evidenza che le Istituzioni europee hanno predisposto un «sistema multilivello» di responsabilità [55] che prevede sia *liability rules*, norme sulla responsabilità civile, sia "*permittance or prohibition" rules*, volte a guidare, *ex ante*, i comportamenti dei vari soggetti, coinvolti nella "catena di valore" delle entità artificiali intelligenti, in conformità al principio di *accountability*.

Si sottolineeranno i punti di forza e le criticità dell'approccio europeo.

[51] Sull'esigenza di modernizzazione della disciplina attualmente vigente sulla sicurezza dei prodotti, cfr. I. ZURITA MARTÍN, *Las propuestas de reforma legislativa del Libro Blanco europeo sobre inteligencia artificial en materia de seguridad y responsabilidad civil*, in *Actualidad Jurídica Iberoamericana*, 2021, n. 4, pp. 452 ss.
[52] Bruxelles, 21.4.2021. COM (2021) 202 final. 2021/0105(COD).
[53] Bruxelles, 30.6.2021COM (2021) 346 final, 2021/0170(COD).
[54] Come noto, la letteratura giuridica ha ricondotto i nuovi danni nell'alveo degli schemi della responsabilità civile vigenti nel nostro ordinamento giuridico. Per un'analisi delle più rilevanti ricostruzioni dottrinali, mi si consenta di rinviare a G. D'ALFONSO, *Il regime della responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, consultabile *online* in *EJPLT*, 2022, 1, pp. 101 ss.
[55] La locuzione è di G. COMANDÉ, *Multilayered (Accountable) Liability for Artificial Intelligence*, in S. LOHSS, R. SCHULZE, D. STAUDENMAYER (a cura di), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, 2019, p. 178 ss.

2.1. Le questioni affrontate dal legislatore europeo. L'individuazione del soggetto responsabile nell'ambito della "catena di valore" del sistema digitale.

In via preliminare, si precisi che, a partire dalla Risoluzione del Parlamento europeo del 16 febbraio 2017, «recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica», i provvedimenti di *soft* e di *hard law* sottolineano che l'Unione Europea si prefigge di coniugare la promozione dell'innovazione tecnologica con le esigenze di garantire la sicurezza e l'affidabilità dei prodotti e dei servizi digitali e di apprestare una tutela effettiva dei diritti e delle libertà fondamentali dei destinatari dei comportamenti e delle decisioni dei sistemi intelligenti[56].

Sin dai primi interventi, i provvedimenti adottati dalle Istituzioni Europee confluiscono nel dare attuazione alla linea giuspolitica, per la quale devono essere i diritti fondamentali ed i valori europei a guidare lo sviluppo del mercato e non viceversa[57].

Nell'apprestare un efficace complesso di tutele, si perseguono due obiettivi: evitare che l'utilizzo di tecnologie digitali possa implicare una diminuzione di sicurezza e di responsabilità rispetto a quella tradizionale (c.d. equivalenza funzionale); allocare i danni nel modo più idoneo, in capo al soggetto che sia meglio in grado di minimizzarli[58].

Ciò premesso, si indagherà sulla posizione assunta dalle Istituzioni Europee, in relazione a taluni profili critici.

Il primo aspetto da analizzare attiene all'individuazione del soggetto responsabile, nell'ambito della "catena di valore" dei sistemi intelligenti.

Si parta dalla considerazione che la presenza di tecniche sempre più sofisticate, alle quali collaborino molteplici attori (principalmente, il progettista, il programmatore, l'ideatore e l'addestratore dell'algoritmo; il produttore, il distributore; l'utilizzatore del sistema digitale), oltre che il sovrapporsi dei loro ruoli e delle loro competenze (nell'ideazione, nella progettazione, nello sviluppo, nella diffusione ed utilizzazione di tali sistemi e nell'impiego di algoritmi per l'autoapprendimento) possono rendere complesso stabilire la progressione della serie di nessi causali ed incerta l'identificazione dei soggetti danneggianti, come pure l'individuazione dei relativi criteri di imputazione della responsabilità[59].

---

[56] Cfr. A. PAJNO, M. BASSINI, G. DE GREGORIO, M. MACCHIA, F.P. PATTI, O. POLLICINO, S. QUATTROCOLO, D. SIMEOLI, P. SIRENA, *AI: profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista*, consultabile *online* sul sito www.biodiritto.org, p. 2. Per un'articolata e puntuale rassegna degli atti di *soft* ed *hard law*, cfr. G.T. ELMI, S. MARCHIAFAVA, *Sviluppi recenti in tema di intelligenza artificiale e diritto: una rassegna di legislazione, giurisprudenza e dottrina*, in Riv.it. informatica e diritto, 2022, n. 2.

[57] Cfr. G. RESTA, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale*?, *Dir.inf. e informatica*, 2022, par. 3, consultabile *online* sul sito http://dejure.it

[58] Cfr. Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità, cit., pp. 19, 22.

[59] Cfr. M. GAMBINI, *op.cit.*, p. 333. La dottrina si interroga se la circostanza che l'algoritmo abbia appreso in maniera autonoma, in modo non prevedibile, interrompa il nesso di causalità tra l'istruzione iniziale, conferita alla macchina dall'operatore economico, ed il risultato finale dell'evento dannoso prodotto dalla condotta della stessa, al di fuori del controllo e dell'intervento umano. Come pure, in situazioni di incertezza probatoria, ci si domanda non solo chi sia il responsabile, tra i vari soggetti coinvolti nell'operatività

Addirittura, taluni attori, in maniera progressiva, potrebbero acquisire il carattere dell'anonimato, con la conseguenza che potrebbe ricorrere il pericolo dei c.dd. danni anonimi[60].

Per di più, il numero dei soggetti responsabili potrebbe risultare tanto elevato da rendere impossibile, se non eccessivamente oneroso, per il soggetto leso, agire in giudizio per ottenere il ristoro: i costi giudiziari potrebbero essere troppo ingenti, potrebbero porsi problemi di giurisdizione, di notifiche da compiere e le parti entrerebbero in conflitto, esercitando domande trasversali e di manleva, per fare in modo che la responsabilità gravi sugli altri[61].

A fronte di tali difficoltà, il legislatore ha il compito di garantire ai soggetti danneggiati la possibilità effettiva di «raggiungere» il responsabile, senza dover affrontare difficoltà insormontabili[62]. In particolar modo, quando il problema sussista nella circostanza che l'evento dannoso è stato causato dal concorso delle condotte di più operatori economici, seppur indipendenti tra loro, è essenziale un modello costruito su responsabilità concorrenti che spinga, a monte, i diversi attori dei processi algoritmici a minimizzarne i rischi e a prevenire i pericoli di pregiudizio e, a valle, garantisca un'equa distribuzione degli oneri economici del risarcimento del danno tra i soggetti coinvolti nell'illecito[63].

In tale contesto, la responsabilità non può che essere solidale e «multipla» e gravare in capo a coloro che siano coinvolti nella "catena di valore", ravvisandosi l'elemento unificante nella circostanza che tutti cooperino per il raggiungimento di un obiettivo comune, consistente nel progettare, programmare e produrre un'intelligenza artificiale e le sue componenti[64]. La solidarietà passiva rafforzerà la posizione del creditore, conferendogli la possibilità di scegliere il corresponsabile più solvibile, impedendo che il danno rimanga anonimo[65]; il *solvens*, a sua volta, avvierà l'azione di regresso verso gli altri corresponsabili, in misura proporzionale alla responsabilità di ciascuno di essi.

Il giudice dovrà interpretare, in concreto, la relazione sussistente tra l'ideatore o il programmatore dell'algoritmo, il produttore del bene o il prestatore del servizio che lo incorpori ed, eventualmente, i soggetti terzi, rispetto al processo di ideazione, programmazione e sviluppo delle applicazioni intelligenti (quali il proprietario o l'utilizzatore, il gestore di rete e i potenziali

---

dell'algoritmo, ma anche se siano responsabili coloro che, seppure non abbiamo determinato l'evento che abbia provocato il danno, avrebbero potuto impedirlo Cfr. M. INFANTINO, *op.cit.*, nota 44.

[60] Cfr. D. DI SABATO, *Sistemi riparatori e risarcitori*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico*, *op.cit.*, p. 341. A titolo esplicativo, si pensi che la maggior parte degli algoritmi opera, grazie al contributo ed al coordinamento di più fattori. I codici sono redatti sovente da una pluralità di autori, quali imprese *high-tech*, sviluppatori *in house*, piccole *start-up* e contributori autonomi, che spesso lavorano senza coordinarsi, ciascuno scrivendo una parte del codice. Sul punto cfr. M. INFANTINO, *op.cit.*, par. 4.

[61] Cfr. G. CAPILLI, *op.cit.,* p. 477.

[62] Cfr. V. DI GREGORIO, *op.cit.*, p. 61.

[63] Cfr. M. GAMBINI, *op.cit.*, p. 332.

[64] Cfr. G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, 2019, p. 174 che richiama la teoria dell'impresa comune, avanzata da D.C.VLADECK, *Machines without Principals: Liability Rules and Artificial Intelligence*, in *Wash.L.Prev.*, 89, 117, 2014, p. 149.

[65] Cfr. P. PERLINGIERI, *Presentazione*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico, op.cit,* p. X.

aggressori esterni)[66]; per identificare, successivamente, l'effettivo ruolo da loro svolto sia singolarmente, sia in forma associata e porre sempre la dovuta attenzione «al *cui prodest*, secondo il broccardo *ibi commoda ubi incommoda*!»[67].

La scelta tra tali soggetti e l'eventuale configurabilità di una loro responsabilità cumulativa discenderà dalle diverse abilità delle applicazioni, dall'identificazione del compito svolto da ciascuno di essi, tanto più dalle circostanze del caso concreto[68]. In realtà, pur dovendosi riconoscere un ruolo centrale all'ideatore dell'algoritmo, la sua responsabilità deve essere cumulativa con quella del produttore del dispositivo che lo incorpori e con quella del suo utilizzatore/proprietario/custode. A sua volta, la responsabilità di quest'ultimo non potrà essere esclusa, sostenendo che potrebbe non avere le competenze per comprendere o correggere il funzionamento dell'algoritmo, considerato che, in ogni caso, se ne assume il rischio nel momento stesso in cui decide di acquistare ovvero adoperare il bene o il servizio in cui esso è incorporato. In caso contrario, ne deriverebbe una riduzione di tutela del soggetto leso, per il quale potrebbe essere complicato acquisire le informazioni essenziali, per agire in giudizio contro l'ideatore o il programmatore dell'algoritmo.

L'autorità giudiziaria dovrà sicuramente vagliare e graduare, di volta in volta, le responsabilità dei molteplici soggetti, compensando l'eventuale abbassamento del livello di responsabilità dei proprietari/utilizzatori/custodi del prodotto digitale con il rafforzamento della responsabilità del suo produttore e/o dell'ideatore dell'algoritmo[69].

In merito al profilo dei criteri di imputazione della responsabilità, è condivisibile l'orientamento dell'*Expert Group on Liability and New Technologies*[70]. Il Gruppo di esperti ha capovolto la posizione espressa dal Parlamento europeo[71] che, al fine di colmare i cc.dd. "vuoti di responsabilità", sollevati dal diffondersi delle tecnologie emergenti, aveva preferito l'elaborazione di nuove categorie e di nuove norme, proponendo, come possibili soluzioni normative, due modelli alternativi di attribuzione di responsabilità: quello della responsabilità oggettiva e quello della gestione dei rischi, da riferire, quest'ultimo, al soggetto che, tra i numerosi potenzialmente coinvolti nel verificarsi del danno, sia quello causalmente «più vicino al prodotto», a seconda del malfunzionamento che si verifichi in concreto e sia, pertanto, in grado di minimizzare i rischi e di affrontare l'impatto negativo. A differenza del Parlamento europeo, il Gruppo di esperti ha dichiarato che tali due approcci debbono essere complementari nell'attribuzione della responsabilità, soprattutto nei casi in cui l'utilizzo della tecnologia potrebbe determinare un aumento dei rischi di danno. Si è affermato che, in conformità

---

[66] Cfr. M. GAMBINI, *op.loc.ult.cit.*

[67] Cfr. P. PERLINGIERI, *Relazione conclusiva*, in. P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico, op.cit.*, p. 387.

[68] Per le notazioni che seguono cfr. M. GAMBINI, *op.cit.*, p. 332 s.

[69] Cfr. U. SALANITRO, *op.cit.*, p. 1266.

[70] Nel parere dal titolo "*Liability for Artificial intelligence and other emerging digital technologies. Report from the Expert Group on Liability and New Technologies – New Technologies Formation, European Union"*, pubblicato a maggio del 2019, punti 5-12, p. 25 ss.

[71] Nella Risoluzione del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica.

ai principi di giusta ed efficiente allocazione dei danni, si dovrà imputare la responsabilità oggettiva (a prescindere dall'accertamento della sussistenza di un comportamento colposo) al soggetto che gestisca e controlli il rischio che possa scaturire dall'immissione nel mercato del sistema intelligente e che benefici dell'operazione. Secondo tale punto di vista, la gestione del rischio rappresenta uno dei possibili criteri di imputazione della responsabilità oggettiva che sussisterà quand'anche l'impresa abbia adottato tutte le precauzioni obbligatorie, ma vi sia un rischio "residuo", connesso al tipo di attività svolta, che graverà sul soggetto che sia in condizione di sopportare i costi della collettività[72].

Si è altresì chiarito che l'imputazione della responsabilità per colpa può operare sulla base del presupposto che siano stabiliti i criteri normativi di riferimento, al fine di verificare se la condotta dei soggetti, coinvolti nella gestione delle entità artificiali intelligenti, sia stata diligente.

Si è, tanto più, sostenuta la possibile coesistenza di diverse forme di imputazione della responsabilità.

Il Gruppo di esperti è anche intervenuto sulla questione se l'imprevedibilità dei rischi connessi all'impiego delle tecnologie digitali debba condurre all'imposizione di una polizza assicurativa in capo agli operatori economici del settore. Si è esclusa l'opportunità di prescrivere l'assicurazione obbligatoria per tutti gli *smart devices*, valutando che debba essere adottata unicamente nei casi in cui l'evento dannoso sia prevedibile, calcolabile e quantificabile in somme che potrebbero condurre all'insolvenza del soggetto danneggiante, sia che debba rispondere per responsabilità oggettiva, sia per colpa. Contemporaneamente si è prospettata la possibile istituzione di fondi di compensazione, che troverebbero applicazione nei soli settori sprovvisti di assicurazione obbligatoria[73].

2.2. (segue) La probatio "diabolica" del nesso di causalità tra l'operato del sistema intelligente e l'evento dannoso.

Il secondo profilo riguarda le difficoltà che il ricorrente dovrà affrontare nel costituire la prova del nesso di causalità tra l'operato del sistema ad alta complessità tecnologica e l'evento dannoso.

La complessità e l'opacità tecnica che caratterizza i codici sottostanti agli algoritmi rende problematica l'identificazione della causa del pregiudizio: non è facile capire se derivi da un difetto del codice, dalla sua interazione con altri prodotti intelligenti, dalla qualità dei dati e delle istruzioni ricevute dall'algoritmo o dal modo in cui esso sia stato usato[74]. Gli ostacoli alla

[72] Cfr. V. DI GREGORIO, *op.cit*, p. 62.

[73] Sul punto, cfr. U. RICCIARDELLI, *Automazione self-learning e responsabilità civile: note a margine di una riflessione europea*, consultabile *online* sul sito https://rivista.camminodiritto.it/, 20 maggio 2022, p. 26 s. Sulla questione, cfr. U. SALANITRO, *op.cit.*, p. 1274, il quale ha tratteggiato la versione di un fondo di compensazione, il cui onere di finanziamento ricada non sugli utenti, bensì sui produttori ed eventualmente sui *provider*, secondo un criterio che non sia legato alla quota di mercato, quanto alla frequenza e alla gravità degli incidenti in cui il prodotto o la rete sia coinvolta. Il fondo di compensazione, così strutturato, avrebbe la funzione di coprire i danni anonimi, permettendo una parziale socializzazione dei rischi e avrebbe il vantaggio di consentire un risparmio dei costi amministrativi di gestione delle controversie.

[74] Cfr. M. INFANTINO, *op.cit.*, par. 4.

comprensione dei meccanismi inferenziali, sui quali si basano i processi decisionali automatizzati, rendono ardua la contestazione in sede giudiziaria[75].

Un argine determinante a tali implicazioni delle intelligenze artificiali è indubitabilmente rappresentato dal principio di trasparenza algoritmica[76], la cui rilevanza è emersa, in ambito europeo, già nel 2018, nella Comunicazione della Commissione al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni sull'Intelligenza artificiale per l'Europa, ove si è affermato che l'Unione Europea deve assicurare una cornice etica e giuridica che sia rispettosa dei diritti e delle libertà fondamentali dei cittadini, sul piano economico e sociale, oltre che dei principi di trasparenza e di responsabilità[77].

Si è autorevolmente affermato che codesto principio permette di accertare e correggere possibili errori del processo automatizzato, a tutela del singolo e della correttezza della procedura, sia in fase preventiva (con obblighi informativi sulla logica da seguire), sia in fase successiva, con il riconoscimento del diritto alla spiegazione delle decisioni o dei comportamenti assunti dal sistema tecnologico[78]. Nella medesima prospettiva, il principio è stato qualificato, «in prima approssimazione», come l'obbligo, posto in capo ai soggetti che adottino risoluzioni, adoperando sistemi automatizzati di trattamento dei dati personali, di fornire ai destinatari una spiegazione comprensibile delle procedure utilizzate e di motivare le risoluzioni assunte, sulla loro scorta[79].

A livello europeo, il principio è stato declinato in diverse modalità.

Nella c.d. Legge sui servizi digitali (*Digital Service Act*), entrata in vigore il 16 novembre 2022[80] (affiancata dalla c.d. legge sui mercati digitali, *Digital Markets Act*, entrata in vigore il primo novembre 2022[81]), il legislatore europeo ha accolto, per le grandi piattaforme *online*, una soluzione che si impernia su una serie di principi, tra i quali la trasparenza, l'accessibilità ai dati e agli algoritmi, l'informativa completa agli utenti, l'autonomia nella scelta del grado di profilazione[82].

Si presti ulteriormente attenzione alla proposta di Regolamento del Parlamento europeo e del Consiglio, del 21 aprile 2021 (c.d. legge

---

[75] Cfr. G. MOBILIO, *op.cit.*, p. 285; E. TROISI, *Automated Decision Making and right to explanation. The right of access as ex post information,* consultabile *online* in *EJPLT*, 2022, 1, p. 184.

[76] Cfr. P. STANZIONE, *GDPR e tutela della vita democratica*, *Relazione al convegno "Gli Stati Generali del diritto di internet*", consultabile *online* sul sito https://dirittodiinternet.it/atti-digitali-di-gli-stati-generali-del-diritto-di-internetluiss-161718-dicembre-2021-di-giuseppe-cassano-e-francesco-di-ciommo-direttori-scientifici-premessa-gli-atti-digitali-fanno, p. 6.

[77] Bruxelles, 25 aprile 2018, COM (2018) 237 final.

[78] Cfr. P. STANZIONE, *op.loc.ult.cit.* Prestigiosa dottrina sottolinea che l'algoritmo deve essere conoscibile e trasparente in tutti i suoi passaggi. È determinante garantire la completezza e la selezione dei dati e la loro adeguatezza, allo scopo della loro applicazione al caso concreto, considerato che ciò evita che la decisione possa essere neutra; come pure che i dati siano verificati, sia in via preventiva, sia successivamente al loro trattamento, al fine di impedire distorsioni. Dalla correttezza dell'algoritmo conseguirà l'idoneità della decisione automatizzata ad essere valutata giudizialmente. Per tali argomentazioni, cfr. P. PERLINGIERI, *Struttura algoritmica e interpretazione*, in *Tecnologie e diritto*, 2020, p. 487; ID. *Relazione conclusiva, op.cit.*, pp. 387, 390.

[79] Cfr. D. POLETTI, *Decisioni algoritmiche e diritto alla comprensione*, *Relazione al convegno "Gli Stati Generali del diritto di internet*", 2021, cit., p. 1.

[80] Regolamento 2022/2065/UE e che modifica la direttiva 2000/31/CE (c.d. regolamento sui servizi digitali).

[81] Regolamento 2022/1925/UE, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive 2019/1937/UE e 2020/1828/UE (c.d. regolamento sui mercati digitali).

[82] Cfr. D. POLETTI, *op.cit.*, p. 3.

sull'intelligenza artificiale)[83] che, nel dettare regole armonizzate, relative all'immissione nel mercato, alla messa a disposizione, alla messa in servizio e all'uso di sistemi intelligenti, ha scelto un modello basato sul rischio.

La proposta costituirà oggetto di attenta analisi *infra* (par. **4.1.1**.). In tale sede, preme sottolineare che ha disposto norme specifiche in materia di trasparenza algoritmica, per quanto concerne i sistemi "ad alto rischio" che, come vedremo, sono identificati sulla base della loro destinazione e del loro impatto. L'art. 12 ha stabilito che essi dovranno essere progettati e sviluppati, in maniera tale che il loro funzionamento sia tracciabile durante tutto il ciclo di vita, con la registrazione automatica degli eventi ("*log*")[84], e sia "sufficientemente" trasparente da consentire agli utenti di interpretare l'*output* e usarlo adeguatamente (art. 13). Tali sistemi dovranno essere accompagnati da istruzioni per l'uso, in un formato digitale o non digitale appropriato, con l'indicazione delle loro caratteristiche e dei loro limiti, in modo tale che il loro funzionamento sia trasparente e non opaco: a tal uopo, questi documenti dovranno contenere informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili agli utenti e a chiunque acquisti o adoperi sistemi digitali.

Invece, per i sistemi di intelligenza artificiale "a rischio basso o limitato", il legislatore europeo ha fissato solo i requisiti minimi di trasparenza. Tale scelta è stata oggetto della censura che la normativa, nello statuire obblighi di trasparenza «molto vaghi» (art. 52), sembra incidere «in maniera recessiva» su tale categoria, che, malgrado sia qualificata a "rischio limitato" include applicazioni che possono essere pericolose[85]. Precisamente, si dispone che, quando vengono usati sistemi intelligenti destinati a interagire con le persone fisiche, i "fornitori" dovranno semplicemente notificare ai consumatori/cittadini la circostanza che essi sono operativi in quell'ambito, a meno che non risulti evidente dalle circostanze e dal contesto di utilizzo. Quando si tratti di sistemi di riconoscimento delle emozioni o di categorizzazione biometrica, gli "utenti" dovranno informare le persone fisiche che vi siano esposte delle loro modalità di funzionamento. Per quanto riguarda i cc.dd. "*deep fake*", che sono sistemi che generano o manipolano immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri, gli "utenti" dovranno rendere noto che il contenuto è stato generato o manipolato artificialmente.

Il provvedimento *in fieri* è stato oggetto dell'ulteriore critica di essere intervenuto sul piano degli obblighi di trasparenza, senza riconoscere al destinatario delle risoluzioni del sistema tecnologico nessun diritto di accesso alle informazioni sul suo funzionamento; in ciò, distinguendosi dal Regolamento 2016/679/UE in materia di protezione dei dati personali (c.d. *GDPR*) che ha istituito il diritto del soggetto interessato al loro trattamento di

[83] Bruxelles, 21.4.2021 COM(2021) 206 final 2021/0106(COD)

[84] I *log* indicano il periodo di ogni impiego del sistema (data e ora di inizio e data e ora di fine) e identificano le persone fisiche coinvolte nella verifica dei risultati. Cfr. F.A. NANNI, *Analisi della Proposta di Regolamento sull'intelligenza artificiale pubblicata dalla Commissione europea il 21 aprile 2021*, in *Cyberlaws.it*, 2021.

[85] Cfr. D. POLETTI, *op.loc.ult.cit.*

accedere alle informazioni significative sia sulla logica impiegata, sia sull'importanza e sulle conseguenze previste dallo stesso[86].

A tal proposito, la letteratura giuridica si è posta il quesito se al principio di trasparenza algoritmica possa essere ricollegato un vero e proprio diritto dei destinatari di processi decisionali automatizzati di comprendere non solo la loro architettura e le loro caratteristiche, ma tanto più i criteri adottati e le ragioni delle singole risoluzioni cui siano sottoposti[87]: diritto qualificabile come diritto alla "spiegazione" o all'"interpretazione" o alla "comprensibilità" dell'algoritmo.

Goodman e Flexmann sono stati tra i primi studiosi a rinvenire, nella regolamentazione del *GDPR,* gli estremi di quello che hanno definito "il diritto all'interpretabilità umana dell'algoritmo", ricavandone un fondamento nel considerando 71, nel combinato disposto degli artt. 13 e 14 (obbligo di notifica), dell'art. 22 (divieto di essere sottoposto a una decisione completamente automatizzata), cui si affiancano il diritto di accesso (art. 15) ed il diritto di ottenere le informazioni riguardanti il trattamento dei dati personali (art. 12)[88]. Nella stessa direzione, il Art. 29 *Working Party*, alla luce del considerando 71 e dell'art. 22 *GDPR*, ha sostenuto che è nodale che i processi decisionali 'completamente' automatizzati siano controbilanciati dall'obbligo di fornire alla persona interessata le informazioni puntuali che la riguardino, dal diritto di ottenere un intervento umano ovvero di esprimere il suo punto di vista e dal diritto di conseguire una spiegazione sulla decisione presa, con la precisazione delle valutazioni che ne siano state alla base, oltre che dal diritto di poterla contestare[89].

Altra dottrina nega che l'art. 22 *GDPR* possa costituire l'appiglio normativo, per il riconoscimento del diritto alla spiegazione algoritmica, dichiarando che la norma non indica espressamente il diritto dell'interessato a essere informato sull'uso del procedimento automatizzato[90]. Taluni sottolineano che l'art. 22 è pieno di eccezioni che ne impedirebbero comunque un'applicazione piena[91]. Si è altresì osservato che il diritto alla spiegazione algoritmica non potrebbe trovare fondamento nel considerando 71, perché non si tratterebbe di una previsione giuridicamente vincolante[92].

---

[86] Cfr. G. SCHNEIDER, *Intelligenza artificiale e decisioni automatizzate: la responsabilità "regolatoria" d'impresa, oltre la compliance*, in *Riv.dir.impresa*, 2020, p. 50 s.

[87] Cfr. G. MOBILIO, *op.cit.*, pp. 284-293.

[88] Cfr. GOODMAN, S. FLEXMAN, *European Union Regulation on algorithmic decision-making and a "Right to explanation"*, in *AI MAGAZINE*, 2017, p. 51 ss. Sulla stessa linea, si riconosce che l'interpretazione sistematica di tali norme garantisca una "*legibility*" dei dati personali e degli algoritmi analitici, da intendersi come comprensibilità del funzionamento di questi ultimi. Cfr. G. MALGIERI, G. COMANDÉ, *Why a right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, p. 245 ss.

[89] Cfr. G. SIMEONE, *Machine learning e tutela della privacy alla luce del GDPR*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale, op. cit.*, p. 285 che fa riferimento al *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation* 2016/679, adottate il 3 ottobre 2017 e riviste il 6 febbraio 2018 dall'art. 29 *Working Party.*

[90] Cfr., *ex multis*, tra i primi commentatori, S. WATCHER, B. MITTELSTADT, I. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does non Exist in the General Data Protection Regulation,* in *International Data Privacy Law*, 2017, 7(2), 76–99.

[91] Cfr. M. PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in U. RUFFOLO (a cura di), *XXVI, Lezioni, op.cit.*, p. 73.

[92] Cfr. F. SARZANA DI S. IPPOLITO, M. NICOTRA (a cura di), *Diritto della Blockchain, Intelligenza artificiale e Iot, Padova*, 2018, p. 260. Tale argomentazione potrebbe essere confutata, rammentando che, ancorché i

In ogni modo, si rimarchi che, pur riconoscendo un fondamento normativo al diritto alla comprensibilità o alla spiegazione algoritmica, in fondo, non sarebbe neanche chiaro chi sia il soggetto obbligato ad assolvere l'obbligo di "spiegabilità" e verso chi sia rivolta la spiegazione. Si evidenzi che la spiegazione cambia, a seconda del destinatario in un rapporto dialogico e in considerazione del fatto che gli attori, coinvolti nel processo decisionale automatizzato, possono essere tanti e tutti spinti da esigenze di spiegazioni difformi[93].

Il dibattito sulla configurabilità di tale diritto non è sopito[94] e poche sono le pronunce giurisprudenziali sul tema. In ogni caso, quantunque sia auspicabile un intervento normativo che garantisca la trasparenza degli algoritmi in senso ampio, con riferimento a tutte le possibili applicazioni dell'intelligenza artificiale ed oltre i limiti, di cui all'art. 22 *GDPR*; da un altro punto di vista, il bisogno di ottenere la spiegazione del funzionamento degli algoritmi incontra i limiti correlati sia alle privative industriali ed alla segretezza commerciale, sia alle conoscenze tecniche altamente qualificate, necessarie per capirne il significato ed il funzionamento. In effetti, qualsivoglia sia il linguaggio di programmazione utilizzato, la scrittura e la lettura degli algoritmi esige competenze speciali e la comprensione del percorso che ha condotto l'algoritmo ad uno specifico risultato è tanto più complicata, quanto più autonomo ed intelligente sia lo stesso[95].

In conclusione, a dispetto di tali problematiche, la posizione probatoria del ricorrente può essere "alleggerita" dall'imposizione, in capo ai danneggianti convenuti, di obblighi di *disclosure* di informazioni sugli elementi di prova, necessari alla dimostrazione della sussistenza del nesso di causalità tra l'evento dannoso e il funzionamento dello *smart device*- quantomeno per quanto attiene alle applicazioni di intelligenza artificiale ritenute a rischio elevato e ad ambiti particolarmente "sensibili", quali quello sanitario ed automobilistico[96].

Questa opzione è stata accolta dalle Istituzioni europee, nelle due recenti proposte di direttive sulla responsabilità civile che saranno esaminate *infra.*

2.3. (segue) Principio di accountability e "sistema multilivello" di responsabilità.

Alla luce delle riflessioni svolte, appare chiaro che la complessità, l'autonomia, l'opacità dei sistemi di intelligenza artificiale e l'incertezza delle regole del loro funzionamento rendono i tradizionali paradigmi della

---

considerando non abbiano autonomo valore normativo, può, ad ogni modo, riconoscersi, come ribadito dalla Corte di Giustizia dell'Unione Europea, un loro ruolo ermeneutico supplementare, facendo luce sull'interpretazione da attribuire ad una norma di legge. Cfr. C. TABBARRINI, *Comprendere la "Big Mind": il GDPR sana il divario di intelligibilità uomo-macchina?*, in *Dir.inf. e informatica*, 2019, p. 555 ss., par. 2., consultabile *online* sul sito http://dejure.it

[93] Cfr. M. PALMIRANI, *op.cit.*, p. 72 s. che richiama S. WATCHER, B. MITTELSTADT, I. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does non Exist in the General Data Protection Regulation, op.loc.ult.cit.* e J.H.N. JANSSEN, *The right to explanation: means for "white boxing' the black-box?*, Tilburg, 2019, *passim.*

[94] Parte della dottrina identifica il diritto alla spiegazione del processo decisionale automatizzato nel diritto di accesso, di cui all'articolo 15 *GDPR*. Cfr. E. TROISI, *op.ult.cit.,* p. 197. *Contra* G. FINOCCHIARO, *Intelligenza e protezione dei dati personali*, in *Giur.it*, 2019, p.1675.

[95] Per tali osservazioni, cfr. M. INFANTINO, *op.cit.*, par. 4.

[96] Cfr. A. AMIDEI, *op.ult.cit.*, p. 159.

responsabilità civile inefficienti, per garantire una tutela effettiva dei diritti e delle libertà fondamentali dei destinatari delle loro risoluzioni.

Ne consegue che, in tale contesto, la responsabilità civile non può avere un ruolo prioritario[97] e che è compito del legislatore affrontare due ordini di questioni giuridiche: le «*issues of liability*», attinenti alle tematiche di natura prettamente civilistica e le «*issues of permittance*», concernenti le esigenze di regolamentazione pubblicistica del settore[98].

Sovviene, cioè, la necessità di sviluppare, accanto alla disciplina della responsabilità civile "algoritmica", norme amministrative che stabiliscano i parametri su cui orientare la programmazione, la produzione e la commercializzazione dei sistemi digitali e che fissino nuove procedure per la loro verifica e convalida, allo scopo di poter valutare e controllare la sicurezza, la trasparenza, la comprensibilità, la rendicontabilità e la responsabilità etica degli stessi[99].

Solo in tal modo, potrà realizzarsi un'intelligenza artificiale affidabile ed antropocentrica[100] e costruire un'architettura di entità artificiali intelligenti, idonea a garantire la loro conformità ai principi etici ed alle normative vigenti dell'Unione Europea[101].

Il modello legislativo più congruo a risolvere i problemi giuridici correlati all'innovazione tecnologica deve essere permeato dai principi di prevenzione e di precauzione ed elaborare un "sistema multilivello di responsabilità" che sia imperniato sul principio di *accountability,* analogamente a quanto previsto dal *GDPR*[102]. Si deve, cioè, puntare alla massima responsabilizzazione dei soggetti coinvolti nell'intero processo, a partire dall'ideazione e dalla programmazione

---

[97] Cfr. D. DI SABATO, *op.ult.cit.,* p. 343.

[98] Sul punto cfr. A. AMIDEI, *Intelligenza Artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur.it.*, 2019, p. 1718.

[99] Cfr. il Parere del Comitato economico e sociale europeo su «L'intelligenza artificiale. Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società», Document 52016IE5369 (punto 3.16).

[100] Cfr. Commissione europea, Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie, Orientamenti etici per un'IA affidabile, Ufficio delle pubblicazioni, 2019, punti 87 e ss.

[101] Cfr. M. GAMBINI, *op.cit.*, p. 326. In relazione ai profili etici dell'Intelligenza artificiale è molto importante la Risoluzione del Parlamento europeo del 20 ottobre 2020, «recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate» (2020/2012(INL)), ove si è previsto, in linea con la logica del *based risk*, il bisogno di regole che fissino un'impostazione etica predefinita, sin dalla progettazione dei sistemi intelligenti; la possibilità di un intervento umano, al fine di sopperire all'asimmetria tra coloro che impieghino le tecnologie digitali e coloro che vi siano assoggettati. Alla Risoluzione è allegata la proposta di Regolamento del Parlamento europeo e del Consiglio «sui principi etici per lo sviluppo, la diffusione e l'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate» che intende «istituire un quadro normativo dell'Unione di principi etici e obblighi giuridici per lo sviluppo, la diffusione e l'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate nell'Unione». Esso statuisce molteplici e specifici obblighi per le tecnologie ad "alto rischio". Per un approfondimento, cfr. M. CASTILLA BAREA, *op.loc.ult.cit.* Già prima dell'emanazione del provvedimento, la dottrina ha posto in evidenza che le Istituzioni Europee sono profondamente consapevoli della necessità di realizzare una cornice di regole per lo sviluppo di un'intelligenza artificiale antropocentrica «nel senso di tutelante e potenziante l'essere umano in quanto tale». Cfr. *Per un'intelligenza antropocentrica. Intervista a Lucilla Gatt*, consultabile *online* in *Diritto mercato tecnologia*, 21 febbraio 2020.

[102] Sul punto cfr. G. COMANDÉ, *Multilayered (Accountable) Liability for Artificial Intelligence*, in S. LOHSS, R. SCHULZE, D. STAUDENMAYER (a cura di), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, 2019, p. 178l; M. GAMBINI, *op.cit.*, p. 325, s. Il *GDPR* affida al titolare del trattamento la scelta delle soluzioni più idonee, per il raggiungimento dell'obiettivo della gestione del rischio, derivante dal trattamento dei dati personali, prevedendo che dovrà, di seguito, risponderne, qualora sorgano problemi. Cfr. R. CARLEO, *Il principio di accountability nel GDPR: dalla regola alla auto-regolazione*, in *Nuovo diritto civile*, 2021, p. 366. Sul punto si tornerà *infra*.

fino all'impiego delle applicazioni algoritmiche, facendo gravare su di loro l'obbligo di rendere conto delle decisioni assunte a coloro che ne subiscano gli effetti.

Sotto un altro punto di vista, le regole della responsabilità civile, quale che sia la norma applicabile scelta, devono essere "immerse" nel più ampio perimetro della responsabilizzazione dei ruoli di tutti i soggetti presenti nel ciclo di vita dei sistemi digitali. Da ciò discenderà una nozione di responsabilità civile che assumerà una connotazione diversa, più ampia e connessa al principio di *accountability*. In tale ottica, la responsabilità civile rappresenterà solo un «tassello del mosaico», dovendo essere integrata e potenziata da altri strumenti pubblicistici di tutela preventiva[103].

3.1.1. Scenari normativi. Le "permittance" rules e la proposta della c.d. legge sull'intelligenza artificiale.

La Commissione europea si sta muovendo in tale direzione.

Per un verso, ha elaborato norme volte a ridurre e gestire i rischi per la sicurezza e a tutelare i diritti fondamentali. Per altro verso, nella consapevolezza dell'impossibilità di eliminare tutti i potenziali rischi e nella persuasione che la sicurezza e la responsabilità sono due facce della stessa medaglia che si applicano in momenti diversi e si rafforzano a vicenda, la Commissione ha dettato norme in materia di responsabilità civile, da applicare allorché tali rischi dovessero concretizzarsi e cagionare danni[104].

Nel quadro normativo che si sta delineando, sul piano delle "*permittance" rules*, si pongono le due proposte di regolamento, *supra* menzionate, l'una relativa alla sicurezza generale di prodotti e l'altra relativa alla sicurezza delle macchine; nonché la proposta di regolamento, definita c.d. legge sull'intelligenza artificiale, che assume una portata di nodale importanza.

La proposta di regolamento si pone l'obiettivo di «delineare una cornice giuridica alta ed armonizzata» [105]: "armonizzata", dacché si impegna a fissare regole uniformi, da applicare a livello europeo; "alta", siccome ha l'ambizione di promuovere lo sviluppo dell'intelligenza artificiale, mirando, da un lato, a ridurre al minimo i rischi per la sicurezza e i diritti fondamentali, intervenendo prima dell'immissione dei sistemi intelligenti sul mercato dell'Unione europea, dall'altro lato, garantendo certezza giuridica.

Il provvedimento *in fieri* si inserisce nell'ambito del disegno strategico europeo di assicurare un mercato digitale comune e di consentire all'Unione Europea «di essere un *leader* mondiale nello sviluppo di un'intelligenza artificiale sicura, affidabile ed etica» e un «*leader* nella produzione

---

[103] Per tali argomentazioni, cfr. G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability*, *op.cit.*, pp. 180, 184.

[104] Cfr. Relazione della Commissione alla Proposta per una direttiva del Parlamento europeo e del Consiglio, relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale; c.d. direttiva sulla responsabilità da intelligenza artificiale/*AI Liability Directive*, Bruxelles 29 settembre 2022, (COM (2022) 496 final 2022/0303 (COD)), punto 1.

[105] Cfr. V. FALCE, *Regolamento IA tra innovazione, valori e concorrenza*, *Relazione al convegno*, dal titolo "*Gli Stati Generali del diritto di internet*", 2021, cit., p. 1.

normativa»[106]. Nel contesto geopolitico, si mira a far sì che il modello europeo divenga un riferimento globale nel mercato delle tecnologie, che possa essere usato nelle altre regioni del mondo [107], riproducendo il c.d. «effetto Bruxelles»[108].

Non sorprende, perciò, che la proposta di regolamento- in modo analogo a quanto previsto dal *GDPR*, in relazione al trattamento transfrontaliero dei dati personali, al *Digital Service Act* e al *Digital Market Act*- individui un ambito di applicazione territoriale che travalica i confini del mercato interno [109]. La normativa e l'apparato sanzionatorio si applicheranno, effettivamente, non soltanto ai "fornitori" e agli "utenti" dei sistemi digitali immessi o utilizzati nel territorio dell'Unione Europea, ma anche ai "fornitori" e agli "utenti" che siano situati al di fuori di tale area, quando l'*output,* prodotto dal sistema sia impiegato in ambito europeo.

La proposta di regolamento definisce in maniera generica e descrittiva (tutti) i sistemi di intelligenza artificiale, all'art. 3, n. 1, adoperando un criterio orizzontale omnicomprensivo. Prevede, infatti**,** regole generali, per profilare uno spazio complessivo, nel quale operino tutti i sistemi digitali (a titolo esplicativo, sia il medico, sia il finanziario), oltre che quelli ancora non ideati.

Tale opzione è stata oggetto della critica che presenterebbe il limite intrinseco di trattare tutte le applicazioni di intelligenza artificiale in modo sostanzialmente omogeneo, quando, viceversa, sono diversissime tra loro e possono assumere distinte caratteristiche, a seconda dell'ambito in cui vengano usate[110].

La nuova disciplina adotta un modello di gestione, basato su una «piramide» ascendente dei rischi, connaturati nell'impiego di dispositivi intelligenti, che va dal rischio "medio o basso", al rischio "alto", fino al rischio "inaccettabile"[111], per compiere una graduazione di regole che fissino divieti, obblighi e misure di *enforcement*, modulandole in funzione del diverso livello di rischio connesso a determinate tipologie di attività. Il «rischio tipico» non è definito in corrispondenza dei valori di mercato, quanto, piuttosto, avendo precipuo riguardo alla cornice dei valori e dei diritti fondamentali riconosciuti dall'Unione Europea[112]. In sostanza, l'obiettivo primario che la proposta persegue è la tutela dei diritti fondamentali e la salvaguardia del processo democratico[113].

---

[106] La relazione introduttiva della proposta di regolamento dichiara lo scopo di «tutelare la sovranità digitale dell'Unione e di sfruttare gli strumenti e i poteri di regolamentazione di quest'ultima per plasmare regole e norme di portata globale» p. 7.

[107] Cfr. G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv.trim.dir.pubbl.*, 2022, pp. 1085 ss. par. 2, consultabile *online* sul sito http://dejure.it; G. RESTA, *op.cit.*, par. 2, il quale offre spunti di comparazione della *policy* europea con la cinese e la statunitense.

[108] Per l'elaborazione di tale tesi, cfr. A. BRADFORD, '*The Brussels Effect'*, 107 Northwestern U.L. Rev. (2013), p. 1.

[109] Cfr. G. RESTA, *op.cit.*, par. 4. L'autore (*ivi*, par. 2) evidenzia come l'adozione di una clausola ampia e strutturalmente indeterminata, come quella dell'art. 2, par. 1, lett. c), tracci una «via molto scivolosa per il legislatore europeo».

[110] Cfr. G. FINOCCHIARO, *op.ult.cit.*, par. 3.

[111] Cfr. Dossier 57, 12 novembre 2021, di commento alla proposta della c.d. Legge sull'intelligenza artificiale della Camera dei Deputati, Ufficio Rapporti con l'Unione europea, XVIII legislatura, p.1.

[112] Cfr. G. RESTA, *op.cit.*, par. 6.

[113] Di fatto, il legislatore tratteggia un modello regolatorio rispondente al «paradigma dei diritti fondamentali». Cfr. G. RESTA, *op.cit.*, par. 3.

Si pone, perciò, un divieto, con eccezioni e deroghe, e si impedisce l'ingresso nel mercato interno ai sistemi intelligenti che creino un rischio "inaccettabile", relativamente alle violazioni delle libertà fondamentali e dei diritti, riconosciuti e garantiti a livello europeo. In concordanza al principio di prevenzione, si vieta, la messa in servizio sia di sistemi che adoperino tecniche subliminali che agiscano senza che una persona ne sia consapevole, sia di quelli che sfruttino la vulnerabilità di uno specifico gruppo di persone, dovuta all'età o alla disabilità fisica o mentale, quando tali sistemi siano volti a distorcere materialmente il comportamento di tali soggetti, in un modo che provochi o possa cagionare a tale persona o a un'altra un danno fisico o psicologico[114]. È vietata l'immissione nel mercato e la messa in servizio di sistemi di *social scoring* (punteggio sociale, adottato in Cina), lesivi della dignità umana e di quelli di identificazione biometrica remota «in tempo reale», in spazi accessibili al pubblico, come quelli di riconoscimento facciale.

Per i sistemi a rischio "basso o limitato", si sono stabiliti (unicamente) obblighi di trasparenza e si incoraggia l'elaborazione di codici di condotta[115].

La normativa si incentra prevalentemente sui sistemi "ad alto rischio", classificati in quelli destinati ad essere usati come componenti di sicurezza di prodotti soggetti a valutazione della conformità *ex ante* da parte di terzi; in altri sistemi intelligenti indipendenti che presentano implicazioni, principalmente in relazione ai diritti fondamentali, esplicitamente elencati nell'allegato III[116].

In linea generale, sono dettate una serie di previsioni volte a far sì che tali sistemi siano affidabili durante la loro progettazione, il loro sviluppo e la loro esecuzione. A tale scopo, li si assoggetta ad una procedura di valutazione di conformità *ex ante* che si concluda con la marcatura CE.

Sono fissati dettagliatamente gli obblighi e i requisiti che i sistemi "ad alto rischio" dovranno rispettare (artt. 8 ss.)[117]. A norma dell'art. 8, al fine di garantire la conformità ad essi, bisognerà tenere conto sia della finalità prevista dall'entità artificiale intelligente, sia del sistema di gestione dei rischi, disposto dall'art. 9.

Prima di tutto, ai sensi dell'art. 9, paragrafi 1 e 2, si dovrà istituire, attuare, documentare e mantenere un modello di gestione dei rischi, vale a dire un processo iterativo continuo, eseguito nel corso dell'intero ciclo di vita di un sistema "ad alto rischio", che richiederà un aggiornamento costante e sistematico. Esso comprenderà le fasi successive di identificazione ed analisi dei rischi noti e prevedibili associati al sistema; la stima e la valutazione dei rischi che potranno emergere, quando il sistema sia utilizzato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile; la valutazione di altri eventuali rischi derivanti dall'analisi dei dati,

---

[114] Cfr. G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir.inf. e informatica*, 2022, par. 3, consultabile *online* sul sito http://dejure.it. L'Autrice puntualizza che la criticità sussiste nelle eccezioni previste dal legislatore.

[115] La dottrina individua, in una prospettiva sistematica, un quarto livello di rischio che si potrebbe definire "minimo" o nullo, nel quale far rientrare tutti gli altri sistemi di intelligenza artificiale che potranno essere sviluppati e impiegati, senza necessità di adeguamento alla normativa suddetta. Cfr. E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in D. BUZZELLI, M. PALAZZO (a cura di), *Intelligenza artificiale e diritti della persona, op.cit.*, p. 101, p. 107.

[116] Cfr. Relazione della Commissione europea che accompagna la proposta, punto 5.2.3.

[117] Per le considerazioni che seguono, cfr. G. FINOCCHIARO, *op.ult.cit.*, par. 3.

raccolti dal monitoraggio successivo all'immissione sul mercato; oltre che l'adozione di adeguate misure di gestione dei rischi.

Nell'ottica del principio di *accountability*, i risultati elaborati dai sistemi "ad alto rischio" dovranno essere verificati e tracciati, lungo il loro intero ciclo di vita[118]. La documentazione tecnica che li riguarderà dovrà essere redatta, prima della loro immissione sul mercato o della loro messa in servizio e in modo tale da dimostrare che il sistema digitale è conforme ai requisiti statuiti dal Regolamento; dovrà essere sottoposta ad aggiornamento continuo; fornirà alle autorità nazionali competenti e agli organismi notificati tutte le informazioni necessarie per valutare codesta conformità. Sono statuiti obblighi di conservazione delle registrazioni automatiche degli eventi (*file di log*) (art. 12).

I sistemi "ad alto rischio" devono essere progettati e sviluppati, in modo tale da garantire la trasparenza; con strumenti che ne consentano la supervisione umana, mirante a prevenire e ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali (art. 14); in modo tale da ottenere, in conformità alla loro finalità, un adeguato livello di accuratezza, robustezza e cibersicurezza che duri per l'intero ciclo di vita (art. 15).

Sono poi individuati alcuni criteri di qualità per i *set* di dati adoperati per l'addestramento, la convalida e la prova. Tali *set* devono essere sottoposti ad adeguate pratiche di *governance* e di gestione dei dati, di cui all'art. 10, par. 2, e devono essere pertinenti, rappresentativi, esenti da errori e completi e statisticamente appropriati.

Ulteriori obblighi e requisiti derivano, per tali sistemi, dalle norme che fissano specifici adempimenti proporzionati, in capo ai soggetti coinvolti nella filiera della loro creazione e del loro utilizzo: il "fornitore" (*ex* art. 3, par. 1, n. 2); l'"utente" (*ex* art. 3, par. 1, n. 4); l'"importatore" (*ex* art. 3, par. 1, n. 6) ed il "distributore" (*ex* art. 3, par. 1, n. 7).

In più, si prevede l'individuazione o l'istituzione, da parte degli Stati membri, di un'autorità di vigilanza e controllo dell'applicazione del Regolamento. Si istituisce il Comitato europeo per l'intelligenza artificiale, costituito dai rappresentanti degli Stati membri e della Commissione (art. 58), con il compito di raccogliere e condividere le migliori pratiche, di vigilare sull'attuazione della disciplina, oltre che di facilitare l'attuazione del provvedimento *in fieri* e di contribuire ad un'efficace cooperazione con le autorità nazionali di vigilanza e con la Commissione.

Si stabiliscono strumenti di *enforcement*, attribuendo all'autorità di sorveglianza nazionale poteri e misure, per assicurare il rispetto dei requisiti e degli obblighi menzionati. Specificamente l'autorità, se dovesse avere motivi sufficienti per ritenere che un sistema intelligente presenti un rischio per la salute o la sicurezza o per la tutela dei diritti fondamentali delle persone (ai sensi dell'art. 65, par. 1), effettuerà una sua valutazione, relativamente alla sua conformità ai requisiti e agli obblighi suddetti.

A loro volta, i fornitori saranno tenuti, in conformità al principio di *accountability*, a dimostrare all'autorità la "conformità" del sistema "ad alto rischio".

[118] Cfr. F.A. NANNI, *op.loc.ult.cit.*

In ogni caso se, nel corso di tale valutazione, l'autorità rileverà talune difformità, potrà imporre all'operatore pertinente l'adozione di misure appropriate per far cessare la violazione; ritirare il sistema dal mercato o richiamarlo per un tempo ragionevole, commisurato alla natura del rischio (art. 65, par. 2). Di tali azioni dovrà essere data comunicazione sia alla Commissione europea, sia agli altri Stati membri, per l'eventuale attivazione di corrispondenti misure di salvaguardia.

Infine, il regolamento statuisce che dovranno essere approntate, da parte degli Stati membri, le sanzioni amministrative pecuniarie, applicabili in caso di sua violazione e che le stesse dovranno essere effettive, dissuasive e proporzionate, dovendo, in particolar modo, tenere conto degli interessi dei "fornitori" di piccole o medie dimensioni e delle *start-up* e della loro sostenibilità economica.

3.1.2. (segue) Punti di forza e profili critici della disciplina.

Tratteggiati i capisaldi della disciplina, può elencarsi, tra i punti di forza, la scelta dello strumento normativo del regolamento, il cui impiego ha il pregio di assicurare l'uniformità in ambito europeo, nell'ottica di fornire la certezza del diritto necessaria sia agli operatori economici, per agevolare gli investimenti, l'innovazione e la concorrenza in tale settore; sia agli utilizzatori, per facilitare la circolazione delle tecnologie emergenti nel mercato e dare loro fiducia sul conseguimento di un elevato livello di tutela dei propri diritti.

La proposta di regolamento presenta una serie di criticità, tra le quali, in primo luogo, la rigidità delle definizioni dei sistemi digitali[119], siccome non solo non si tiene conto delle difformità tra le diverse applicazioni di intelligenza artificiale, ma neppure delle innovazioni, dal momento che qualunque sviluppo tecnologico dovrà essere inserito nella "griglia" definita dal legislatore. Sebbene la classificazione dei sistemi digitali sarà soggetta a revisione, come previsto nel regolamento, sicuramente la rapidità del progresso tecnologico determina il pericolo che le applicazioni future di intelligenza artificiale saranno regolamentate nella prospettiva attuale. Il metodo prescelto non è, pertanto, sufficientemente dinamico, per seguire gli sviluppi futuri[120].

In realtà, l'inadeguatezza della proposta di regolamento, sotto questo punto di vista, discende dalla circostanza che, nel redigerla, si è prediletto un approccio *top-down*. È, difatti, il legislatore ad identificare le tecnologie dell'intelligenza artificiale, a determinare le pratiche proibite e rischiose e ad individuare, *ex ante*, il diverso livello di rischio, dal quale far discendere le regole applicabili, lasciando poco spazio alla valutazione dei destinatari delle stesse. Questo metodo implica il pericolo di elaborare delle categorie normative astratte che non rappresentino in modo congruo le caratteristiche ed i rischi delle tecnologie digitali emergenti [121].

[119] Per le riflessioni che seguono, cfr. G. FINOCCHIARO, *op.ult.cit*, par. 4.
[120] Per tale critica, cfr. G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale, op.cit.*, par. 4.
[121] Sul punto, cfr. G. RESTA, *op.cit.*, par. 6.

Sarebbe, diversamente, più congruo un approccio *bottom-up*[122], come quello impiegato nel *GDPR*, ove l'apprezzamento del rischio è conferito, in prima battuta, ad una valutazione decentralizzata. Il provvedimento si contraddistingue per l'impianto normativo fondato sul principio di *accountability*, ossia sulla responsabilizzazione del titolare del trattamento che è tenuto a mettere in atto misure tecniche ed organizzative "idonee" a garantire un livello di sicurezza confacente al rischio, come pure a dare attuazione ai principi ed alle norme del regolamento. Tali misure dovranno essere scelte, in conformità alle caratteristiche peculiari del trattamento, più precisamente, ai sensi dell'art. 32, «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche». La decisione sull'appropriatezza delle risoluzioni da adottare sarà rimessa alla "discrezionalità" del titolare del trattamento che non sarà, però, illimitata, poiché dovrà essere necessariamente parametrata alle condizioni descritte. Il titolare del trattamento, oltre a valutare e scegliere le misure di sicurezza idonee, dovrà compiere un'attività di continuo monitoraggio, anche attraverso l'elaborazione di modelli organizzativi specifici. Inoltre, costui dovrà essere in grado di dimostrare tutto, provando la congruità delle scelte di regolamentazione compiute in modo autonomo[123].

Quest'impostazione consente un adattamento costante del modello di gestione del rischio da parte del titolare del trattamento dei dati personali e si basa evidentemente sul convincimento che costui sia il soggetto nella posizione migliore per gestire e valutare il rischio[124].

Tale risultato è stato raggiunto dal legislatore della *privacy*, cambiando la tecnica legislativa (originariamente adoperata nel recepimento Direttiva 95/46/CE), passando da un approccio che si basava su regole molto dettagliate a quello (diverso) del *GDPR*, che si fonda su principi generali e sulla responsabilizzazione del titolare del trattamento[125]. Si sono previste norme c.dd. "in bianco", per 'delegare' i privati ad individuare le regole più idonee, rendendoli responsabili e gravandoli dell'onere di fornire la prova della conformità alle stesse.

Si è, in tal modo, incentivato il ricorso all'autodisciplina, mediante codici di condotta, inquadrabili in linea con il principio di sussidiarietà orizzontale *ex* art. 118 Cost., la cui redazione è stata affidata ai destinatari delle norme, più vicini agli interessi generali che devono essere regolati; oltre che per mezzo

---

[122] Cfr. G. CONTISSA, F. GALLI, F. GODANO, GA. SARTOR, *Il Regolamento europeo sull'intelligenza artificiale. Analisi informatico-giuridica*, consultabile *online* in *i-lex. Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, 23 dicembre, 2021, p. 1 ss.

[123] Per tali notazioni, cfr. R. CARLEO, *op.cit.*, p. 356 ss. Si è affermato (G. FINOCCHIARO, *Intelligenza e protezione dei dati personali*, *op.cit.*, p. 1676) che l'*accountability* può tradursi come «responsabilità e, insieme, prova della responsabilità» ed è un meccanismo a due livelli, l'uno di attuazione di misure, l'altro di conservazione delle prove.

[124] Cfr. G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale, op.cit.* par. 4, secondo la quale, mentre il sistema di gestione del rischio è accompagnato dal principio di *accountability* nel *GDPR*, ciò non accadrebbe nella proposta della c.d. legge sull'intelligenza artificiale, dove la valutazione e la gestione del rischio dei sistemi intelligenti non è rimessa alle scelte degli operatori economici, ma al legislatore che detta regole tecniche, senza lasciare spazio a questi ultimi.

[125] Cfr. R. CATERINA, *Novità e continuità nel Regolamento generale sulla protezione dei dati*, in *Giur.it.*, 2019, p. 2777.

dell'elaborazione di *standard* "tecnici" di comportamento, non determinati dal legislatore, ma delegati ad organi non legislativi[126].

Si rilevi che i codici di condotta e l'elaborazione di *standard* "tecnici" comportamentali assumono rilevanza altresì nella disciplina della proposta della c.d. legge sull'intelligenza artificiale.

Anzitutto, l'art. 8 dispone che la "conformità" del sistema intelligente dovrà essere valutata alla stregua di determinati "*standard*". Essi saranno elaborati dalle *standard-setting organizations* europee[127]. È essenziale sottolineare che, se, per un verso, i produttori ed i fornitori di sistemi intelligenti potranno, in linea di principio, prescindere dalle norme tecniche armonizzate, elaborate da tali organizzazioni e provvedere autonomamente a riempire di contenuto la previsione legislativa; per altro verso, la presunzione di conformità, ai sensi dell'art. 40, potrà ritenersi sussistente unicamente quando vi sarà un adeguamento agli *standard,* elaborati da tali organizzazioni. Da ciò discende che «il vero ruolo nomotetico» finirà per l'essere svolto dalle *standard-setting organizations*. Tale circostanza presenta la problematicità che le organizzazioni suddette sono private; conseguentemente, le stesse 'vendono' *standard* (a loro volta protetti dal diritto d'autore) ed il loro operato provocherà una gamma di seri problemi, in termini di trasparenza e rappresentatività, rispetto a delle scelte che si riverbereranno sui diritti e sulle libertà fondamentali dei destinatari delle risoluzioni dei sistemi digitali e sullo stesso processo democratico.

Per quanto concerne i codici di condotta, la proposta di regolamento, al titolo IX, istituisce una cornice per la loro creazione che mira a incoraggiare i fornitori di sistemi intelligenti "non ad alto rischio" ad applicare volontariamente i requisiti obbligatori, previsti per quelli "ad alto rischio", concernenti i dati, la documentazione e la tracciabilità, la fornitura di informazioni e la trasparenza, la sorveglianza umana, la robustezza e la precisione. Le imprese che dovessero introdurre i codici di condotta per i sistemi "non ad alto rischio" lo faranno su base volontaria e potranno attuarli autonomamente[128].

Si aggiunga che recentemente la Commissione europea ha inaugurato un *sandbox*, da intendersi come uno "spazio di sperimentazione normativa", in cui le aziende potranno testare i loro prodotti e servizi, interagendo con le autorità di regolamentazione pertinenti. Il fine di tale iniziativa è di garantire certezza giuridica, nell'ambito delle soluzioni tecnologiche decentralizzate, individuando gli ostacoli normativi all'introduzione delle scelte degli operatori economici e fornendo consulenza giuridica, sulla base delle *best practices* e dell'evoluzione normativa, in un contesto dedicato, riservato e sicuro. Lo spazio

[126] Per tali argomentazioni, cfr. R. CARLEO, *op.cit.*, p. 363 s.

[127] Per le osservazioni sul tema G. RESTA, *op.cit.*, par. 6, che menziona il *CEN*, *European Commitee for Standardization* e il *CENELEC, European Committee for Electrotechnical Standardization*.

[128] Tali codici potranno altresì comprendere impegni volontari relativi, ad esempio, alla sostenibilità ambientale, all'accessibilità da parte delle persone con disabilità, alla partecipazione dei portatori di interessi alla progettazione e allo sviluppo dei sistemi di intelligenza artificiale, come pure alla diversità dei gruppi che si occupano dello sviluppo. Cfr. Relazione alla proposta di regolamento. Punto 5.2.7.

di sperimentazione è finanziato, per gli anni 2023-2026, dal *Digital Europe Programme*[129].

Alla luce di tali considerazioni, può affermarsi che, a fronte dei limiti della tecnica normativa prescelta, nella proposta di regolamento, cionondimeno sia i codici di condotta, seppure limitatamente a coloro che decidano di adottarli, sia i *sandboxes* avranno, senza dubbio, un ruolo fondamentale nell'adeguamento di suddetta disciplina alla realtà complessa ed in continua evoluzione delle intelligenze artificiali[130].

Un ulteriore aspetto critico della proposta di regolamento è individuabile nella circostanza che il *risk-based approach* implica che i rilevanti oneri amministrativi di redazione e di aggiornamento della documentazione, di certificazione, di notifiche, di marcatura incomberanno sulle imprese, indipendentemente dalle loro dimensioni e dalla tipologia di applicazione dell'intelligenza artificiale. Come ovvio, il peso di tali oneri e costi graverà in misura minore sulle grandi imprese ed in misura maggiore sulle piccole e medie imprese e sulle *start up*. L'opzione di dettare la medesima regolamentazione, senza differenziare tra i soggetti e i distinti ambiti di operatività delle nuove tecnologie, è stata confutata, argomentando che le applicazioni di intelligenza artificiale possono essere molto diverse tra loro ed essere declinate in maniera difforme[131]. Pur condividendo tale obiezione, occorre porre in evidenza che il legislatore europeo ha conferito agli Stati membri la funzione di prevedere misure di sostegno per le piccole e medie imprese e che il Consiglio europeo, nel c.d. orientamento generale del 6 dicembre 2022 (*infra*), ha previsto innovativamente talune misure a loro supporto.

Ulteriormente, alla domanda se la proposta di regolamento tuteli idoneamente i diritti ed i valori europei costantemente richiamati, si risponde che esso lascia completamente scoperto il profilo dei diritti e dei rimedi individuali[132]. Il provvedimento *in fieri*, pur proclamando di voler difendere i valori ed i diritti fondamentali dell'Unione europea dai rischi dell'intelligenza artificiale, si focalizza sugli obblighi e sulle prerogative del "fornitore", dell'"utente", dell'"importatore" e del "distributore", definendo una cornice amministrativa per l'immissione dei sistemi digitali nel mercato. Non riconosce, tuttavia, ai destinatari dei processi decisionali automatizzati diritti, quali il diritto ad ottenere una spiegazione del meccanismo di funzionamento dell'entità artificiale intelligente e dell'algoritmo e il diritto a non essere soggetti a decisioni discriminatorie. Né si configurano, distintamente dal *GDPR*, nuovi strumenti di tutela che la persona, individualmente o collettivamente, possa attivare, per rendere la tutela effettiva, più rapida ed efficace[133].

Ebbene, si segnali che, il 6 dicembre 2022, il Consiglio ha adottato la sua posizione comune (c.d. orientamento generale) sulla proposta di regolamento,

---

[129] Cfr. https://www.corrierecomunicazioni.it/digital-economy/blockchain-leuropa-lancia-la-prima-sandbox-normativa/

[130] Cfr. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'UE in materia di intelligenza artificiale*, in *BioLaw Jorunal*, 2021/2, p. 29, consultabile online sul sito https://www.biodiritto.org

[131] Per le considerazioni di tale critica, cfr. G. FINOCCHIARO, *op.ult.cit.*, par. 4.

[132] Per il commento su tale questione, cfr. G. RESTA, *op.cit.,* par. 6; G. FINOCCHIARO, *op.ult.cit.*, par. 4.

[133] Saranno certamente applicabili i principi sostanziali previsti dal *GDPR* a tutela dei dati personali.

apportando delle modifiche al testo originario e intervenendo su taluni aspetti problematici evidenziati[134].

Primariamente, si circoscrive la definizione di intelligenza artificiale ai sistemi sviluppati mediante l'apprendimento automatico e a quelli basati sulla logica e sulla conoscenza, al fine di semplificare la distinzione tra sistemi *software* più semplici e le tecnologie di intelligenza artificiale. Nella classificazione di queste ultime, si impone di prendere in considerazione altresì la rilevanza dell'*output* del sistema tecnologico, rispetto all'azione pertinente oppure alla decisione da assumere. Si aggiunge, in tal modo, un livello orizzontale alla catalogazione, per evitare l'inclusione, tra le intelligenze artificiali "ad alto rischio", di quelle che non presentino il pericolo di causare gravi violazioni dei diritti fondamentali o altri rischi significativi.

Ancora, dal momento che i sistemi intelligenti sono sviluppati e distribuiti attraverso "catene di valore" complesse, sono stati chiariti ed adeguati i requisiti per i sistemi ad "alto rischio", allo scopo di renderli tecnicamente più realizzabili e meno onerosi per i portatori di interessi. A tal fine, il testo contiene chiarimenti sull'assegnazione di ruoli e di responsabilità ai vari soggetti coinvolti nelle catene di sviluppo e di distribuzione delle tecnologie emergenti, in modo specifico, i "fornitori" e gli "utenti"; oltre che precisazioni sui rapporti tra la responsabilità, ai sensi del Regolamento sull'intelligenza artificiale, e gli altri regimi previsti dalle diverse normative preesistenti, quali quella sulla protezione dei dati personali e la normativa settoriale, come quella riguardante l'ambito dei servizi finanziari.

In linea con il principio di proporzionalità, in forza del quale è indispensabile diversificare la posizione delle piccole-medie imprese e di quelle di grandi dimensioni, vi sono novità concernenti la qualità dei dati e la documentazione tecnica che le piccole e medie imprese dovranno redigere, per provare la conformità dei loro sistemi "ad alto rischio" ai requisiti previsti. Nella stessa direzione, si differenziano i massimali delle sanzioni amministrative, per renderli più proporzionati, in caso di violazioni da parte delle piccole e medie imprese e delle *start-up*.

Si pongano in evidenza le puntualizzazioni sulle procedure di valutazione della conformità e sulla vigilanza del mercato e l'introduzione di disposizioni, per conferire maggiore autonomia e rafforzare il ruolo del comitato per l'intelligenza artificiale e per garantire il coinvolgimento dei portatori di interessi.

La posizione definitiva del Parlamento europeo sulla proposta di Regolamento dovrebbe volgere al termine, a fine marzo 2023. In seguito, avrà inizio il trilogo tra il Consiglio, il Parlamento e la Commissione e il testo verrà adottato[135].

---

[134] Sul punto e per l'analisi di altre modifiche innovative, cfr. il Comunicato stampa del Consiglio europeo, 6 dicembre 2022, consultabile *online* sul sito https://www.consilium.europa.eu/it/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/; M. MARTORANA, R. SAVELLA *Intelligenza artificiale: orientamento del Consiglio europeo e ultimi sviluppi nella definizione del Regolamento*, consultabile *online* sul sito https://www.altalex.com/documents/news/2023/02/15/intelligenza-artificiale-orientamento-consiglio-europeo-ultimi-sviluppi-definizione-regolamento.

[135] Il Regolamento, una volta recepite le indicazioni dei pareri, si applicherà dopo che siano trascorsi due anni dalla sua effettiva entrata in vigore, per consentire a tutti gli operatori di predisporre gli adempimenti

Conclusivamente, alla luce delle notazioni critiche riportate, può dichiararsi che il modello di gestione del rischio, approntato dalla proposta di regolamento, si presenta rigido e statico, difformemente dal modello flessibile e dinamico, costruito dai principi ispiratori e dalla tecnica normativa del *GDPR*. Sarebbe, quindi, auspicabile un cambio di rotta delle Istituzioni europee che, nel revisionare la disciplina della proposta sulla c.d. "intelligenza artificiale", si ponga nel solco del modello virtuoso offerto dal *GDPR* e si focalizzi sull'esigenza di: considerare 'realmente' la rapidità dello sviluppo tecnologico; conferire agli operatori economici una maggiore discrezionalità, seppur parametrata su requisiti prefissati, affinché possa effettuare le scelte più adatte al settore in cui agisca e alle peculiarità del sistema intelligente; garantire strumenti di tutela effettivi ai soggetti danneggiati dalle risoluzioni dei sistemi intelligenti.

3.2.1. (segue) Le "liability" rules. La Risoluzione del Parlamento europeo «recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale».

Sul fronte delle *"liability" rules*, si incentri l'attenzione anzitutto sulla Risoluzione del Parlamento europeo, del 20 ottobre 2020, che ha chiesto alla Commissione di presentare, sulla base dell'articolo 225 TFUE, una proposta di regolamento sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale, seguendo le raccomandazioni dettagliate, figuranti nell'allegato alla risoluzione stessa.

Il Parlamento ha prospettato l'applicazione del regolamento nel territorio dell'Unione Europea, dove un'attività, un dispositivo o un processo virtuale o fisico, guidato da un sistema digitale, arrechi un danno o un pregiudizio alla vita, alla salute, all'integrità fisica di un individuo, al patrimonio di una persona fisica o giuridica ovvero un danno non patrimoniale rilevante, risultante in una perdita economica verificabile (art. 2, par. 1).

Il Parlamento europeo ha abbandonato la posizione, inizialmente assunta (nella Risoluzione del 2017, recante norme di diritto civile sulla robotica, cit.), del riconoscimento della "personalità elettronica" ai sistemi intelligenti [136], proponendo la soluzione innovativa di configurare, come responsabile, il c.d. *deployer*, l'operatore degli stessi. Tale opzione è stata ispirata dalla circostanza che costui beneficia dell'andamento dell'automa ed esercita il controllo sul rischio che vi è associato, in modo analogo al proprietario di un'automobile; inoltre, considerata la complessità delle entità artificiali intelligenti, l'operatore, in molti casi, sarà il primo punto di contatto visibile per il soggetto leso (punto 10 risoluzione).

La proposta di regolamento, nel sancire la responsabilità degli "operatori", li ha classificati sulla base del grado di supervisione che adoperino sul loro

necessari dal punto di vista organizzativo, tecnico e commerciale, al fine di poter essere *compliant* ai sistemi intelligenti, come strutturati dalla Proposta.

[136] Il Parlamento europeo si è basato sulla posizione negativa espressa dal Comitato economico e sociale europeo che ha esposto perplessità di carattere giuridico ed etico. Cfr. il Parere del Comitato economico e sociale europeo, 526a sessione plenaria del CESE del 31 maggio e primo giugno 2017 su "L'intelligenza artificiale. Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società", (2017/C 288/01), punto 3.33.

funzionamento. Si è differenziato tra l'"operatore *front-end*" e l'"operatore *back-end*", definendo il primo come la persona fisica o giuridica che effettua un certo grado di sorveglianza su un rischio connesso all'operatività del sistema intelligente e che ne beneficia (quale, ad esempio, il proprietario o il custode dell'autovettura o del dispositivo automatizzato); il secondo come la persona fisica o giuridica che, su base continuativa, stabilisce le caratteristiche della tecnologia, fornisce i dati e il servizio di supporto di *back-end* essenziale ed è in grado di esplicare un elevato grado di verifica sul pericolo, connesso all'operatività o al funzionamento del sistema tecnologico (per esempio, il gestore di una autostrada attrezzata per la guida automatizzata)[137].

Seguendo un metodo basato sul rischio, la proposta di regolamento ha delineato un duplice statuto giuridico, misurato sul grado di automazione del sistema digitale[138].

Per gli operatori di sistemi "ad alto rischio" (quali, ad esempio, gli aeromobili senza equipaggio, i veicoli con livello di automazione elevato, i sistemi autonomi di gestione del traffico, i dispositivi autonomi di pulizia di luoghi pubblici)[139], si è disposto un regime di responsabilità oggettiva, stabilendo che costoro non possano eludere la propria responsabilità, sostenendo di avere agito con la dovuta diligenza o che il pregiudizio sia stato cagionato da un'attività, da un dispositivo o da un processo autonomo, guidato dal loro sistema di intelligenza artificiale; e individuando l'unica esimente nella causa di forza maggiore. Le attività "ad alto rischio" sono state qualificate (art. 3, lett. c)), in base alla probabilità e alla gravità dei potenziali danni, al grado di autonomia e alle modalità o all'ambito di utilizzo dello strumento digitale.

L'individuazione delle attività "ad alto rischio" è stata deputata alla Commissione europea con un apposito allegato, statuendo che debba essere sottoposto al suo vaglio ed aggiornamento, almeno a scadenza semestrale.

Il legislatore europeo ha imposto a tale categoria di operatori la stipula di una polizza assicurativa, a copertura della propria attività, distinguendo la tipologia di assicurazione (art. 4, par. 4), a seconda che si tratti di operatore *front end* oppure *back en*d. D'altra parte, il Parlamento europeo ha ritenuto che la copertura della responsabilità civile rappresenti uno dei fattori determinanti per il successo delle nuove tecnologie e che spinga il pubblico ad avere fiducia, nonostante la possibilità di subire pregiudizi o di dover affrontare azioni legali (par. 23 della risoluzione cui è allegata la proposta di regolamento).

Si è, poi, sottoposto l'operatore di un sistema digitale non configurabile "ad alto rischio" (e non inserito nell'elenco allegato al regolamento in ragione della circostanza che l'automazione non è tanto elevata) ad un regime di responsabilità per colpa "aggravata" da un complesso di presunzioni[140]. Si è, cioè, esclusa la responsabilità dell'operatore che riesca a dimostrare che la lesione cagionata non sia imputabile a sua colpa, per uno dei seguenti motivi: il sistema si è attivato, senza che ne fosse a conoscenza e siano state adottate

[137] Cfr. U. SALANITRO, *op.cit.*, p. 1275.
[138] Cfr. C. LAENZA, *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*, in *Resp. civ. e prev.*, 2021, p. 1013.
[139] Per un'attenta analisi della categoria dei sistemi di intelligenza artificiale "ad alto rischio", introdotta, per la prima volta, nella proposta di regolamento, cfr. R. LOBIANCO, *Veicoli a guida autonoma e responsabilità civile: regime attuale e prospettive di riforma - I e II Parte*, in *Resp. civ. e prev.*, 2020, p. 724 ss., p. 1080 ss.
[140] Cfr. C. LAENZA, *op.cit.*, p. 1011 ss.

tutte le misure ragionevoli e necessarie, per impedire tale attivazione oppure costui ha svolto diligentemente le operazioni appropriate all'uso dell'intelligenza artificiale (selezionando un meccanismo idoneo al compito e alle competenze, mettendolo debitamente in funzione, monitorando le attività e mantenendo l'affidabilità operativa, mediante periodici aggiornamenti).

Si è dettata la regola della responsabilità solidale, sia quando vi dovesse essere un concorso di colpa di più operatori, sia nel caso in cui più operatori dovessero essere coinvolti in un danno causato da un'attività "ad alto rischio". Si è prevista l'esperibilità, da parte del *solvens*, di un'azione di regresso verso gli altri operatori, in misura proporzionale alla sua responsabilità.

Il provvedimento ha predisposto la riduzione del grado di responsabilità dell'operatore o la sua esclusione, rispettivamente quando il pregiudizio dovesse essere prodotto dal concorso di colpa del soggetto danneggiato oppure possa essergli esclusivamente imputabile.

In aggiunta, il Parlamento europeo ha ritenuto che la disciplina della responsabilità civile per colpa, vigente negli Stati membri, offra, il più delle volte, un livello sufficiente di tutela alle persone che subiscano danni, in seguito all'interferenza di un terzo, quale un *hacker*, dato che, in tal caso, il soggetto leso avvierà un'azione basata sulla colpa[141]. Si è comunque profilata la necessità di ulteriori norme, per integrare il diritto nazionale in materia di responsabilità civile, in ipotesi specifiche, incluse quelle in cui il terzo sia irrintracciabile oppure insolvibile.

La proposta di regolamento redatta dal Parlamento europeo, ai fini di una redazione da parte della Commissione, in linea con le indicazioni fornite, è stata oggetto di svariate critiche.

Prima di tutto, in relazione all'ambito oggettivo di applicazione, si è contestata la scelta di unificare la regolamentazione dei danni determinati dai sistemi intelligenti, usando un criterio orizzontale omnicomprensivo, invece di diversificare le applicazioni dell'intelligenza artificiale ed i relativi contesti di riferimento, quali, a titolo esplicativo, quello domestico, il medico, il finanziario oppure l'industriale[142].

In merito all'ambito soggettivo di applicazione, si è espresso scetticismo verso la distinzione tra operatore *back-end* e *front-end*, dichiarando che sarebbe stato preferibile, per il danneggiato, identificare, a monte, un "*entry point*", al quale rivolgersi in caso di danni, per rimettere, di seguito, a rivalse ed altri meccanismi la distribuzione della responsabilità tra i vari soggetti coinvolti, nella catena del sistema digitale[143].

Dal punto di vista processuale, si è rilevato che il «regime flessibile» di responsabilità prescelto[144] avvantaggerebbe la posizione processuale di coloro che abbiano subito un pregiudizio dagli operatori di un sistema "ad alto rischio", per i quali è stato statuito un regime di responsabilità oggettiva, con l'esimente della causa di forza maggiore. Vieppiù, la proposta di regolamento non ha

---

[141] Cfr. Risoluzione del 20 ottobre 2020, recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, cit. (punto 9).

[142] Cfr. A. BERTOLINI, F. EPISCOPO, *The Expert Group's Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies: a critical assessmen*t, in *European Journal of Risk Regulation*, 2021, 12, 3, pp. 648 ss.

[143] Cfr. ID., *op.cit.* p. 656.

[144] Secondo la locuzione elaborata da U. SALANITRO, *op.cit.*, p. 1276.

previsto nulla riguardo alla *probatio* "diabolica" del nesso di causalità tra l'operato del sistema digitale e l'evento dannoso.

Infine, si evidenzi che la proposta di regolamento ha spostato l'attenzione dal produttore all'operatore, chiarendo, tuttavia, la coesistenza con la disciplina della responsabilità per danno da prodotto difettoso e la necessità di uno stretto coordinamento ed allineamento tra le due normative, a livello europeo e nazionale (obiettivo 6, allegato alla risoluzione)[145]. In particolare, l'art. 11, nel regolamentare la responsabilità in solido, ha fissato i criteri di prevalenza dell'una sull'altra, quando l'operatore sia anche il produttore di un sistema tecnologico. Precipuamente la norma ha sancito che, se un operatore di *front-end* dovesse essere altresì il produttore del sistema di intelligenza artificiale, le disposizioni del presente regolamento dovrebbero prevalere su quelle della direttiva sulla responsabilità per danno da prodotti difettosi; se l'operatore di *back-end* fosse anche il produttore, ai sensi dell'articolo 3 della direttiva suddetta, sarebbe opportuna la sua applicabilità a tale soggetto; se vi fosse un solo operatore che fosse anche il produttore del sistema, le previsioni del presente regolamento dovrebbero prevalere su quelle della direttiva.

Per di più, l'art. 12, par. 3, ha disposto che, qualora l'operatore di un sistema tecnologico difettoso dovesse "indennizzare" interamente la persona interessata per danni o pregiudizi, sia che dovesse rispondere a titolo di responsabilità oggettiva, sia che dovesse rispondere a titolo di colpa presunta, potrebbe esperire un'azione di regresso nei confronti del produttore dello *smart device* difettoso, conformemente alla disciplina europea ed alle norme nazionali che regolamentano la responsabilità per danno da prodotto difettoso.

Si osservi, infine, che il legislatore aveva optato per lo strumento normativo del regolamento, ritenendo insufficiente la direttiva, in ragione della rilevanza strategica del settore[146], nella consapevolezza che, se lo si fosse approvato, avrebbe comunque imposto esigenze di coordinamento con la disciplina nazionale ed un intervento di adeguamento a quella europea.

Concludendo, occorre rimarcare che tale iniziativa legislativa non ha avuto seguito, giacché la Commissione europea ha avanzato una differente proposta di regolamentazione della responsabilità civile extracontrattuale per l'intelligenza artificiale, per le ipotesi che non siano riconducibili al paradigma della responsabilità per danno da prodotto difettoso.

3.2.2. (segue) La proposta di revisione della direttiva sulla responsabilità per danni da prodotto difettoso.

Invero, il 28 settembre 2022, la Commissione europea ha presentato due proposte di direttive che dovranno essere approvate dal Parlamento europeo e dal Consiglio, in un pacchetto finalizzato ad adeguare le norme sulla responsabilità civile all'economia circolare, all'era digitale e all'impatto delle catene globali del valore, garantendo l'allineamento dovuto tra questi due strumenti giuridici necessari.

---

[145] Sulla coesistenza di tali regole, cfr. V. DI GREGORIO, *op.cit.* p. 55 ss.
[146] Cfr. U. SALANITRO, *op.cit*, p. 1274, s.

La prima propone la revisione della direttiva sulla responsabilità per danno da prodotto difettoso. Obiettivo della sua modernizzazione è di garantire la certezza giuridica sia alle imprese che devono potere innovare nel settore delle tecnologie digitali emergenti, oltre che assumere i nuovi modelli di economia circolare, modificando, in maniera sostanziale i prodotti, nella consapevolezza delle responsabilità che possano incombere su di loro e calcolando i rischi da dover sopportare; sia ai potenziali danneggiati dai sistemi digitali che devono poter accedere a un panorama normativo semplificato, rispetto a quello attualmente vigente. Si avverte, in effetti, la necessità di apprestare strumenti di tutela effettiva, rispetto ai nuovi danni e ai nuovi difetti, e di fornire la garanzia di trovare sempre un responsabile in Europa, quand'anche il prodotto provenga da uno Stato al di fuori dell'Unione Europea[147].

La seconda è la c.d. *AI Liability Directive* che introduce un regime di responsabilità differenziato per il settore dell'intelligenza artificiale, da applicare ai soli giudizi civili, aventi ad oggetto la richiesta di risarcimento di danni, promossi davanti ai giudici nazionali, in caso di colpa extracontrattuale. La disciplina non include i rischi derivanti dalla produzione e dall'impiego di prodotti digitali, ad eccezione delle ipotesi di violazione di normative di sicurezza, ponendosi in rapporto di complementarità alla proposta di direttiva sulla responsabilità oggettiva del produttore.

Entrambe le proposte di direttive sono, a loro volta, complementari alla proposta della c.d. legge sull'intelligenza artificiale [148].

Orbene, si rimarchi, prima di tutto, che, nella redazione della disciplina di revisione della direttiva della responsabilità per danno da prodotto difettoso, la Commissione ha optato per lo strumento normativo della direttiva, anche se il Parlamento le aveva proposto di valutare se la direttiva attualmente vigente dovesse essere trasformata, in fase di revisione, in regolamento[149]. L'art. 3 ha stabilito il livello di armonizzazione massima.

La proposta di revisione, pur mantenendo l'impianto della responsabilità oggettiva dei produttori per il risarcimento dei danni causati da prodotti non sicuri, ha previsto una serie di disposizioni innovative, per uniformare il regime della responsabilità del produttore alle nuove sfide del settore digitale.

Primariamente si amplia l'ambito oggettivo di applicazione, intervenendo sulla disciplina del danno, sulla definizione del "prodotto" e di quella di "difetto".

Si riconosce il diritto al risarcimento del danno a "qualunque persona fisica" che subisca un pregiudizio da un prodotto difettoso, nella sfera patrimoniale e in quella personale. Oltre ai danni a, o la distruzione della proprietà[150], alla morte o alle lesioni personali, si ricomprendono, in maniera innovativa, tra i

[147] Progetto di parere, CESE, 16 gennaio 2023, Proposta di direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi. INT/1002, Revisione della direttiva sulla responsabilità per danno da prodotti difettosi, punti 1.3., 2.1.

[148] Sul punto, cfr. "*Consistency with other Union policies*" della proposta della Commissione della direttiva, consultabile *online* sul sito https://ec.europa.eu/info/sites/default/files/1_1_197605_prop_dir_ai_en.pdf, p. 5 s.

[149] Risoluzione del Parlamento europeo del 20 ottobre 2020, recante raccomandazioni alla Commissione sul regime di responsabilità civile per l'intelligenza artificiale intelligenza artificiale, cit., (punto 8).

[150] Le persone potranno chiedere il risarcimento del danno sia quando la proprietà danneggiata sia impiegata per scopi professionali, sia quando lo sia per scopi personali.

danni, quelli alla salute psicologica scientificamente riconosciuti e la perdita o la corruzione di dati personali, non usati esclusivamente a fini professionali[151].

La Commissione, dopo aver precisato, nella relazione alla proposta, che i sistemi tecnologici ed i beni che si basino sull'intelligenza artificiale sono considerati "prodotti", amplia notevolmente tale nozione, comprendendo, nell'ambito di applicazione della normativa, le componente digitali, quali le applicazioni ed altri *software* "integrati" in un prodotto o "interconnessi"- che rientrano nelle definizioni di "componente" (articolo 4, paragrafo 3), di "servizio correlato" (articolo 4, paragrafo 4) e di "fabbricante" (articolo 4, paragrafo 11)[152].

Un'altra importante novità concerne il concetto di "difetto", disciplinato dall'art. 6. Si statuisce un nuovo "*test* di difettosità" del prodotto, rispetto alla sicurezza «che il grande pubblico può legittimamente attendersi tenuto conto di tutte le circostanze». Questo *test*, coincidente, in sostanza, con quello previsto dalla direttiva attualmente vigente, è adeguato ai nuovi prodotti, con l'imposizione di considerare criteri riferiti, in modo specifico, agli *smart devices*, quali: i requisiti di *cyber-security*; i potenziali effetti negativi sul prodotto causati dalla sua capacità di apprendere successivamente al rilascio sul mercato [153] e «gli effetti sul prodotto di altri prodotti che ci si può ragionevolmente attendere siano utilizzati» insieme allo stesso, prendendo in considerazione la connettività tra i sistemi[154].

In tale ottica, vengono in rilievo i danni provocati dalla circostanza che prodotti, come i robot, i droni o i sistemi domestici intelligenti, siano resi insicuri da aggiornamenti *software*, dall'intelligenza artificiale oppure da servizi digitali necessari per il funzionamento del prodotto; nonché quelli che siano cagionati dalla condotta dei produttori che non gestiscano la vulnerabilità dei sistemi informatici[155].

Ad ogni modo, la proposta chiarisce che tutti i parametri di sicurezza obbligatori, sia quelli stabiliti dall'Unione Europea, sia quelli previsti in ambito nazionale, debbono essere presi in considerazione in sede giudiziale, quando si valuti la difettosità di un prodotto.

L'art. 7, nel regolamentare la responsabilità degli "operatori economici", definisce "la gerarchia delle responsabilità" tra i soggetti coinvolti nella catena di approvvigionamento del prodotto difettoso, in misura proporzionata al ruolo di ciascuno di essi. È, in tal modo, garantita la ricerca dell'operatore responsabile, ai fini del risarcimento del danno[156]. Tra i soggetti responsabili in prima linea, si pone il fabbricante del prodotto e quello della componente che

---

[151] Le nuove regole non permetteranno, nondimeno, il risarcimento per la violazione dei diritti fondamentali, come quando l'impiego discriminatorio di un *software* di reclutamento impedisca l'esito positivo di un colloquio di lavoro. Cfr. *Presse release*, 28 september 2022, Bruxelles, "*New liability rules on products and AI to protect consumers and foster innovation*", consultabile *online* sul sito https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807".

[152] Progetto di parere, CESE, cit., punto 4.5.

[153] Cfr. S. Neri, R. Almanza, *Percorsi di riforma: la responsabilità da prodotto difettoso alla prova dell'AI*, consultabile *online* sul sito hhtps://www.wfw.come/articles, 9 febbraio 2023.

[154] Cfr. G. Proietti, *Responsabilità per danno da prodotti difettosi alla luce degli ultimi sviluppi tecnologici*, consultabile *online* sul sito www.dirittobancario.it, 27 ottobre 2022, par. 3.

[155] Cfr. *Presse release*, 28 september 2022, Bruxelles, "*New liability rules on products and AI to protect consumers and foster innovation*", cit.

[156] Sul punto cfr. Progetto di parere, CESE, punti 3.3., 4.1.

sia la causa del difetto cagionato. Potranno essere responsabili, oltre ai fabbricanti di *hardware*, anche i fornitori di *software* e di servizi digitali che incidano sul funzionamento del prodotto[157]. Qualora si tratti di un fabbricante stabilito al di fuori dell'Unione Europea, può essere ritenuto responsabile l'importatore o, in sua mancanza, il rappresentante autorizzato dal fabbricante. Vengono anche indicati, come responsabili, il fornitore di servizi di logistica, il distributore o il fornitore di una piattaforma *on line*.

L'art. 11 dispone che, qualora vi siano due o più operatori economici responsabili dello stesso danno, ai sensi della direttiva, gli Stati membri devono assicurare che rispondano solidalmente.

In più, la proposta di direttiva introduce due importanti nuove misure, nella prospettiva della mitigazione dell'onere probatorio del soggetto danneggiato: una sulla divulgazione degli elementi di prova, già disciplinata dalla maggior parte degli Stati membri; l'altra sulla presunzione del carattere difettoso del prodotto o del nesso di causalità tra difetto e danno, già oggetto di "codificazione" negli indirizzi giurisprudenziali, considerati favorevoli all'attore[158].

L'art. 8 stabilisce che gli Stati membri devono attivarsi, affinché il danneggiato, quando ricorrano fatti e prove sufficienti a sostenere la plausibilità della domanda risarcitoria, possa ottenere dal Tribunale un ordine, nei confronti del convenuto, di "divulgare" gli elementi di prova a sua disposizione che siano pertinenti, a condizione che costui si sia rifiutato di esibirli spontaneamente. Tale divulgazione è da intendersi, nel nostro ordinamento, come un ordine di esibizione che dovrà rispondere al principio di proporzionalità, considerando i legittimi interessi di tutte le parti e al principio di necessità, ovverosia nei limiti della richiesta risarcitoria[159].

Si osservi che la fissazione di regole sulla divulgazione di prove rilevanti da parte di coloro che ne dispongano, ai fini dell'accertamento della responsabilità, è importantissimo per i danneggiati, per i quali l'accesso alle informazioni suddette avrà un ruolo determinante nella decisione di agire in giudizio; come pure, in quanto rappresenterà un incentivo per gli operatori economici a rispettare gli obblighi di documentazione delle informazioni pertinenti, stabiliti dalla proposta della c.d. legge sull'intelligenza artificiale[160].

La proposta di direttiva, dopo aver ribadito la necessaria dimostrazione, da parte del danneggiato, del danno, del difetto e del nesso di causalità tra difetto e danno, interviene con l'intento di alleggerire l'onere della prova a carico di quest'ultimo. A tale scopo, l'art. 9, par. 2, prevede una presunzione di difettosità del prodotto, quando il convenuto non abbia adempiuto all'obbligo di divulgazione, di cui all'art. 8; nelle ipotesi in cui il ricorrente provi che il prodotto non è conforme ai requisiti di sicurezza obbligatori, finalizzati alla protezione dalla medesima tipologia di rischio, di cui al danno verificatosi ovvero dimostri che il danno è stato provocato da un evidente malfunzionamento del prodotto, durante il normale utilizzo o in circostanze ordinarie.

---

[157] Cfr. G. PROIETTI, *op.cit*, par. 2.
[158] Progetto di parere, CESE, cit., punto 4.8.
[159] Cfr. G. PROIETTI, *op.cit.*, par. 3.
[160] Cfr. considerando 16 della c.d. *AI Liability Directive*.

L'art. 9, par. 3, prevede una presunzione relativa del nesso di causalità tra il difetto del prodotto e l'evento dannoso, quando è stato accertato che il prodotto è difettoso e che il danno causato è di natura tipicamente coerente con il difetto in questione.

L'art. 9, par. 4, interviene sulla delicata questione delle imponenti difficoltà probatorie (sollevate, in particolar modo, dalla capacità di autoapprendimento dei sistemi di intelligenza artificiale), disponendo che, quando il giudice nazionale ritenga che il ricorrente abbia difficoltà eccessive, nei casi caratterizzati dalla particolare complessità tecnica o scientifica sulla prova del difetto o sul nesso di causalità o su entrambi, sussisterà una loro presunzione. Ciò succede se il danneggiato dimostri, sulla base di prove sufficientemente rilevanti, che il prodotto abbia contribuito a cagionare il danno e che sia probabile che lo stesso fosse difettoso o che il suo carattere difettoso sia una possibile causa del danno o entrambi gli aspetti. Il convenuto avrà, comunque, il diritto di contestare l'esistenza delle difficoltà eccessive o delle probabilità suddette (art. 9, par. 5).

Inoltre, la proposta della Commissione regolamenta le ipotesi, in cui i pregiudizi si verifichino, anni dopo l'acquisto o la messa in circolazione del prodotto nel mercato.

L'art. 10, par. 1, lett. c), include, tra i casi di esonero dalla responsabilità, quello in cui sia probabile che il difetto che abbia prodotto il danno non sussistesse, al momento della immissione del prodotto sul mercato, oppure, nel caso di un distributore, al tempo della sua messa a disposizione ovvero che tale difetto sia sopravvenuto dopo tale momento. In deroga a tale previsione, l'esimente non troverà applicazione, quando la difettosità del prodotto, in costanza di controllo da parte del fabbricante, sia dovuta a una delle seguenti cause: un servizio correlato; il *software*, compresi gli aggiornamenti o i suoi potenziamenti; la mancanza delle migliorie o degli aggiornamenti del *software*, necessari per mantenere la sicurezza (art. 10, par. 2)[161].

Nella proposta di revisione, permane l'esonero da responsabilità per il c.d. rischio da sviluppo (art. 10, par. 1, lett. e)), il quale, contrariamente alla disciplina oggi vigente, non potrà essere oggetto di deroga da parte degli Stati membri.

Pare chiaro che, con tale previsione, la Commissione europea si è posta l'obiettivo di realizzare la piena armonizzazione della disciplina europea del

[161] Al riguardo, particolarmente interessanti sono le riflessioni dottrinali, effettuate già prima della proposta di revisione della direttiva, oggetto di analisi, in relazione all'inapplicabilità ai prodotti digitali dell'esimente del "difetto sopravvenuto". L'Autrice parte dalla precisazione che i beni digitali sono connotati da *openness by design*, ossia sono concepiti per non essere completi di tutto ciò che occorre, al momento della loro messa in circolazione, e per essere soggetti a successive integrazioni ed aggiornamenti delle componenti immateriali e/o per richiedere accesso a dati, sistemi e reti, etc. Di qui, si sostiene che è richiesto un nuovo punto di vista, nel senso che l'*an* ed il *quomodo* delle modificazioni, cui il prodotto è soggetto, vengono in rilievo a partire dal suo stesso *design*, anche allo scopo dell'individuazione di un difetto di progettazione. In aggiunta, il fabbricante mantiene una stretta relazione con il prodotto e con il suo utente, anche a seguito della sua messa in circolazione, nell'ambito di rapporto che può definirsi "di durata", ed è pertanto in grado di acquisire conoscenza dei rischi insiti nello stesso e di gestirli. In questa prospettiva, qualora il danno sia cagionato dagli elementi aggiunti dopo l'immissione in commercio (ad esempio, dal malfunzionamento dell'app scaricata da internet, etc.), ma concepiti come elementi di un unitario prodotto, il produttore non potrà avvalersi dell'esimente del difetto sopravvenuto. Alla stessa stregua, neanche l'imprevedibilità delle azioni della macchina, riscontrabile nei prodotti di *machine learning*, varrebbe ad escludere la responsabilità del produttore, affermando che il difetto sia sopravvenuto. Cfr. R. MONTINARO, *op.cit.*, p. 359 ss.

rischio da sviluppo, superando il dettato della direttiva 85/374/CEE che aveva rimesso agli Stati membri la libertà di scegliere se farlo gravare in capo al consumatore oppure al produttore.

Sicché, in futuro, a seguito del recepimento della direttiva di revisione di quella attualmente vigente, tutte le discipline nazionali europee allocheranno il rischio da sviluppo tecnologico scientifico in capo all'utilizzatore del prodotto, esonerando l'impresa dalla responsabilità, ogni qualvolta il difetto sarà già esistente ed oggettivamente imputabile al produttore, al momento della messa in circolazione del prodotto nel mercato, ma la scienza e le conoscenze tecniche non consentiranno di identificarlo.

Siffatta causa di esclusione della responsabilità del produttore ha un'indiscutibile valenza politica, dal momento che favorisce la circolazione sul mercato di prodotti nuovi e la competitività delle imprese[162].

Da un altro punto di vista, a tali finalità, sottese all'indirizzo legislativo, si contrappone l'esigenza di garantire la sicurezza dei prodotti e di proteggere i consumatori danneggiati.

Si è, a tal proposito, sostenuto che l'eccezione del rischio da sviluppo contrasterebbe con il principio giuridico europeo di precauzione[163], finalizzato ad offrire una tutela anticipata, allorquando non vi sia certezza scientifica sul grado di offensività di una determinata attività d'impresa o di determinati beni o servizi, ma sussista il semplice sospetto che siano potenzialmente pericolosi e che possano provocare un rischio ad interessi "sensibili", quali l'ambiente, la salute umana, la sicurezza degli utenti o dei consumatori [164].

In Italia, ove il legislatore si è allineato all'opzione, accolta da taluni Stati membri, di introdurre l'esimente del rischio da sviluppo[165], si è consolidato l'orientamento giurisprudenziale che ha fatto ricorso al regime di responsabilità contemplato dall'art. 2050 c.c., quale alternativa rispetto alla disciplina della responsabilità del produttore, proprio al fine di assicurare un'adeguata tutela a coloro che subiscano danni, cagionati da rischi che non era possibile prendere in considerazione, al momento in cui la sicurezza del prodotto è stata valutata dal produttore[166].

---

[162] Cfr. D. Caruso, R. Pardolesi, *Per una storia della Direttiva 1985/374/CEE*, in *Danno resp.*, 2012, p. 9 ss.

[163] Cfr. G. Comandé, *La responsabilità civile per danno da prodotto difettoso…assunta con precauzione*, in *Danno e resp.*, 2013, p. 107; F. Santonostaso *Principio di «precauzione» e responsabilità d'impresa: rischio tecnologico e attività pericolosa «per sua natura». Prime riflessioni su un tema di ricerca*, in *Contratto e impresa Europa*, 2005, p. 78. Sul tema, *ex multis*, cfr. D. Cerini, *Responsabilità del produttore e rischio da sviluppo oltre la lettera della Direttiva 85/374/CEE*, in *Dir.econ.ass.,* 1996, p. 29; U. Rizzo, *op.cit.,* p. 380 ss.; G. Visintini, *L'esimente del rischio da sviluppo come criterio della responsabilità del produttore (l'esperienza italiana e tedesca e la direttiva comunitaria*), in *Resp.civ.prev.*, 2004, p. 1267.

[164] Cfr. F. Stella, *Il rischio da ignoto tecnologico e il mito delle discipline,* in Aa.Vv., *Il rischio da ignoto tecnologico*, Milano, 2002, p. 10 ss.; V. F. De Leonardis, *Il principio di precauzione nell'amministrazione del rischio*, Milano, 2005, p. 20; G. Comandé, *L'assicurazione e la responsabilità civile come strumenti e veicoli dell'analisi economica del diritto*, in ID. (a cura di), *Gli strumenti della precauzione: nuovi rischi, assicurazione e responsabilità*, Milano, 2006, p. 23 ss., p. 45 ss

[165] Il legislatore italiano è stato spinto da ragioni di politica del diritto di non creare uno svantaggio competitivo alle imprese italiane e di non scoraggiare le imprese straniere ad investire in Italia. Cfr. V. Buonocore, *L'impresa*, Torino, 2002, p. 302.

[166] Cfr. E. Al Mureden, *La conformità dei prodotti agli standard tecnici tra tutela del consumatore e limiti alla responsabilità del fabbricante*, in *Actualidad Juridica Iberoamericana*, n. 17, 2022, p. 894 s., p. 902 s. Cfr. L. Cabella Pisu, *op.cit.*, p. 645 che parla di una vera e propria casistica parallela. Si è parlato di una «fuga dalla disciplina del danno da prodotto difettoso», con il consolidarsi dell'orientamento che ha fatto ricorso ad altre forme di responsabilità, principalmente alla responsabilità per l'esercizio di attività pericolose, per

Si è parlato, al riguardo, di un "aggiramento" della tenuta tecnica dell'eccezione del rischio da sviluppo, operato dalla giurisprudenza, attraverso una lettura 'precauzionale' delle regole generali di imputazione della responsabilità civile, in modo puntuale della responsabilità per attività pericolose[167].

Per comprendere la portata di tale indirizzo giurisprudenziale, si precisi che l'art. 2050 c.c. viene prevalentemente interpretato ed applicato, "nel diritto vivente" come un'ipotesi di responsabilità oggettiva "per rischio di impresa"[168]. Ciò fa sì che, allorché l'attività venga classificata come pericolosa, la giurisprudenza maggioritaria tenda a non considerare mai raggiunta la prova liberatoria, posta in capo all'esercente l'attività, che esula dalla dimostrazione dell'assenza di colpa e consiste nella dimostrazione di aver adottato tutte le misure idonee a prevenire il danno[169]. Tale prova è, difatti, divenuta talmente rigorosa da essere equiparata al caso fortuito[170].

La regola, di cui all'art. 2050 c.c., è stata ampliamente applicata dalla giurisprudenza, allo scopo di garantire al soggetto danneggiato una posizione di favore, anche allorquando l'attività svolta dal danneggiante risulti poco rappresentativa sul piano del pericolo: le corti hanno invocato la sussistenza dell'elemento della pericolosità anche in casi relativi ad attività non pericolose in sé, ma che divengono tali, in riferimento ai soggetti che siano destinatari delle stesse[171].

---

offrire una risposta alle problematiche correlate ai danni cagionati dalla produzione di massa. Cfr. R. MONTINARO, *op.cit.*, p. 352; ID. *Dubbio scientifico e responsabilità civile*, Milano, 2012, p. 155 ss. Numerosissimi i contributi sul tema. *Ex multis*, cfr. G. COMANDÉ, *L'assicurazione e la responsabilità civile come strumenti e veicoli dell'analisi economica del diritto*, *op.cit.*, p. 23 ss.; F. DEGL'INNOCENTI, *Rischio di impresa e responsabilità civile. La tutela dell'ambiente tra prevenzione e riparazione dei danni*, Firenze University Press, 2013, p. 48 ss.

[167] Cfr. G. COMANDÉ, *La responsabilità civile per danno da prodotto difettoso*, *op.cit.*, p. 109. Per una lettura restrittiva del principio di precauzione, in rapporto all'applicabilità dell'art. 2050 c.c., C. CASTRONOVO, *Sentieri di responsabilità civile europea*, in *Europa dir. priv.*, 2008, p. 787.

[168] Influente dottrina ha sviluppato questa tesi, alla luce di un'interpretazione sistematica delle fattispecie di responsabilità speciali di cui agli artt. 2050-2054 c.c., strettamente correlata al *rischio* di impresa ed alle ripercussioni sul mercato assicurativo, fattori significativi che incidono sulla ripartizione dei danni e dei relativi costi dei consociati. L'Autore ha puntualizzato che la funzione della responsabilità oggettiva non è di punire, bensì di imputare a chiunque il «rischio oggettivamente creato» dalla propria attività, nella misura in cui esso sia esprimibile in costo ed amministrabile dal punto di vista economico, con le conoscenze e con i mezzi di previdenza che un buon amministratore abbia a propria disposizione. Cfr. P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, pp. 193 ss. La dottrina e la giurisprudenza prevalente e più recente si sono discostate dall'indirizzo più risalente che qualificava la responsabilità per l'esercizio delle attività pericolose come responsabilità per colpa, pur se "aggravata", con semplificazione dell'onere probatorio a favore del danneggiato; per configurarla, differentemente, come responsabilità oggettiva. Tra le voci più autorevoli che hanno configurato il regime di cui all'art. 2050 c.c. come responsabilità per colpa « aggravata », si v. A. DE CUPIS, *Il danno. Teoria generale della responsabilità civile*, Milano, 1979, p. 88 ss.; P. FORCHIELLI, *La colpa lievissima*, in *Riv.dir.civ.*, 1963, I, p. 202; E. PARAGLIA, *Appunti in tema di responsabilità da esercizio di attività pericolose*, in *Diritto e pratica nell'assicurazione*, 1975, p. 645. Fautori della ricostruzione della responsabilità oggettiva sono M. FRANZONI, *Responsabilità per l'esercizio di attività pericolose*, in G. ALPA, M. Bessone (diretta da), *La responsabilità civile. Una rassegna di dottrina e giurisprudenza*, Torino, 1987, p. 459 ss.; P.G. MONATERI, *La responsabilità civile*, in R. SACCO (diretto da), *Trattato di diritto civile*, Torino, 1998, p. 674 ss.

[169] Cfr. E. AL MUREDEN, *I danni da uso del cellulare tra tutela previdenziale e limiti della responsabilità del produttore*, in *Resp.civ.prev.*, 2010, p. 1392 ss., par. 4 (consultabile *online* sul sito dejure.it), il quale richiama C. CASTRONOVO, *La nuova responsabilità civile*, III es., Milano, 2006, p. 302, il quale afferma che la giurisprudenza «non si accontenta mai».

[170] Cfr. M. FRANZONI, *Responsabilità per l'esercizio di attività pericolose*, op.cit., p. 459.

[171] Come nel caso di attività di maneggio di cavalli, ove si individua il pericolo nella circostanza che i soggetti siano inesperti; Cass., 19 giugno 2008, n. 16637, in *Foro it.*, rep. 2009. Sul punto, cfr. A. FUSARO, *Attività pericolose e dintorni*, in *Riv.dir.civ.* 2013, p. 1339. A livello legislativo, la portata applicativa della norma è stata

Durevole è, poi, il ricorso al regime della responsabilità per attività pericolose, al fine di assicurare una protezione idonea a coloro che subiscano danni da prodotti qualificabili come 'conformi', alla luce della disciplina sulla sicurezza dei prodotti e delle norme tecniche armonizzate, ma la cui pericolosità sia conosciuta, al momento dell'ideazione dello *standard* legislativo e sia deliberatamente inclusa nell'ambito dei rischi correlati, in modo ragionevole, all'uso normale del prodotto. L'applicazione dell'art. 2050 c.c. impedisce al produttore di escludere la propria responsabilità, affermando il carattere non difettoso del prodotto, dedotto dalla conformità dello stesso agli *standard* previsti per la sua immissione nel mercato. L'impiego del regime della responsabilità per attività pericolosa ha, perciò, limitato il rigore dell'impostazione, secondo la quale, una volta approvata la conformità del prodotto agli *standard* legislativi che ne governano la sicurezza, non resterebbe spazio per configurare la responsabilità del fabbricante per i danni da questo cagionati[172]. In tale prospettiva, sono stati considerati pericolosi prodotti quali le bombole del gas [173], i derivati del tabacco [174], i fuochi di artificio e principalmente i farmaci [175] ed è stata loro applicata la disciplina dettata dall'art. 2050 c.c.

L'interpretazione della norma in tali termini ha permesso di attribuire rilevanza anche ai profili di dannosità e di pericolosità 'potenziale' dei prodotti che potrebbero rientrare nei rischi che il produttore non avrebbe potuto prendere in considerazione, al momento in cui la sicurezza del prodotto è stata valutata (c.d. rischio da sviluppo)[176]. Segnatamente l'applicazione dell'art. 2050 c.c. impedisce al produttore di liberarsi dalla propria responsabilità, richiamando l'esimente del rischio da sviluppo[177], dando, così, attuazione al principio di precauzione.

Ordunque, alla luce delle osservazioni svolte, ci si è domandati se il consumatore danneggiato possa scegliere tra la tutela extracontrattuale generale e la tutela extracontrattuale speciale ed invocare il regime della responsabilità per l'esercizio delle attività pericolose, in quanto più favorevole, per lo stesso, dal punto di vista processuale (e più gravoso, viceversa, per il produttore danneggiante), rispetto alla disciplina della responsabilità per danno da prodotto difettoso[178].

---

ampliata, in particolare, dall'art. 15, d.lg. 30 giugno 2003, n. 196 (Codice in materia di trattamento dei dati personali), secondo cui "chiunque cagioni danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile".

[172] Sul punto, cfr. E. AL MUREDEN, *La conformità dei prodotti agli standard tecnici tra tutela del consumatore e limiti alla responsabilità del fabbricante*, *op.cit.*, p. 902.

[173] Cfr. Cass., 26 luglio 2012, n. 13214, in *Giustizia civile. Massimario annotato della Cassazione*, 2012, p. 967.

[174] Tra le numerose pronunce, cfr. Cass., 11 ottobre 2018, n. 25161*, Giur.it.*, 2019, p. 1319; Cass., 21 gennaio 2020, n. 1165, dejure.it.

[175] Per il caso di danni causati da un farmaco antiobesità, cfr. Trib. Roma, 20 aprile 2002, in *Resp.civ.*, 2002, 1107. Sul tema, cfr. A. QUERCI, *Biotecnologie e scienze della vita nelle recenti normative di origine comunitaria: le nuove frontiere della responsabilità civile*, ivi, 2010, 219 s., 231.

[176] Cfr. E. AL MUREDEN, *La conformità dei prodotti agli standard tecnici tra tutela del consumatore e limiti alla responsabilità del fabbricante*, op.cit., p. 902, s.; ID., *I danni da uso del cellulare tra tutela previdenziale e limiti della responsabilità del produttore, op.cit.*, par. 4.

[177] Cfr. E. AL MUREDEN, *op.loc.ult.cit.*; F. CAFAGGI, *La responsabilità dell'impresa per i prodotti difettosi*, in N. LIPARI (a cura di), *Trattato di diritto privato europeo*, Padova, 2003, p. 562 ss.

[178] Sul punto e per le considerazioni che seguono, cfr. R. MONTINARO, *Responsabilità del produttore di farmaci, art. 2050 c.c. e gestione precauzionale del rischio*, in *Resp.civ.*, 2019, p. 1587 ss., par. 2, consultabile online sul sito *dejure.it*

La giurisprudenza ha ammesso la scelta tra tali due regimi, quand'anche ricorrano i presupposti per applicare la disciplina di derivazione europea, ponendo, a fondamento del ragionamento, la circostanza che l'art. 127 c. cons., nel trasporre l'art. 13 della direttiva 85/374/CEE, statuisce che le disposizioni sulla responsabilità da prodotto difettoso «non escludono né limitano i diritti che siano attribuiti al danneggiato da altre leggi»[179].

La letteratura giuridica ha affermato che tale ricostruzione, di fatto, vanifica le finalità armonizzatrici della direttiva sulla responsabilità del produttore e che l'art. 13 deve essere interpretato nel senso che non può ammettersi il cumulo della tutela extracontrattuale, predisposta dalla direttiva e di quella prevista dall'art. 2050 c.c., poiché hanno, in sostanza, la medesima natura extracontrattuale e lo stesso fondamento oggettivo. Si può, per contro, consentire il cumulo tra azione extra-contrattuale, ai sensi del codice del consumo, e l'azione contrattuale, quale quella della garanzia per vizi, nei casi in cui tra produttore e danneggiato esista anche un rapporto contrattuale, per esempio la compravendita[180].

L'indirizzo ermeneutico descritto è stato altresì criticato dalla Corte di Giustizia dell'Unione europea che, in una pronuncia non recente, ha assunto una posizione restrittiva riguardo al rapporto tra la disciplina nazionale di recepimento della direttiva e le normative nazionali di fonte diversa, stabilendo che i diritti riconosciuti al danneggiato, in virtù di una regolamentazione di carattere generale che abbiano lo stesso fondamento della direttiva, possono essere limitati oppure esclusi in ragione dell'applicazione di quest'ultima, frutto di un delicato contemperamento degli interessi del produttore e del consumatore[181].

La Corte di Giustizia ha costantemente condannato ogni «disallineamento», realizzato da parte della giurisprudenza nazionale, ponendo in evidenza che esso finisce col rappresentare «un *vulnus* al valore dell'armonizzazione»[182].

Concludendo, la disciplina di derivazione europea non potrà essere disapplicata, al solo fine di realizzare una tutela rafforzata del soggetto danneggiato, invocando il regime della responsabilità per attività pericolosa che non prevede l'esimente del rischio da sviluppo che, come visto, favorisce la posizione del produttore[183].

Ciò detto, si puntualizzi che la Corte di Giustizia dell'Unione Europea ha interpretato in modo restrittivo il rischio da sviluppo, precisando che, nel determinare l'ambito di estensione delle conoscenze scientifiche e tecniche previste dalla direttiva, si dovrà escludere la responsabilità del produttore

---

[179] Tra le numerose pronunce, cfr. Cass. civ., 27 luglio 1991, n. 8395, in *Giur. it.*, 1992, I, 1331, con nota di A. BARENGHI, *In tema di farmaci difettosi*; Cass. civ., 20 luglio 1993, n. 8069, in *Resp.civ.*, 1994, p. 61, con nota di A. BUSATO, *I danni da emoderivati: le diverse forme di tutela*, in *Foro it.*, 1994, I, 455; Cass. civ., 1° febbraio 1995, n. 1138, *ivi*, 1996, 144, con nota di S. BASTIANON, *La Cassazione, il « Trilergan » e la responsabilità per danni da emoderivati infetti.*

[180] Cfr. L. CABELLA PISU, *op.cit.*, p. 621.

[181] Cfr. Corte giust. CE, 25 aprile 2002, causa C-183/00, in *Foro it.,* 2002, IV, 294, con nota di A. PALMIERI, R. PARDOLESI, *Difetti del prodotto e del diritto privato europeo*. Sul punto cfr. G. PONZANELLI*, Armonizzazione del diritto v. protezione del consumatore: il caso della responsabilità del produttore,* in *Danno e resp.*, 2002, 728 s. Sul punto e per le riflessioni che seguono, cfr. R. MONTINARO, *op.ult.cit.*, par. 2.

[182] Cfr. E. AL MUREDEN, *La conformità dei prodotti agli standard tecnici tra tutela del consumatore e limiti alla responsabilità del fabbricante*, *op.cit*, p. 903.

[183] Cfr. L. CABELLA PISU, *op.cit*, p. 631.

soltanto quando, al momento della messa in circolazione del prodotto, il livello 'più alto' delle conoscenze della scienza e della tecnica, "accessibili" in qualsiasi settore produttivo, non consentiva di scoprire l'esistenza del difetto del prodotto[184].

In tale prospettiva, la previsione del rischio da sviluppo deve essere interpretata nel senso che, da un lato, al produttore devono essere imputati tutti i rischi di danno che siano messi in luce dalle più avanzate conoscenze tecnico-scientifiche, sempre che siano accessibili; dall'altro lato, sul danneggiato devono gravare unicamente quei rischi che ricadono al di fuori dello scibile umano[185].

Avendo precipuo riguardo ai prodotti digitali, la nozione di conoscenza oggettiva, disponibile al tempo della messa in circolazione nel mercato degli stessi, assume rilievo, nella misura in cui, di certo, essa influisce sulla valutazione del comportamento del produttore e/o dell'ideatore dell'algoritmo, in riferimento alle applicazioni di intelligenza artificiale. Si terrà conto della circostanza che tali soggetti non hanno saputo né individuare, né prevedere gli elementi di conoscenza scientifica e tecnica che avrebbero permesso loro di valutare il prodotto come non sicuro, dato che propriamente si sarebbe evoluto in una determinata direzione, e che, di conseguenza, li avrebbero spinti ad adottare tutte le misure di precauzione occorrenti per impedire, o quantomeno, limitare il danno[186].

3.2.3.(segue) La proposta c.d. AI Liability Directive.

La proposta c.d. *AI Liability Directive* statuisce l'applicabilità della disciplina alle azioni civili di responsabilità extracontrattuale intentate, nell'ambito di regimi di responsabilità per colpa, da parte di coloro che abbiano subito un danno da un sistema digitale, determinato da un'azione o un'omissione intenzionalmente lesiva o colposa di determinati soggetti coinvolti nella "catena di valore" del sistema.

La proposta rientra, come gli altri provvedimenti *in fieri* esaminati, nella strategia europea di promuovere la diffusione di un'intelligenza artificiale affidabile. Si prefigge, a tal uopo, di ridurre l'incertezza giuridica per le imprese che la sviluppano o la utilizzano, in relazione alla possibile esposizione alla responsabilità, e di garantire efficaci strumenti di tutela ai soggetti danneggiati.

La Commissione europea parte, anzitutto, dalla considerazione che le norme nazionali, vigenti in materia di responsabilità, in particolare per colpa, non sono idonee a gestire le azioni per i danni cagionati da prodotti e servizi basati sull'intelligenza artificiale, considerato che la complessità, l'autonomia e

---

[184] Cfr. Corte CE, 29 maggio 1997, C-300/95, in *Foro it.*, 1997, IV, c. 387, con nota di G. PONZANELLI, *Regno Unito, Corte di Giustizia ed eccezione dello «state of art»*.

[185] Cfr. R. MONTINARO, *Responsabilità da prodotto difettoso, op.cit.,* p. 354. Si sostiene che l'indubbia valenza politica del rischio da sviluppo ha condotto a ricomprendere nel suo ambito unicamente i rischi assolutamente imprevedibili sconosciuti e non i difetti, la cui potenziale presenza sia conosciuta o conoscibile, alla luce dalle più avanzate conoscenze tecnico-scientifiche, ma non siano eliminabili nel corso dei processi produttivi attuali. Cfr. F. SANTONOSTASO, *op.cit.*, p. 99, il quale richiama U. CARNEVALI, *Responsabilità del produttore*, in *Enc.dir., Aggiornamento*, II, 1998, p. 946; V. BUONOCORE, *OP.CIT.* p. 303; A. STOPPA, *Responsabilità del produttore*, in *Dig.disc.priv., sez.civ.*, XVIII, Torino, 1998, p. 135.

[186] Sul punto, cfr. G. CAPILLI, *op.cit.*, p. 481.

l'opacità che li caratterizza possono rendere difficile o eccessivamente costoso, da parte del ricorrente, identificare la persona responsabile e dimostrare che sussistono i presupposti ai fini dell'esito positivo di un'azione di responsabilità.

La Commissione valuta altresì che le strategie nazionali, relative al contesto digitale, rivelano che numerosi Stati membri stanno valutando di predisporre un'azione legislativa in materia di responsabilità civile per l'intelligenza artificiale o che la stanno pianificando concretamente. Si prevede che, qualora non vi fosse un intervento da parte dell'Unione Europea, gli Stati membri adegueranno le norme interne in materia di responsabilità civile alle nuove sfide poste dall'intelligenza artificiale. La c.d. *AI Liability Directive* è, dunque, finalizzata a prevenire la frammentazione che potrebbe provenire da adeguamenti specifici all'intelligenza artificiale, da parte delle norme nazionali in materia di responsabilità civile.

A tale scopo**,** la Commissione ha valutato che la direttiva è lo strumento normativo più idoneo per la proposta in esame, dato che garantisce l'effetto di armonizzazione e la certezza del diritto auspicati, prevedendo, al contempo, la flessibilità per consentire agli Stati membri, nel recepimento nazionale, di integrare le misure armonizzate[187].

In linea con il livello di armonizzazione minima prescelto, i legislatori nazionali potranno adottare o mantenere le normative interne più favorevoli, rispetto alla disciplina dettata dalla proposta di direttiva, purché siano compatibili con il diritto dell'Unione europea (art. 1, n. 4).

La proposta della direttiva presenta la peculiarità di dar luogo ad un'armonizzazione *mirata* delle norme degli Stati membri, in materia di responsabilità civile extracontrattuale per colpa, statuendo disposizioni solamente in materia dell'onere della prova. Non interviene sugli aspetti generali della responsabilità civile, quali la definizione di colpa, di causalità, i diversi tipi di danno che determinano le richieste di risarcimento, la distribuzione della responsabilità sugli autori del medesimo illecito, il concorso di colpa, la quantificazione dei danni e i termini di prescrizione[188].

La Commissione europea, in considerazione della circostanza che i soggetti danneggiati potrebbero dover sostenere costi iniziali molto elevati e affrontare procedimenti giudiziari molto più lunghi rispetto a quanto succede nei casi che non riguardino l'intelligenza artificiale, con la conseguenza che costoro sarebbero dissuasi dall'agire in giudizio, introduce dei meccanismi di alleggerimento probatorio, al fine gestire tali difficoltà, nonché per completare il quadro giuridico delineato con la proposta della c.d. legge sull'intelligenza artificiale[189].

Precisamente la proposta di direttiva prevede due strumenti giuridici di facilitazione dell'onere della prova degli attori, nelle azioni che possono essere basate sul diritto nazionale o sulle altre normative europee.

In primis, è riconosciuto il diritto del soggetto danneggiato di accedere a quegli elementi che possano costituire una prova, nei casi in cui si tratti di un

---

[187] Relazione della Commissione alla proposta, punto 2.

[188] Cfr. G.T. ELMI, S. MARCHIAFAVA, *op.loc.ult.cit.*

[189] Cfr. A NERI, *Verso un nuovo regime della responsabilità da intelligenza artificiale: presunzioni e diritto di accesso alle prove in favore dei soggetti danneggiati*, consultabile *online* sul sito www.wfw.com/articles, 22 dicembre 2022

sistema di intelligenza artificiale "ad alto rischio", come definiti dalla proposta della c.d. legge sull'intelligenza artificiale[190]. L'art. 3 dispone che gli Stati membri debbano predisporre un meccanismo procedurale, per mezzo del quale l'autorità giudiziaria possa ordinare ad un "fornitore", come pure ad un soggetto che soggiaccia agli stessi obblighi di quest'ultimo, o ad un "utente" di esibire quelle prove pertinenti che siano a sua disposizione, relative allo specifico sistema "ad alto rischio". Specularmente a quanto stabilito dalla proposta di direttiva sulla responsabilità per danno da prodotto difettoso, il ricorrente, al fine di ottenere tale ordine, deve presentare, a sostegno della richiesta, fatti e prove sufficienti a sostenere l'ammissibilità della domanda di risarcimento del danno; in più, l'ordine dell'autorità sarà subordinato alla circostanze che uno dei soggetti menzionati si sia rifiutato di esibire gli elementi di prova spontaneamente e che si reputi che il sistema intelligente abbia causato un danno.

L'ordine di esibizione dovrà rispondere ai principi di necessità e di proporzionalità. Quanto a quest'ultimo, l'art. 3, par. 4, nell'imporre ai giudici nazionali di tenere in considerazione gli interessi legittimi di tutte le parti, si riferisce alla tutela dei segreti commerciali, ai sensi della direttiva UE 2016/943 (direttiva c.d. "*trade secret*") ed alla normativa nazionale di recepimento. Si lascia, a tal punto, alle corti di merito l'arduo compito di bilanciare l'interesse sotteso alla richiesta della divulgazione/conservazione degli elementi di prova e l'esigenza di tutela del segreto commerciale[191].

Gli Stati membri dovranno introdurre idonei sistemi di impugnazione delle decisioni relative alle richieste di divulgazione.

Qualora il convenuto non rispetti l'ordine del giudice nazionale di esibire e conservare le prove, secondo quanto previsto dall'art. 3, paragrafi 1 e 2, vi sarà una presunzione di inosservanza di un obbligo di diligenza.

In secondo luogo, la proposta di direttiva elabora presunzioni confutabili, relative all'onere della prova del nesso di causalità[192].

L'art. 4 stabilisce che gli organi giurisdizionali presumono l'esistenza del nesso di causalità tra la colpa del convenuto e l'*output* prodotto da un sistema intelligente o la mancata generazione di un *output* da parte del sistema che abbia cagionato il danno, quando ricorrano le condizioni elencate dalle lett. a), b) e c): la dimostrazione, da parte del ricorrente, dell'inosservanza colposa, da parte del convenuto o di una persona della cui condotta costui è responsabile, degli obblighi di diligenza, previsti dalla disciplina nazionale o europea (quale anche la proposta della c.d. legge sull'intelligenza artificiale), posti a prevenire il danno verificatosi (lett. a)); la ragionevole probabilità, sulla base delle

---

[190] Per il commento all'art. 3 della proposta di direttiva, cfr. G. PROIETTI, *Sistemi di intelligenza artificiale e responsabilità: la proposta di AI liability Directive*, consultabile *online* sul sito www.dirittobancario.it , 6 ottobre 2022, p. 3.

[191] Cfr. G. LUSARDI, *Danni causati dall'intelligenza artificiale, chi paga? Cosa prevede la proposta di direttiva UE,* par. 4, consultabile *online* sul sito www.agendadigitale, 9 dicembre 2022,

[192] Per l'analisi dell'art. 4, cfr. il commento all'art. 4, contenuto nella proposta di direttiva, "*Presumption of causal link in the case of fault* (art. 4)", consultabile *online* sul sito https://ec.europa.eu/info/sites/default/files/1_1_197605_prop_dir_ai_en.pdf, pp.13 s.; G. LUSARDI, *op.cit.,* par. 3; G. PROIETTI, *op.ult.cit.*, p. 4, s.

circostanze del caso concreto, che tale condotta colposa abbia influito sull'*output* creato dal sistema o sulla sua incapacità di produrlo; la prova, fornita dal ricorrente, che l'*output* compiuto dal sistema digitale o la sua incapacità di elaborarlo abbia provocato il danno.

Per i sistemi intelligenti "ad alto rischio", l'art. 4 statuisce un regime differenziato, nel senso che, nell'ambito delle azioni promosse contro i "fornitori" o gli "utenti", la presunzione di causalità è limitata al caso del mancato rispetto degli obblighi previsti dalla proposta di regolamento, rispettivamente richiamati, per i primi, dall'art. 4, par. 2 e, per i secondi, dall'art. 4, par. 3.

Per tale categoria di sistemi intelligenti, sussiste un'eccezione alla presunzione di causalità, laddove il convenuto dimostri che all'attore siano ragionevolmente accessibili le prove e che abbia le competenze idonee a provare il nesso causale.

Quando la richiesta risarcitoria riguardi un sistema "non ad alto rischio" (che non è soggetto ai requisiti obbligatori della proposta della c.d. legge sull'intelligenza artificiale), la presunzione di causalità si applicherà, solo quando la prova del nesso di causalità sia ritenuta eccessivamente complessa per l'attore.

Per i casi in cui il convenuto usi il sistema intelligente nell'ambito di un'attività personale non professionale, la presunzione di causalità si applicherà unicamente quando costui abbia interferito materialmente con le sue condizioni di funzionamento oppure quando fosse tenuto ed in grado di determinarle ed abbia omesso di farlo. Tale previsione esprime il bisogno di contemperare gli interessi delle persone lese e quelli degli utenti non professionali, escludendo l'applicazione della presunzione di causalità, nelle ipotesi in cui tali soggetti non aggiungano rischi con il loro comportamento.

L'articolo 4, par. 7, dispone che il convenuto abbia il diritto di confutare la presunzione di causalità, di cui all'articolo 4, par. 1.

Un riesame dell'applicazione della direttiva, da parte della Commissione europea, è previsto nel termine di cinque anni, allo scopo di presentare una relazione al Parlamento europeo e al Consiglio, nonché al Comitato economico e sociale europeo (art. 5).

Conclusioni.

In chiusura, può osservarsi che il contesto normativo che disciplinerà i sistemi di intelligenza artificiale si sta muovendo nella direzione della prevenzione dei rischi, prevalentemente in riferimento ai sistemi "ad alto rischio", accostando, alla regolamentazione della sicurezza, la normativa sulla responsabilità civile improntata ad un *favor* delle vittime dei danni cagionati da 'tutti' i sistemi digitali[193].

Di fatto, da un lato, la mancata adozione, da parte delle categorie degli operatori economici obbligati, delle misure tecniche ed organizzative di sicurezza, previste dalla proposta della c.d. legge dell'intelligenza artificiale,

[193] Cfr. ID. *op.loc.ult.cit.*

condurrà all'irrogazione di sanzioni amministrative; dall'altro lato, la violazione degli obblighi di conformità ai parametri di sicurezza suddetti determinerà una presunzione di difettosità del *digital device* (ai sensi della proposta di revisione della direttiva sulla responsabilità per danno da prodotto difettoso), oltre che la responsabilità aggravata per colpa presunta del "fornitore" o dell'"utente" e, di conseguenza, l'obbligo di risarcimento del danno (ai sensi della proposta c.d. *AI Liability Directive*)[194].

In realtà, però, la violazione di *standard* di sicurezza prefissati non comporterà automaticamente la "difettosità" del sistema intelligente[195]; così come, l'adesione agli stessi non implicherà necessariamente l'esonero dalla responsabilità in caso di danni, perché il sistema conforme potrebbe essere "difettoso"[196]. In altri termini, il rispetto di certi *standard* denoterà unicamente la conformità ad un astratto modello regolamentare, fissato sulla base di criteri statici e non dinamici, ma ciò non escluderà che il sistema digitale provochi danni a terzi, in sede di utilizzo da parte del fruitore finale[197].

Ad ogni modo, senza dubbio, la predisposizione, accanto alla normativa civilistica della responsabilità civile, della regolamentazione pubblicistica ha il merito di disegnare un panorama normativo, in cui gli strumenti di tutela successiva convergono con quelli di tutela preventiva, fondati sulla valutazione dei rischi e sulla loro limitazione, attraverso l'uso di una serie di misure tecniche predeterminate ed oggetto di costante monitoraggio e aggiornamento, in conformità al principio di precauzione[198].

Deve, tuttavia, muoversi una critica alle Istituzioni europee per il cambio di rotta, nella disciplina della responsabilità civile extracontrattuale, al di fuori del regime della responsabilità per danno da prodotto difettoso.

La c.d. *AI Liability Directive* non si pone nel solco della regolamentazione dettata dalla proposta di regolamento, il cui contenuto è stato raccomandato alla Commissione dal Parlamento europeo, nella Risoluzione sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale.

In primis, a differenza della Commissione che ha optato, nella proposta di direttiva, per l'approccio dell'armonizzazione minima, diversamente il Parlamento europeo aveva prescelto lo strumento normativo del regolamento che avrebbe garantito uniformità, attraverso l'introduzione di regimi di responsabilità pienamente armonizzati.

---

[194] Analogamente a quanto previsto dal GDPR (artt. 83 e 84 *GDPR*), secondo il quale alla mancata adozione, da parte del titolare del trattamento, delle misure impostegli, conseguono ingenti sanzioni amministrative e la violazione degli obblighi determina la responsabilità aggravata per colpa presunta del titolare (e del responsabile) del trattamento e, di conseguenza, l'obbligo di risarcimento del danno, *ex* art. 82. Sul punto, cfr. M. GAMBINI, *op.cit.,* p. 322.

[195] Cfr. U. RUFFOLO, *La responsabilità da artificial intelligence, algoritmo e smart product: per i fondamenti di un diritto dell'intelligenza artificiale self-learning*, in ID. (a cura di) *Intelligenza artificiale. Il diritto, i diritti, l'etica*, op.cit., p. 144.

[196] Cfr. U. RUFFOLO, E. AL MUREDEN, *Authonomous vehicles e responsabilità nel nostro sistema e in quello statunitense*, in *Giur.it.*, 2019, pp. 1709; Cfr. A. FUSARO, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuov.giur.comm.*, 2020, pp. 1353,1348.

[197] Cfr. A. AMIDEI, *Intelligenza artificiale e product liability*, *op.cit.*, p. 1722

[198] Cfr. R. CARLEO, *op.cit.*, p. 361. La dottrina sottolinea che tra le cc.dd. "*issues of permittance*" e le "*issues of liability*", sussiste un rapporto di complementarietà e non di reciproca alternatività. Cfr. M. BUTTEN, A. DE STREEL, M. PEITZ, *Eu liability rules for the age of artificial intelligence*, in *Centre of regulation in Europe*, 2021, p. 45.

In secondo luogo, la proposta di regolamento prevedeva un regime di responsabilità oggettiva per gli operatori di sistemi intelligenti "ad alto rischio", regime che, come ampiamente argomentato dall'*Expert Group on liability and new technologies*, risulta essere il più idoneo a garantire la gestione del rischio e ad assicurare un'allocazione dei danni giusta ed efficiente.

Ancora, la proposta di direttiva, incentrandosi esclusivamente sulle difficoltà probatorie, con l'obiettivo di predisporre un assetto unitario in ambito europeo, presenta talune criticità, tra le quali: la difficoltà di identificare, nella catena della produzione e dell'utilizzo di un sistema intelligente, il soggetto responsabile; il richiamo a nozioni di carattere nazionale, come quello della colpa; le differenze che possono sussistere, negli Stati membri, in relazione alla nozione di danno risarcibile e, non da ultimo, il ruolo degli organi giurisdizionali nazionali, che potrebbero creare disomogeneità nel mercato unitario[199].

Alla luce di quanto detto, è auspicabile che l'Unione Europea formuli un nuovo e generale modello di responsabilità civile per i danni cagionati dalle applicazioni di intelligenza artificiale, che vada oltre l'impostazione dell'armonizzazione minima della proposta di direttiva e superi i limiti della proposta di regolamento, raccomandata dal Parlamento europeo[200]; offrendo, per di più, una risposta operativa all'opportunità di introdurre azioni collettive, soprattutto quando gli incidenti algoritmici provochino danni di valore ridotto ad una pluralità di soggetti, e al problema di come finanziare le controversie e alla questione del luogo in cui radicare la causa, quando vi siano conflitti transfrontalieri[201].

Solo così, si potranno realmente proteggere i diritti fondamentali ed i valori europei.

Infine, voglia riflettersi sulla tecnica legislativa adottata dalle Istituzioni europee.

Si premetta che, negli ultimi anni, si è assistito ad un profluvio di iniziative legislative in materia di intelligenza artificiale. Tale circostanza ha indotto la dottrina ad obiettare che il continuo interventismo, volto a "plasmare il futuro digitale europeo", starebbe, effettivamente, manifestando «un eccesso di protagonismo normativo», in materia di regolazione del mercato digitale[202].

In aggiunta, tale settore, «stretto in una morsa giuridica», rischierebbe di essere compresso e di non riuscire ad esprimere le proprie potenzialità[203]. Ci si dovrebbe avvalere dei vantaggi e delle opportunità offerte dalle intelligenze artificiali che rappresentano un "volano" per lo sviluppo economico, scientifico e sociale globale, benché provvedendo a minimizzare i rischi e le criticità che le stesse presentano[204].

La dottrina si è posta il quesito se sia davvero conveniente adottare regole puntuali e specifiche, che rischino di essere superate, in breve tempo, dal

---

[199] Cfr. A NERI, *op.loc.ult.cit.*

[200] Per tali riflessioni, cfr. G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale, op.cit.*, par.4.

[201] Cfr. M. INFANTINO, *op.cit.*, par. 6.

[202] Cfr. autorevolmente T.E. FROSINI, *Dma, Dsa e intelligenza artificiale. L'Europa non stritoli l'innovazione,* consultabile *online* sul sito https://formiche.net/2021/10/dma-dsa-intelligenza-artificiale-frosini/

[203] Cfr. ID., *La privacy nell'era dell'intelligenza artificiale*, consultabile *online* sul sito *DPCE Online,* 2022, 1, vol. 5, p. 281.

[204] Cfr. ID., *L'orizzonte giuridico dell'intelligenza artificiale*, in *BioLaw Journal, Rivista del Biodiritto*, 1/2022, p. 160, consultabile online sul sito https://www.biodiritto.org

progresso tecnologico talmente veloce e mutevole da farle divenire facilmente obsolete[205].

La regolamentazione della materia si dovrebbe improntare sul principio della neutralità tecnologica, ormai affermato in ambito internazionale, in forza del quale il diritto dovrebbe rimanere neutro, rispetto alla tecnologia: la norma giuridica non si dovrebbe riferire ad un livello di sicurezza predeterminato oppure ad una tecnologia peculiare; all'opposto, si dovrebbe limitare a prevedere l'obiettivo da raggiungere, senza individuare le modalità tecniche per la sua realizzazione[206].

In tale direzione, risultano sempre più necessarie «una tavola di principi valoriali» ed una diffusa consapevolezza culturale ed "etica" che possano trovare attuazione sia nella prassi, sia nelle pronunce giudiziali. A fronte dell'imprevedibilità dello sviluppo tecnologico, apparirebbe irragionevole pretendere «un diritto calcolabile» e "perdente" ogni atteggiamento formalistico che escluda il ricorso ai principi e ai valori sui quali la civiltà giuridica si è venuta man mano formandosi[207].

Di qui, l'esigenza di comprendere come, nel contesto tecnologico in continua evoluzione, sia nodale l'impiego di una tecnica legislativa che si serva, più che di "norme ipertrofiche" di dettaglio[208]che impongono dei veri e propri «fardelli burocratici»[209], distintamente di principi, che permettano l'interpretazione che sia idonea alla risoluzione del caso concreto, tenendo conto dell'ambito di riferimento[210].

---

[205] Cfr. T.E. FROSINI, *Dma, Dsa, op.loc.ult.cit.;* P. PERLINGIERI, *Relazione conclusiva*, in *Il trattamento algoritmico, op.cit.,* p. 388 ss.

[206] Cfr. G. FINOCCHIARO, *La proposta di regolamento*, *op.cit.*, par. 1, nota 11, la quale precisa che tale principio si è affermato nell'elaborazione dell'*UNCITRAL*, già nel *Model Law or Electronic Commerce* del 1996.

[207] Per tale ricostruzione, cfr. P. PERLINGIERI, *Relazione conclusiva*, in *Il trattamento algoritmico dei dati tra etica, diritto ed economia, op.cit.,* p. 388 ss.

[208] La locuzione è di T.E. FROSINI, *L'orizzonte giuridico*, *op.cit.,* p. 161.

[209] L'espressione è di G. FINOCCHIARO, *La proposta di regolamento*, *op.loc.ult.cit.*

[210] Cfr. autorevolmente P. PERLINGIERI, *Note sul «potenziamento cognitivo»*, in *Tecnologie e diritto*, 2021, p. 214, il quale rimarca che spetterebbe un ruolo determinante alle autorità indipendenti nazionali e sovranazionali.

Mignozzi A, 'Digital divide ed enti del terzo settore nella società del terzo millennio' (2022) 2 EJPLT, 67-83.
DOI: https://doi.org/10.57230/EJPLT222AM

EJPLT
ISSN 2704-8012



Digital divide ed enti del terzo settore nella società del terzo millennio.

Digital divide and third sector entities in the third millennium society.

ALESSIA MIGNOZZI
Associate Professor of Private Law
Università della Campania Luigi Vanvitelli

Abstract

L'inarrestabile evoluzione tecnologica comporta l'accesso a fonti di informazione e comunicazione assai rilevanti non solo per lo sviluppo economico e sociale, ma anche per l'esplicazione della personalità dell'individuo. Per ragioni socio-economiche e di poca dimestichezza con i device, gran parte della popolazione (costituita, soprattutto, da donne, anziani, immigrati e disabili) non può beneficiare dell'uso di tali tecnologie informatiche, vedendosi preclusa la possibilità di esercitare alcuni diritti individuali fondamentali. Di qui l'importante ruolo delle organizzazioni aventi natura ideale, quali gli enti del terzo settore che, in virtù del principio di sussidiarietà orizzontale, possono contribuire ad attenuare il digital divide e a realizzare in concreto i nuovi diritti digitali, preservando la persona nel mercato digitale.

The unstoppable technological evolution entails access to sources of information and communication that are very relevant not only for economic and social development, but also for the fulfilment of the individual's personality. For socio-economic reasons and due to unfamiliarity with devices, a large part of the population (mainly women, the elderly, immigrants and the disabled) cannot benefit from the use of these information technologies, seeing themselves precluded from exercising certain fundamental individual rights. Hence the important role of organisations of an ideal nature, such as third-sector entities, which, by virtue of the principle of horizontal subsidiarity, can help to alleviate the digital divide and make the new digital rights a reality, preserving the individual in the digital marketplace.

© The author(s) 2022, 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: Europa digitale; digital divide; diritti della persona; ETS.

Summary: Introduzione: Crisi socio-economica ed Europa digitale. – 1. Nuove tecnologie, *social network* e diritti della persona. – 2. Emersione del problema del *digital divide* e rilevanza degli studi di settore. – 3. Le soluzioni del legislatore italiano prima e dopo la pandemia da covid-19. La Dichiarazione europea dei principi e dei diritti digitali. – Conclusioni: Gli ETS quale strumento concreto del diritto privato per il superamento del *digital divide* e la promozione della persona nello spazio digitale.

Introduzione: Crisi socio-economica ed Europa digitale.*

Il rapido sviluppo economico su scala globale comporta il quotidiano confronto della società contemporanea con situazioni critiche derivanti da alti livelli di inquinamento, problemi energetici (maggiormente attuali a causa della guerra Russia-Ucraina) e di sicurezza, accompagnate da degrado urbanistico-edilizio e disparità socio-economiche.

A tali realtà concrete sembra poter rispondere l'impiego delle nuove tecnologie, strumento centrale della strategia europea, fondata su una crescita "intelligente", "sostenibile" e "inclusiva".

L'obiettivo di un'Europa digitale (Programma 2021-2027) rappresenta una priorità strategica per la trasformazione digitale dell'economia, dell'industria e della società europea, i cui cittadini ne saranno i primi fruitori sulla scorta della Comunicazione n. 67/2020 della Commissione al Parlamento Europeo, al Consiglio e al Comitato economico e sociale europeo e al comitato delle regioni (COM (2020) 67 final del 20 febbraio 2020 «Plasmare il futuro digitale dell'Europa» - accolto anche dal Consiglio dell'UE nella seduta del 9 giugno 2021[1]) e della più recente Decisione, 14 dicembre 2022, n. 2481, adottata dal Parlamento europeo e dal Consiglio dell'Unione europea, che istituisce il programma strategico per il decennio digitale 2030 allo scopo di conseguire, accelerare e plasmare una trasformazione digitale efficace per l'economia e la società europea. La trasformazione digitale costituisce un fattore chiave del «*Green Deal* europeo» e del Next Generation UE, e quindi anche del PNRR: intelligenza artificiale, 5G, 6G, *blockchain*, *cloud*, computazione di prossimità, *internet of things*[2] devono accelerare e massimizzare l'impatto delle

* Il lavoro è il risultato del Progetto di ricerca finanziato dal Ministerio de Ciencia e innovacion Spagnolo, Referencia PID2019-108669RB-100/AEI/10.13039/501100011033, Titulo "Derecho e inteligencia artificial: nuevos horizontes juridicos de la personalidad y la responsabilidad roboticas". Investigador Principal Margarita Castilla Barea, Profesora titular, Facultad de Derecho, Campus de Jerez, Universidad de Cádiz, Spagna.

[1] Il fulcro della comunicazione consiste nell'esigenza di una trasformazione sostanziale della società con soluzioni digitali affidabili, al servizio delle persone, in linea con i valori comuni dell'Europa: democrazia, rispetto dei diritti fondamentali e sostenibilità. Sostenibilità che diventa principio fondamentale per il cambiamento del paradigma socioeconomico e per il superamento delle diseguaglianze. Cfr. P. PIRAS, *Innovazione tecnologica e divario digitale*, in *Dir. econ.*, 2022, 2, 111.

[2] L'espressione *Internet of Things* (IoT) fa riferimento ad infrastrutture caratterizzate da innumerevoli sensori progettati per registrare, processare, immagazzinare dati che interagiscono mediante una rete di comunicazione elettronica. L'IoT costituisce un ulteriore sviluppo di *Internet*, conseguente alla connessione in rete di oggetti materiali intelligenti, dotati di un identificativo univoco, riconoscibile anche in

politiche anche per affrontare i cambiamenti climatici e proteggere l'ambiente. La decisione promuove, infatti, un "ambiente digitale antropocentrico", finalizzato a diffondere l'uso delle competenze digitali, per consentire l'accesso alle tecnologie a condizioni eque e ridurre il divario digitale, promuovendo un contesto normativo che sostenga infrastrutture e tecnologie digitali sostenibili e che promuova la partecipazione *online* alla vita democratica e ai servizi pubblici[3], per contribuire pienamente alla transizione verde e digitale.

Il programma europeo va, poi, coordinato con l'Agenda 2030 per lo sviluppo sostenibile e monitorato nella sua attuazione con l'indice di digitalizzazione dell'economia e della società (DESI), affinché si possa intervenire *in itinere* con eventuali aggiustamenti per la realizzazione degli obiettivi[4].

A fronte di tali epocali trasformazioni, al giurista non resta che analizzare il fenomeno, determinarne le implicazioni per il sistema ordinamentale e individuare le regole che lo conformano. Il giusprivatista, in particolare, è chiamato a verificare se le nuove tecnologie compromettano diritti e tutele della persona, garantiti in àmbito nazionale, europeo e internazionale, o se, addirittura, vadano ridefiniti i diritti della persona alla luce dell'era digitale[5]. Tecnologia e digitalizzazione devono essere funzionali al miglioramento della qualità della vita delle persone e non fini a sé stesse, soprattutto in periodi caratterizzati da scarsità di risorse, come quello attuale.

1. Nuove tecnologie, social network e diritti della persona.

Se è vero che grazie alla tecnologia si accede a fonti di informazione e comunicazione fondamentali non solo per lo sviluppo economico e sociale, ma anche per l'esplicazione della personalità dell'individuo, è parimenti vero che, purtroppo, per ragioni socio-economiche e di poca dimestichezza con i *device* (come precedentemente dimostrato dalla relazione DESI 2022), gran parte della popolazione (costituita, soprattutto, da donne, anziani, immigrati, disabili e minori) non può beneficiare dell'uso di tali tecnologie informatiche, vedendosi preclusa la possibilità di esercitare alcuni diritti individuali fondamentali. Tramontati i tentativi di riforma costituzionale che configurano un vero e proprio "diritto di accesso" alla rete *internet*, si può riconoscere il

radiofrequenza. Ci troviamo di fronte già al *web* 3.0 e, quindi, alla possibilità che le cose dialoghino tra loro grazie alla Rete, con inevitabili conseguenze da un punto di vista giuridico, poiché tali rapporti non hanno esseri umani come "parti". Per approfondimenti circa la modalità di protezione delle soluzioni basate sull' *Internet of Things*, v. E. PEZZOLI, *Internet of things*, *tecnologia blockchain e diritti Ip*, in *Dir. ind.*, 2020, 113.

[3] Mentre il cittadino di un sistema democratico tradizionale legge e sceglie le informazioni attraverso i *media* tradizionali (stampa, radio e televisione, cui spetta la narrazione e interpretazione degli eventi) e le condivide seguendo uno schema lineare e unidirezionale (dall'alto verso il basso), nei regimi democratici contemporanei, i lettori, gli ascoltatori, gli spettatori attingono le informazioni alle fonti passivamente, potendo al più condividerle e commentarle con cerchie ristrette di contatti, seguendo un andamento circolare. G. SGUEO, *La visione e la voce nella transizione digitale dei governi democratici*, in *Riv. trim. dir. pub.*, 2022, 4, 1015.

[4] L'indice di digitalizzazione dell'economia e della società (DESI) per il 2022 colloca l'Italia in una buona posizione rispetto alla connettività, ma in uno stadio critico rispetto all'acquisizione di competenze digitali di base e avanzate, con importanti ricadute nell'utilizzo dei relativi servizi; in *https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance*.

[5] V. G. RESTA, *Le nuove frontiere dei diritti della personalità*, in G. ALPA E G. RESTA, *Le persone e la famiglia 1. Le persone fisiche e i diritti della personalità*, in *Trattato di diritto civile* diretto da R. Sacco, Utet, Torino, 2019, 365.

diritto ad esercitare, anche attraverso la rete, libertà costituzionalmente garantite[6].

Internet è un esempio di *network* virtuale, una rete sociale che identifica e riunisce comunità virtuali che condividono idee, attitudini, risorse, preferenze, comportamenti, necessità, rischi e altre caratteristiche che non dipendono dalla prossimità geografica[7], che consente a chiunque abbia una sufficiente alfabetizzazione informatica piena libertà di accesso non solo all'informazione (intesa quale diritto ad informarsi, ad essere informato e di fare informazione), ma anche al diritto a partecipare alla vita sociale e politica, realizzando la piena esplicazione della personalità dell'individuo (art. 2 Cost.) in condizioni di assoluta democrazia ed eguaglianza[8].

In particolare, le nuove tecnologie possono annoverarsi in «ogni altro mezzo di diffusione» previsto dall'art. 21 Cost.[9], in tema di libertà di manifestazione del pensiero; situazione giuridica, quest'ultima, espressione del valore unitario della persona e di istanze di promozione della collettività, in quanto al singolo viene garantita la possibilità di esprimere opinioni e valutazioni di ogni sorta anche attraverso la rete, ove si attingono e si forniscono informazioni[10]. All'esercizio di tale libertà consegue l'attribuzione di doveri in capo a colui che esprime idee e fa informazione, nonché responsabilità per le conseguenze eventualmente pregiudizievoli che la loro diffusione può avere su interessi di pari rango del singolo o della collettività. *Internet*, luogo virtuale complesso e

---

[6] Per i riferimenti normativi e i commenti relativi alle proposte di riforma costituzionale, v. M.R. ALLEGRI, *Il diritto di accesso a Internet: profili costituzionali*, in *Riv. dir. media*, 2021, 68, nonché G. D'IPPOLITO, *Il diritto di accesso ad Internet in Italia: dal 21(-bis) al 34-bis*, ivi, 2021, 82.

[7] M.E.J. NEWMAN, *Networks. An Introduction*, Oxford, 2010, 23-25.

[8] L'evoluzione tecnologica del sistema delle telecomunicazioni sta ridefinendo diritti della personalità come il diritto alla riservatezza e il diritto alla personalità individuale, conferendo al primo una qualificazione statica sul tipo dei diritti assoluti ed al secondo una connotazione che vede il soggetto decidere come fare circolare le informazioni al proprio riguardo. Emblematico, in tal senso, è il caso Google v. Vividown, ove in primo grado il Tribunale di Milano (Trib. Milano 24 febbraio 2010), eccedendo nella salvaguardia del valore persona, sancì in capo al *service provider* la responsabilità penale per il reato di trattamento illecito di dati personali per omessa vigilanza, attribuendo agli intermediari dell'informazione l'obbligo preventivo di controllo sui dati immessi (G. CASSANO, A. CONTALDO, *Diritti della persona, internet e responsabilità dei soggetti intermediari*, in *Corr. giur.*, 2010, 8). La nota vicenda processuale si evolve in appello ove, invece, la Corte ambrosiana (Corte d'appello Milano, 27 febbraio 2013) esclude che l'*host provider*, anche se attivo, debba impedire reati realizzati dagli utenti della rete, stabilendo che non spetta al *provider* verificare che i propri utenti non trattino illecitamente dati di terzi; controllo, peraltro, impossibile dal punto di vista tecnico, e non imposto da alcuna norma. Cfr. A. INGRASSIA, *La decisione d'Appello nel caso Google vs Vivi down: assolti i manager, ripensato il ruolo del provider in rete*, in *Corr. Merito*, 2013, 766. La vicenda si conclude presso la Suprema Corte che conferma in pieno la decisione dei giudici di appello (Corte di Cassazione, sez. III Penale, 3 febbraio 2014, n. 5107): v. F. NOTARI, *La controversa responsabilità dell'Internet Service Provider in materia di privacy nella giurisprudenza europea e interna: il caso Google*, in *Amministrazione in cammino,* 30/04/2016.

[9] Vale la pena di ricordare che, oltre all'art. 21 della nostra Costituzione, anche l'art. 10 della Convenzione Europea dei diritti dell'uomo garantisce la libera manifestazione del pensiero; il che dimostra che tale diritto è frutto del riconoscimento dell'uomo-persona in quanto tale: prescinde, cioè, dalle previsioni all'interno delle Costituzioni dei singoli Stati. Cfr. M. DE SALVIA, *La Convenzione europea dei diritti dell'uomo. Procedure e contenuti*, Napoli, 1997, 99.

[10] Sul tema, fra i tanti, v. V. ZENO-ZENCOVICH, *La libertà d'espressione. Media, mercato, potere nella società dell'informazione*, Bologna, 2004, 125; S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004, *passim*; G. AZZARITI, *Internet e Costituzione*, in *Costituzionalismo.it*, 2, 6 ottobre 2011; M. BIANCA, A. GAMBINO E R. MESSINETTI (a cura di), *Libertà di manifestazione del pensiero e diritti fondamentali. Profili applicativi nei social networks*, Milano, 2016, *passim*; G. PITRUZZELLA, *La libertà di informazione nell'era di Internet*, in *Riv. dir. media*, 2018, 20; G.L. CONTI, *Manifestazione del pensiero attraverso la rete e trasformazione della libertà di espressione: c'è ancora da ballare per strada?*, in *Riv. AIC,* 2018, 200; M. BASSINI, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in *Riv. dir. media*, 2021, 67.

articolato, ove oltre all'informazione si realizza anche la comunicazione interattiva[11], per sua natura, considerata la velocità e l'assenza di confini territoriali che lo caratterizza, può ledere in maniera amplificata e irrimediabile altri diritti della persona parimenti tutelati. Di qui il necessario bilanciamento tra tutela di diritti e interessi equiordinati, con la previsione di limiti alle libertà di manifestazione e comunicazione nella rete[12], nel rispetto dei diritti della persona e del diritto alla riservatezza, nell'ottica che la rete non possa essere considerata un "non luogo" senza regole[13]. Al riguardo si pensi, ad esempio, alle numerose violazioni della *privacy*, connesse all'intrinseca natura dei *social network*, che costituiscono uno degli effetti più evidenti dell'impatto di *Internet* sulle relazioni interpersonali (oltre che con enti di qualsiasi natura). I *social*, frutto dell'inarrestabile evoluzione tecnologica, essendo finalizzati alla diffusione di informazioni e dati di ogni natura, costituiscono di per sé una potenziale fonte di violazione di diritti della persona[14]. Tra questi, inevitabilmente, il diritto fondamentale della persona, riconosciuto dall'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), che comprende il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza. Un campo di

[11] In proposito, v. P. COSTANZO, Internet, in *Dig. disc. pubbl.*, Agg.*, Torino, 2000, 357; P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, III. IV ed., Napoli, 2020, 133.

[12] Un interessante esempio di bilanciamento tra diritti contrapposti, su cui è intervenuta di recente la Corte di giustizia dell'Unione europea (a dimostrazione ulteriore che la rete non può essere considerata una zona "franca" del diritto), è fornito dalla libertà di espressione dell'utente (garantita dall'art. 11 della Carta europea dei diritti fondamentali) *versus* il diritto di proprietà intellettuale (art. 17, comma 2, Carta), ove il secondo si pone, in rete, come limite all'esercizio della libertà di espressione. In questo senso, la Polonia ha sollevato la questione di legittimità sull'art. 17 della Direttiva (UE) n. 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e, in particolare, delle lettere b) e c) del par. 4 della medesima disposizione, al fine di determinare se il regime specifico di responsabilità, introdotto dall'articolo 17, paragrafo 4, della direttiva 2019/790 per i fornitori di servizi di condivisione di contenuti *online*, comporti una limitazione dell'esercizio del diritto alla libertà di espressione e d'informazione degli utenti di tali servizi. I fornitori poiché non riescono sempre ad ottenere l'autorizzazione per tutti i contenuti protetti caricati sulle loro piattaforme dagli utenti, al fine di evitare di essere ritenuti responsabili per contenuti illeciti, devono dimostrare di aver compiuto i massimi sforzi (*ex* art.17, paragrafo 4, lettera a), direttiva *copyright* 2019/790) per ottenere un'autorizzazione siffatta. La Corte precisa, infine, che, nonostante i massimi sforzi previsti, il prestatore potrebbe essere tenuto a intervenire *ex post*, a séguito di segnalazione motivata, per rimuovere il contenuto non autorizzato, caricato ugualmente sulla piattaforma, per violazione della libertà di espressione e d'informazione. Corte giust. UE, 26.4.2022, causa C-401/19, in G. M. RICCIO, *Responsabilità delle piattaforme e sistemi di filtraggio: quale destino per la normativa italiana sul diritto d'autore?*, in *Nuova giur. civ. comm.*, 2022, 5, 1032.

[13] Si pensi al caso dell'*ex* Presidente degli Stati Uniti, Donald Trump, i cui profili su diversi *social network*, ad inizio del 2021, furono sospesi, in virtù di una possibile connessione fra alcuni *tweet* del presidente uscente ed i violenti scontri verificatisi a Capitol Hill il 6 gennaio 2021. La vicenda ha sollevato un dibattito politico e giuridico di rilievo circa la legittimità di tale blocco, che, in realtà, sottende la domanda di fondo su quale sia la soglia fino a cui possa spingersi la libertà di espressione sui *social network*, e se questa possa essere compressa o ridimensionata dai grandi colossi della Rete. Cfr. M. CIANCIMINO, *La libertà di espressione nel mondo digitale: alcune coordinate civilistiche in tema di contenuti controversi sui social network*, in *Dir. fam. pers.,* 2022, 1, 360.

[14] I *social network* non sono altro che servizi *web* che consentono ad ognuno di costruirsi un profilo all'interno di un sistema di produzione dell'informazione, cosicché l'utente più che essere un mero fruitore dei contenuti diventa autore degli stessi. Essi sono talmente radicati nella società contemporanea da determinare rilevanti cambiamenti nei modi della comunicazione e diffusione delle idee e delle informazioni, nonché da condizionare comportamenti collettivi ed individuali nel mondo «reale», come dimostrano emblematicamente le manifestazioni che si organizzano in brevissimo tempo in rete ovvero i fatti tragici posti in essere da singole persone per effetto o tramite i medesimi. Circa il radicale mutamento dei rapporti sociali operato dai *social network* e la difficoltà d'inquadramento del fenomeno in ambito giuridico, considerando la pluralità e varietà dei loro caratteri fisionomici, v. C. PERLINGIERI, *Profili civilistici dei social networks*, Napoli, 2014, 15.

applicazione ampio, in cui il legislatore preservare la vita privata e familiare, il domicilio e la corrispondenza da ingerenze arbitrarie dell'autorità pubblica, ma anche obbligare gli Stati membri a garantire che tali diritti siano osservati nei rapporti tra privati, con l'adozione di misure finalizzate ad assicurare il rispetto della vita privata anche nella sfera delle relazioni interpersonali.

A livello europeo, in ossequio all'articolo 52 TUE (che mira a fissare la portata dei diritti e dei principi della Carta europea dei diritti fondamentali e a definire norme per la loro interpretazione), con particolare riferimento al paragrafo 3 (che assicura coerenza tra la CDFUE e la CEDU, affermando che, qualora i diritti della Carta corrispondano ai diritti della CEDU, il loro significato e la loro portata sono identici) i diritti di cui all'articolo 7 della Carta europea dei diritti fondamentali sono omologhi a quelli garantiti dall'articolo 8 della CEDU, con l'unica differenza che, in ragione dell'evoluzione tecnica, il termine "comunicazione" ha sostituito quello di "corrispondenza"[15]. L'art. 8 della CDFUE, invece, relativo alla Protezione dei dati di carattere personale, si differenzia dal più generale diritto al rispetto della vita privata e familiare, in quanto ruota attorno alla nozione di trattamento[16] e di dato personale. Si tratta di una distinzione non solo apparente, in quanto nella prima, rispetto della vita privata e familiare, si manifesta soprattutto il momento individualistico, cui consegue solo una tutela statica di carattere negativo, che consiste sostanzialmente nell'escludere altrui interferenze; mentre nella protezione dei dati, la tutela è dinamica, in quanto segue la circolazione dei dati, fissando regole ineludibili sulle modalità del loro trattamento[17]. Al riconoscimento di tale diritto fondamentale è seguito, come è noto, il quadro solido e coerente del *General Data Protection Regulation*, approvato con 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, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)[18].

---

[15] Per approfondimenti in proposito, a vent'anni dalla proclamazione della Carta, che riafferma «i diritti derivanti in particolare dalle tradizioni costituzionali e dagli obblighi internazionali comuni agli Stati membri, dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, dalle carte sociali adottate dall'Unione e dal Consiglio d'Europa, nonché dalla giurisprudenza della Corte di giustizia dell'Unione europea e da quella della Corte europea dei diritti dell'uomo», v. C. AMALFITANO, *La Carta dei diritti fondamentali dell'Unione europea compie venti anni*, in. C. AMALFITANO, M. D'AMICO E S. LEONE (a cura di), *La Carta dei diritti fondamentali dell'Unione europea nel sistema integrato di tutela. Atti del convegno svoltosi nell'Università degli Studi di Milano a venti anni dalla sua proclamazione*, Torino, 2022, 19.

[16] Per quel che riguarda il concetto di «trattamento», bisogna fare riferimento all'art. 4, n. 2, del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, in base al quale per «trattamento» si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Tutte "operazioni" usuali in un *social network*, ove non occorre un invio dei dati a terzi, ma basta che essi siano "disponibili" all'*account* dell'utente creato nel *social network* o tramite *link* a siti o altri *account* in rete, comunicati a uno o più soggetti determinati ovvero diffusi a soggetti indeterminati. Cfr. E. PELINO, *Trattamento*, in L. BOLOGNINI, E. PELINO E C. BISTOLFI, *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 86.

[17] Così, S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 397.

[18] Tra i tanti, v. E. TOSI, *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice privacy*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, 1.

Ai fini della presente trattazione è interessante notare che per «dato personale» si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile, direttamente o indirettamente, la persona con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, comma 1, GDPR). In tale elenco sono annoverabili immagini, soprannomi o c.dd. *Nickname*, indirizzi e recapiti elettronici, *account* e siti personali, numeri e *password* di accesso, *tag* ecc. riferibili ad una persona fisica, dunque parte assai rilevante dei "materiali" e dei dati immessi quotidianamente in rete dagli utenti nei *social network*, fin dal momento della loro registrazione. Di qui l'attenzione meticolosa alla lesione della protezione delle persone fisiche con riguardo al trattamento dei dati personali, nel cui àmbito vengono distinte violazioni in senso stretto, relative alle regole di trattamento dei dati personali, e violazioni della c.d. riservatezza informatica, comprensiva di tutte le inosservanze del diritto di escludere terzi da determinati dati, spazi e sistemi informatici e ai suoi rimedi[19].

I *social network*, però, non rientrano solo in uno dei tanti mezzi di diffusione (*ex* art. 21 Cost.) in cui si esplica la libertà di manifestazione del pensiero, ma rappresentano anche dei "non luoghi" dove si realizza pienamente la libertà di associazione *ex* art. 18 Cost. che, nella rete, come è noto, è da considerare non solo come mera libertà negativa (cioè come divieto di impedirne lo svolgimento con forza di legge), ma anche come promozione della sua attuazione attraverso un sistema legislativo ed amministrativo idoneo, quale, oggi, si realizza diffusamente nelle reti sociali virtuali, costituite da gruppi di persone connesse tra loro. Infatti, per entrare a far parte di un *social*, occorre costruire, in primo luogo, il proprio profilo personale, partendo dal proprio indirizzo *email*, fino ad arrivare all'indicazione degli interessi e delle esperienze di lavoro, successivamente è possibile invitare amici a far parte della propria rete, i quali a loro volta possono fare lo stesso, cosicché ci si trova ad allargare la cerchia di contatti con gli amici degli amici e così via, fino a comprendere, in teoria, tutta la popolazione del mondo. In base alle proprie passioni o aree di affari, è, poi, possibile costituire anche comunità tematiche, aggregando ad esse altri utenti e stringendo contatti di amicizia o di affari [20].

I *social media*, dunque, in sé considerati, sono un luogo di aggregazione virtuale, parallelo a quelli reali, aperto e connotato da parità di trattamento, in quanto le persone diventano utenti di una medesima piattaforma, all'interno della quale l'iscritto sviluppa attivamente la propria personalità. Non a caso *Facebook* gode del primato di essere la prima grande comunità sociale virtuale,

[19] Per «riservatezza informatica» si intende il "nuovo diritto" di escludere terzi, non autorizzati, dall'accesso e dalla fruizione di spazi, sistemi e dati informatici, a prescindere dal loro contenuto. È un diritto della persona ricavabile dall'art. 8 CEDU e dall'art. 7 della Carta di Nizza, che si correla ai più tradizionali diritti inviolabili della riservatezza, della corrispondenza e della tutela del domicilio, che nel nostro ordinamento trova tutela penale nella fattispecie che punisce l'accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-*ter* c.p., e nel delitto prodromico di detenzione abusiva o procacciamento abusivo di codici di accesso e parole chiave, di cui all'art. 615-*quater* c.p. Cfr. L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei social network. aspetti penali*, in *Giur. Merito*, 2012, 2522.

[20] R. MORO VISCONTI, *La valutazione dei social network*, in *Dir. ind.*, 2020, 71.

quindi non un semplice passivo fruitore di contenuti ma un creatore dei medesimi. I *social*, infatti, sono paragonabili alle comunità intermedie, costituite da persone che si aggregano per realizzare uno scopo comune, che individualmente non potrebbero raggiungere, utile alla formazione ed allo sviluppo della persona. In tal senso l'iscrizione dell'utente alla piattaforma può essere paragonata all'adesione ad un'associazione non riconosciuta.

In quanto ente dal carattere aperto, la registrazione al *social* è subordinata all'accettazione di regole comportamentali, diritti, doveri e responsabilità, come se si trattasse di uno statuto che regolamenta la vita interna di un ente; la maggior parte dei *social media*, infatti, subordina l'iscrizione all'adesione alle condizioni generali di servizio (c.dd. *standard* della *community*), che tendenzialmente non creano un perfetto equilibrio tra diritti ed obblighi nel rapporto tra *hosting provider* ed utente, tanto da far assumere al primo una netta supremazia nei confronti del secondo[21]. La piattaforma, infatti, a séguito dell'iscrizione, disciplina contrattualmente le condotte che gli utenti devono osservare per la sua utilizzazione, cercando di bilanciare i contrapposti interessi nei rapporti tra gli utenti, ai quali deve essere consentito di esercitare all'interno del *media* la libertà di espressione e quella di associazione. Di qui l'esercizio dell'autonomia privata della piattaforma, che, nel regolare i rapporti con gli utenti, cancella i contenuti o, addirittura, limita l'accesso alla piattaforma stessa qualora tali diritti siano violati[22], nella consapevolezza che l'esclusione da *social* quali Facebook, Tiktok o altro può essere estremamente penalizzante non solo per la limitazione della diffusione di informazioni, ma anche per la lesione di interessi di natura economica derivanti dalla perdita di posizione nell'agorà digitale, luogo virtuale in cui vengono poste in essere gran parte delle attività economiche.

Attualmente, in attesa dell'entrata in vigore della normativa europea prevista dal pacchetto *Digital Services Act*[23], per evitare che l'*agĕre* della piattaforma, con le proprie attività economiche, possa impedire la realizzazione di fini primari indicati dalla Costituzione, quali le anzidette libertà di manifestazione del pensiero, libertà di associazione e diritto alla protezione dei dati personali, gli unici limiti invalicabili sono presenti all'interno dello stesso art. 41 Cost.: l'utilità sociale e la dignità della persona[24].

---

[21] G. PASSARELLI, *La metamorfosi dei social media. la rilevanza sociale nell'attuale agorà digitale di un servizio "privatistico"*, in *Nuova giur. civ. comm.*, 2021, 1195.

[22] Sulla crisi del sistema delle fonti ed il ritorno ad un «diritto dei privati» che è non solo *self-regulation*, ma vera e propria autonoma produzione privata del diritto nello spazio digitale, v. E. CREMONA, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli, 2023, 39.

[23] Il Regolamento UE 2022/206 (Digital Services Act) del 27 ottobre 2022 e il Digital Markets Act si preoccupano di regolamentare in modo differenziato e specifico, con strumenti di vigilanza costante, le piattaforme che hanno assunto una posizione rilevante nel mercato o nell'ambito dell'informazione, definendole come *gatekeeper*. Questi ultimi, infatti, saranno sottoposti a stringenti obblighi riguardanti il trattamento dei dati personali, in quanto per le dimensioni imprenditoriali e territoriali facilitano la circolazione delle informazioni, e prevenzione di squilibri contrattuali nei confronti degli utenti finali dei servizi di base forniti dalla piattaforma. A tali obblighi si aggiungono anche divieti di pratiche sleali e di condizioni inique a presidio della concorrenza e della protezione del mercato digitale. Cfr. M. A. ASTONE, *Digital services Act e nuovo quadro di esenzione dalla responsabilità dei prestatori di servizi intermediari: quali prospettive?*, in *Contr. Impr.*, 2022, 4, 1050.

[24] «La variabilità delle situazioni economiche che caratterizza il nostro tempo rende necessari strumenti dotati di particolari virtù di espansione e di adattamento tali da consentire, ferma restando la determinazione degli interessi giuridicamente rilevanti, il mutare nel tempo delle relazioni fra questi e gli

L'inarrestabile evoluzione tecnologica necessita, dunque, di un costante bilanciamento tra diritti e interessi contrapposti: la libertà di espressione e di associazione degli utenti, da un lato, e la libertà di iniziativa economica privata della piattaforma, dall'altro, nel prisma del principio di uguaglianza (art. 3 Cost.). Principio, quest'ultimo, che assume decisiva importanza per evitare che, nell'attuale era digitale, i diritti individuali fondamentali della persona risultino tutelati solo sulla carta[25] a causa del *digital divide*, che impedisce, di fatto, la realizzazione di quell'uguaglianza sostanziale, che supera la programmazione puramente di principio voluta dai nostri Padri costituenti nel 1948.

2. Emersione del problema del digital divide e rilevanza degli studi di settore.

Con l'espressione «*digital divide*» si è soliti indicare la distribuzione non uniforme delle tecnologie dell'informazione e della comunicazione nella società, in particolare la situazione soggettiva caratterizzata dall'impossibilità, per condizioni socio-economiche, tecnologiche, educativo-didattiche o di età anagrafica, di "accedere" al contesto digitale.

Era il lontano 1994 quando il Ntia (*National telecommunication and information administration* americano) introdusse, per la prima volta, nella sua indagine annuale sulle telecomunicazioni la voce circa l'accesso ad *internet,* via cavo. Non a caso, forse, era l'anno in cui Microsoft lanciava il primo *browser* per navigare in internet, rete nata in àmbito militare, utilizzata anche nel campo universitario.

Per la prima volta emerse la consapevolezza di quanto fosse rilevante avere accesso ad *internet* per istituzioni, imprese e cittadini[26], lì dove, però, non tutti gli individui hanno la possibilità di interagire con *devices* tecnologici collegati alla rete; donde l'incapacità di autodeterminarsi nelle fattispecie normative connotate dall'utilizzo di uno strumento tecnologico: si pensi, infatti, alle persone con menomazioni fisiche o psichiche, agli anziani, agli immigrati e ai minori, a soggetti, cioè, vulnerabili per definizione[27].

Poiché non si rinviene alcuna definizione di *digital divide* in normative internazionali, europee e nazionale, per studiare la problematica occorre far ricorso ad altre discipline, quindi confrontarsi con aspetti che non possono essere affrontati attingendo ad un angolo di visuale unico. Di qui la necessità di un lavoro interdisciplinare, che sia non mera giustapposizione di saperi ma creazione di nuova conoscenza con il dialogo tra diverse discipline[28]. Il risultato di tale confronto assume preminente interesse non solo per gli studiosi, ma

atti in cui si svolge l'attività economica di privati». M. NUZZO, *Utilità sociale e autonomia privata*, Milano, 1975, 83.

[25] F. DI CIOMMO, *Diritti della personalità tra media tradizionali e avvento di Internet*, in G. Comandé (a cura di), *Persona e tutele giuridiche*, Torino, 2003, 3.

[26] L. SARTORI, *Il divario digitale. Internet in Il nostro digitale quotidiano*, 4, 2022, pp. 166-172.

[27] I.A. CAGGIANO, *"Privacy" e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in *Familia*, 2018, 3.

[28] G. PASCUZZI, *La definizione del problema nella ricerca interdisciplinare*, in G. BELLANTUONO e U. Izzo (a cura di), *Il rapporto tra diritto, economia e altri saperi: la rivincita del diritto*. Atti della *Lectio Magistralis* di Guido Calabresi in occasione della chiusura dell'anno accademico del Dottorato in Studi Giuridici Comparati ed Europei. Facoltà di Giurisprudenza. Trento, 24 ottobre 2019, Napoli, 2022, 55.

anche, ai fini applicativi, per il formante giurisprudenziale, in virtù del bilanciamento di interessi contrapposti, quali, da un lato, l'inevitabile evoluzione tecnologica e, dall'altro, la tutela dei diritti della persona, soprattutto dei più deboli. D'altra parte, è la persona ad essere al centro del sistema ordinamentale italo-europeo delle fonti[29] e il *digital divide* non fa altro che minarne il pieno sviluppo per i risvolti non solo di carattere socio-economico, ma anche di tutela dal punto di vista giusprivatistico[30], come si è già avuto modo di constatare nelle recenti vicende correlate alla diffusione del coronavirus.

È necessario, dunque, affrontare studi specifici al fine di individuare soluzioni giuridiche volte a promuovere una nuova alfabetizzazione digitale, che aiuti a comprendere realmente i meccanismi tecnici e le dinamiche relazionali che si sviluppano in *Internet*, evitando che il *digital divide* sia, tuttora, una realtà tangibile.

L'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), nel suo Skills Outlook 2019, studio sul divario digitale[31], ha posto l'accento sulle differenze tra individui, famiglie, imprese e aree geografiche relativamente alle opportunità di accesso alle infrastrutture di telecomunicazione di base, ai servizi delle tecnologie dell'informazione e della comunicazione (TIC), prodromici all'uso di *Internet*, che presuppone, a sua volta, la disponibilità di un *computer*. È stato notato che tale capacità varia in modo significativo a seconda che si tratti di Paesi OCSE o meno, in quanto il divario digitale dipende da variabili, quali il reddito, l'istruzione (quanto più alto è il livello, tanto più gli individui hanno accesso alle TIC), le dimensioni e il tipo di famiglia, l'età, il sesso e, infine, il *background* razziale e linguistico. L'analisi dell'OCSE è, dunque, fondamentale affinché gli Stati, disponendo di informazioni sulla natura e l'entità del divario digitale, possano realizzare le necessarie riforme politiche e normative, stabilendo misure idonee a garantire a tutti i cittadini (art. 3 Cost.), nonché alle imprese, l'accesso a nuove tecnologie e servizi.

L'OCSE sottolinea l'importanza della liberalizzazione dei mercati delle telecomunicazioni e della concorrenza nei Paesi aderenti all'organizzazione, che ha stimolato nuovi investimenti e aumentato la domanda di accesso ai servizi di comunicazione grazie all'abbassamento dei costi e all'offerta di prodotti innovativi. D'altra parte le azioni dirette a ridurre il divario digitale spaziano dal potenziamento delle infrastrutture fino alle politiche volte a

---

[29] Sul principio personalistico si veda, P. PERLINGIERI, *La persona e i suoi diritti*, Napoli, 2005, *passim*, (in particolare, «*Prefazione*», IX, par. 1; «*La personalità umana nell'ordinamento giuridico*», *ivi* , 5 ss.; «*A margine della Carta dei diritti fondamentali dell'Unione europea*», *ivi* , 65-69, relazione al Seminario conclusivo dei corsi di Istituzioni di diritto privato "Principi, diritti e regole nella Carta Europea", tenutosi a Firenze il 26-27 aprile 2001, pubblicato in *Riv. giur. Molise Sannio*, 2001, 153), F. GALGANO, *Comm. art. 41 Cost.*, in F. Galgano e S. Rodotà, *Commentario alla Costituzione, artt. 41-44, Rapporti economici*, a cura di Branca, Bologna-Roma, 1982, 26; D. MESSINETTI, voce *Personalità (diritti della*), in *Enc. dir.,* Milano, 1983, XXXIII, *passim*, nonché G. ALPA, *Attuazione e attualità nella Costituzione: il caso dei diritti della persona*, in *Nuova giur. civ.*, 1997, pt. 2, 1, nonché G. ALPA, *La persona nelle costituzioni: sintesi storica*, in *Cultura e diritti*, 2013, 65.

[30] Pone l'accento sulla rilevanza e la necessità di affrontare nel modo più adeguato le sfide e i rischi intrinseci alla società dell'*Information and communications technology*, mettendo al centro della riflessione le persone, con riguardo, specialmente, all'intelligenza artificiale e ad un suo utilizzo etico, E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Dir. fam. pers.* 2022, 3, 1096.

[31] Lo studio rappresenta un primo sforzo per ottenere dati sulle dimensioni del *digital divide*, nuovo fenomeno la cui analisi evidenzia le differenze esistenti tra i diversi Paesi, nonché al loro interno, https://www.oecd.org/sti/1888451.pdf.

migliorare l'alfabetizzazione informatica/*internet*, con la costruzione delle competenze di base già nelle istituzioni scolastiche. Non mancano anche programmi di sostegno per le piccole imprese, in quanto, inevitabilmente, più lente nell'adottare le nuove tecnologie e pregiudicate dalle particolari asimmetrie informative, sempre nell'ottica della cooperazione multilaterale, importante per ridurre le differenze a livello internazionale e migliorare la qualità delle prestazioni. Non a caso l'area OCSE è sempre stata all'avanguardia nella "rivoluzione digitale" e funge da esempio di politiche che sembrano dimostrarsi efficaci per gli altri Paesi[32].

3. Le soluzioni del legislatore italiano prima e dopo la pandemia da covid-19. La Dichiarazione europea dei principi e dei diritti digitali.

Il *digital divide* suscita, al pari dell'analfabetismo[33], uno dei tanti problemi che affliggono il nostro Paese, che, nel tempo, si è preoccupato di contribuire ad attenuare la diseguaglianza, che, di fatto, limita la libertà e l'eguaglianza dei cittadini, precludendo il pieno sviluppo della persona umana e l'effettiva partecipazione all'organizzazione politica, economica e sociale dello Stato (art. 3, comma 2, Cost.).

Il Codice della Amministrazione digitale[34], che trae linfa dall'art. 97 Cost., all'art. 8, rubricato "Alfabetizzazione informatica dei cittadini", ha previsto che lo Stato promuova iniziative volte a favorire l'alfabetizzazione informatica e la cultura digitale tra i cittadini, con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni con azioni concrete. Si riconosce, in tal modo, *ante litteram*, una sorta di vero e proprio diritto sociale di carattere generale, di cui si favorisce la promozione nei rapporti con la P.A.[35], al fine di esercitare i diritti di cittadinanza digitale, sanciti dalla seconda sezione del Capo I, "Carta della cittadinanza digitale"[36]. La Carta riconosce ai cittadini e alle imprese una serie di diritti, tra cui quello all'uso delle tecnologie nei rapporti con la P.A. anche ai fini dell'accesso e della partecipazione al procedimento amministrativo (art. 3); il diritto di accedere ai servizi *on line* delle P.A. tramite

---

[32] M. RAGNEDDA, *Il digital divide. Le diseguaglianze digitali e i suoi vari livelli di analisi*, in *Quad. teoria soc.*, 2018, 81.

[33] Cfr. A. MAIONCHI, *Digital divide: i nuovi analfabeti*, in L. BRUSCAGLIA, R. ROMBOLI, *Diritto pubblico e diritto privato nella rete delle nuove tecnologie*, Pisa, 2011, 63.

[34] D.lg. 7 marzo 2005, n. 82, oggetto di profonde modifiche ad opera del d.lg. 26 agosto 2016, n. 179 e del d.lg. 13 dicembre 2017, n. 217, che ne hanno ampliato la portata.

[35] Circa la possibile configurazione di un vero e proprio diritto di accesso a internet, varie sono le ricostruzioni. Secondo una prima impostazione, esisterebbe una libertà di accesso alla rete, intesa come diritto a che nulla osti, nel rapporto libertà-autorità, all'esercizio delle libertà d'informazione e comunicazione. Secondo altri autori, l'accesso a internet sarebbe configurabile come diritto sociale, ossia una pretesa soggettiva a prestazioni pubbliche, al pari dell'istruzione, della sanità e della previdenza Altri studiosi ancora qualificano l'accesso come diritto fondamentale di rango costituzionale o, addirittura, come diritto umano. P. OTRANTO, LCRAZ, *La garanzia di accesso alla rete e la "città connessa"*, in *Riv. giur. ed.*, 2021, 77.

[36] La locuzione "cittadinanza digitale" identifica una nuova configurazione dei diritti dei cittadini nei confronti delle istituzioni, resa possibile dalle nuove tecnologie. Si tratta dell'evoluzione del concetto di cittadinanza nella realtà digitale, una visione dinamica come lo sviluppo delle tecnologie e, allo stesso tempo, indivisibile nei diritti che vuole definire. G. DUNI, *L'e-Government: dai decreti delegati del marzo 2005 ai futuri decreti entro il 9 marzo 2006*, in *Dir. internet*, 2005, 228.

la propria identità digitale (art. 3 *bis*); l'effettuazione dei pagamenti spettanti a qualunque titolo attraverso sistemi di pagamento elettronico; la partecipazione democratica elettronica finalizzata a favorire l'uso delle nuove tecnologie per facilitare la partecipazione dei cittadini al procedimento democratico con l'esercizio dei diritti civili e politici (art. 9); nonché l'istituzione della figura del difensore civico a garanzia dei diritti digitali di cittadini e imprese (art.17, comma 1-*quater*)[37].

Parimenti, ma con diversi strumenti, il legislatore si è preoccupato di superare il divario digitale di primo livello (*divide* che sottolinea la disparità di trattamento tra le persone che hanno accesso a Internet e coloro che non vi hanno accesso) con gli investimenti nella cosiddetta banda larga. L'articolo 13 *bis* del decreto-legge 18 ottobre 2012, n. 179, infatti, stabilisce che lo Stato riconosce l'importanza del superamento del divario digitale, soprattutto nelle aree depresse del Paese, ai fini della libera diffusione della conoscenza fra i cittadini, l'accesso pieno e aperto alle fonti di informazione e agli strumenti di produzione del sapere. A tale scopo promuove una sorta di Carta di diritti, nella quale sono definiti criteri volti a garantire l'accesso universale della cittadinanza alla rete Internet, senza alcuna discriminazione o forma di censura.

Il Codice dell'amministrazione digitale, dunque, seppur centrale nell'analisi dell'evoluzione dei diritti che compongono la cittadinanza digitale, è inscindibile dalla normativa sulla trasparenza, contenuta nel d.lg. 14 marzo 2013, n. 33, modificato dalla profonda riforma del d.lg. 25 maggio 2016, n. 97. La connessione tra le due direttrici di riforma della pubblica amministrazione, costituite dalla digitalizzazione e dalla trasparenza, deriva dalla centralità assunta dai dati, che a sua volta esige la protezione dei medesimi ad opera del regolamento (UE) 2016/679 e dal d.lg. 30 giugno 2003, n. 196, emendato dal d.lg. 10 agosto 2018, n. 101. Pertanto, se il Codice dell'amministrazione digitale si pone come la fonte normativa principale della cittadinanza digitale e dei diritti che fondano il rapporto fra istituzioni e cittadini, i diritti digitali afferenti alla "persona" trovano allocazione in provvedimenti normativi diversi[38].

Sul *digital divide* si sono soffermati anche alcuni Giudici di merito, *ante litteram*, mettendo in risalto l'importanza che lo strumento tecnologico interattivo ha ormai assunto nella quotidianità.

Significativa la vicenda portata all'attenzione del Giudice di Pace di Trieste, riguardante un episodio molto comune: una nota compagnia telefonica, a causa di disservizi non ben precisati, lasciò una famiglia, costituita da madre e tre figli studenti, senza linea telefonica e ADSL per circa quattro mesi. Dopo un tentativo di conciliazione presso il Corecom, non andato a buon fine, l'attore citò in giudizio la compagnia telefonica, chiedendo il risarcimento del danno. Il Giudice adito, con sentenza n. 587 del 18 luglio 2012[39], ha ritenuto, innanzitutto, che la compagnia telefonica dovesse rispondere per inadempimento *ex* art. 1218 c.c., nonché per violazione dell'art. 2 della Costituzione, richiamando il canone della buona fede oggettiva e correttezza

[37] Per ulteriori approfondimenti, v. G. PASCUZZI, *La cittadinanza digitale. Competenze, diritti e regole per vivere in rete*, Bologna, 2021, 113

[38] F. FAINI, *Il volto dell'amministrazione digitale nel quadro della rinnovata fisionomia dei diritti in rete*, in *Dir. inf.*, 2019, 1099.

[39] Giud. Pace Trieste, 18 luglio 2012, n. 587, in *Pluris online*.

nell'adempimento delle obbligazioni e, *in secundis*, in totale accoglimento del *petitum*, ha condannato la compagnia telefonica convenuta a risarcire anche il danno esistenziale «per le ovvie difficoltà di far fronte alle quotidiane necessità per i rapporti familiari e nei confronti di ogni altro interlocutore esterno». L'inadempimento della compagnia telefonica, sebbene non avesse inciso sulla salute, intesa in senso stretto, della parte attrice, ha reso alquanto difficoltoso lo svolgimento delle quotidiane attività, comportando un'apprensione angosciosa che ha turbato fortemente la sfera emotiva e relazionale dell'interessata. Suffraga la condanna il riferimento non bene precisato ad una giurisprudenza da tempo orientata a ritenere che il distacco o il mancato allaccio della linea telefonica a *internet* costituiscano un danno patrimoniale ed esistenziale per il titolare del contratto e della sua famiglia, danno considerato particolarmente grave in un'epoca in cui la comunicazione è fondamentale in ogni aspetto della vita quotidiana.

A fronte del riconoscimento della diseguaglianza digitale che ha dovuto sopportare la suddetta famiglia per l'inadempimento della compagnia telefonica, dato che senza *internet* le attività quotidiane possono risultare gravemente pregiudicate fino a raggiungere la soglia del danno esistenziale, ci si chiede quale potrebbe essere la norma applicabile a tutela dei soggetti vulnerabili della *smart city*, luogo ideale per l'implementazione delle politiche europee volte alla realizzazione di un'Europa intelligente, sostenibile ed inclusiva. La *smart city* è un modello economico caratterizzato dall'integrazione tra strutture e mezzi tecnologicamente avanzati, proiettata verso politiche di crescita sostenibile finalizzati a migliorare gli *standard* qualitativi della vita umana[40]. La città intelligente si propone di offrire servizi educativi, culturali, sociali e, soprattutto, abitativi, finalizzati a una maggiore coesione sociale; servizi il cui accesso non sarà agevole per la varietà dei bisogni di coloro che vivono nei contesti urbani contemporanei (*users*, consumatori, *prosumers*, turisti, lavoratori di passaggio e, soprattutto, categorie di soggetti vulnerabili, quali migranti, bambini e anziani), generando significative sperequazioni. Sono, infatti, come si è avuto modo di descrivere, proprio le diffuse situazioni di ineguaglianza, soprattutto delle categorie vulnerabili, a costituire il maggiore ostacolo alla concreta applicazione delle nuove tecnologie nelle realtà urbane[41].

Tale problematica, con riguardo in particolare alle categorie deboli[42], è stata un po' anticipata dalla pandemia da Coronavirus che abbiamo vissuto. Il covid 19, infatti, ha imposto un nuovo approccio tecnologico, sia in ambito lavorativo,

---

[40] E. FERRERO, *Le smart cities nell'ordinamento giuridico*, in *Foro amm.*, 2015, 1267.

[41] T. FAVARO, *Verso la smart city: sviluppo economico e rigenerazione urbana*, in *Riv. giur. ed.*, 2020, 87.

[42] Negli scorsi mesi, in tutto il mondo si sono sollevate polemiche attorno alle misure governative di contenimento del Covid-19 che hanno limitato alcune libertà individuali. Il dibattito che ne è derivato ha finito per mettere in evidenza la crisi in cui attualmente versano i diritti fondamentali della persona, i quali, soprattutto nelle moderne reti telematiche, risultano sistematicamente violati con buona pace degli ordinamenti giuridici, e con la conseguenza che attualmente si dà per scontato che *on-line* i dati personali siano saccheggiati e i diritti fondamentali violati senza che nessuno ne risponda. In questo contesto è proliferato il c.d. "Capitalismo della Sorveglianza"; tuttavia, i tempi sembrano oramai maturi per una decisa inversione di rotta, che deve necessariamente passare, tanto per cominciare, attraverso l'erosione, eventualmente anche solo per via pretoria, del principio di sostanziale deresponsabilizzazione dei *provider* di *Internet* garantita, ancora sino ad oggi, dalla direttiva 2000/31/CE. F. DI CIOMMO, *COVID-19 e crisi dei diritti fondamentali della persona: le responsabilità della responsabilità civile*, in *Danno resp.*, 2020, 3, 309

con lo *smart working*, sia nell'istruzione scolastica e universitaria (con l'introduzione di lezioni a distanza), costringendo lavoratori, studenti e professionisti ad adattarsi all'uso di *Pc* e *tablet*, divenuti strumenti indispensabili di lavoro e di apprendimento, con grave nocumento per bambini, anziani, disabili e meno abbienti, analfabeti digitali di ritorno.

Lo Stato italiano nella pandemia è intervenuto in più occasioni per ottemperare il *surplus* di *digital divide*, dovuto all'emergenza, per le categorie svantaggiate. Il decreto-legge c.d. "Cura Italia" (dl 17 marzo 2020, n. 18), diretto ad evitare che gli effetti del *virus* sull'economia reale si trasferissero sulle famiglie con il potenziamento del sistema sanitario, la sospensione delle scadenze delle imposte e dei contributi previdenziali ed assistenziali, ha fornito un notevole impulso alla digitalizzazione dell'istruzione. In particolare, per gli studenti privi di mezzi e in situazione di svantaggio socio-economico[43], l'art. 120 ha stanziato settanta milioni di euro per far acquistare alle scuole (in maniera semplificata e tempestiva, *ex* art. 75), in base al numero degli studenti e al reddito medio della regione, dispositivi elettronici da fornire in comodato d'uso agli studenti privi di mezzi e in situazione di precarietà sociale.

Sempre in tale ottica, per sostenere la digitalizzazione e per combattere il *digital divide* di primo livello, è stato emanato Il Decreto Banda ultralarga – "Piano Scuola" e "Piano voucher famiglie", Decreto 7 agosto 2020 – Piano voucher sulle famiglie a basso reddito. L'agevolazione riguardava famiglie e imprese affinché si dotassero di strumenti tecnologici che fossero in grado di avvicinare tutti, anche coloro che si trovassero in difficoltà economica, ad un minimo livello di benessere "tecnologico". Il Ministero dello sviluppo economico ha promosso, dunque, il "Piano voucher per le famiglie meno abbienti" per garantire la fruizione di servizi di connessione a *internet* in banda ultra-larga.

Alla luce dei provvedimenti emanati in piena pandemia, non rimane che da domandarsi, superata ormai l'emergenza, come il diritto privato potrà promuovere e tutelare i diritti dei vulnerabili digitali nella fruizione dei servizi offerti dalle città tecnologiche. Sembra rispondere a tali interrogativi proprio la Dichiarazione europea dei princípi e dei diritti digitali (Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali 26.1.2022 COM (2022)27). La Carta si propone di promuovere una trasformazione digitale antropocentrica, fondata su solidarietà, inclusione, libertà di scelta, partecipazione allo spazio pubblico digitale, sicurezza e sostenibilità. La dichiarazione riconosce l'importanza dei valori di solidarietà e di inclusione (Capo II), che si traduce nell'impegno a garantire l'accesso alla connettività digitale ad alta velocità e a prezzi accessibili; il diritto all'istruzione e alla formazione; l'accesso ai servizi pubblici *online* di tutta l'Unione, attraverso una identità digitale europea; l'accessibilità alle informazioni della p.a.; l'accesso ai servizi sanitari e assistenziali digitali. Al riconoscimento di tali diritti fa da contrappeso il successivo Capo III, dedicato all'Intelligenza Artificiale, che sancisce l'impegno

[43] G. PESCI, *Il digital divide, l'uguaglianza sostanziale e il diritto all'istruzione*, in *Cyber spazio dir.*, 2021, 259.

delle Istituzioni ad assicurare il rispetto dei diritti fondamentali nell'impiego delle nuove tecnologie, assicurandone un uso trasparente e non discriminatorio, garantendo la supervisione umana dei risultati concernenti la persona.

La Dichiarazione sembra, dunque, da un lato, ampliare il novero delle pretese già riconosciute nell'ordinamento interno dal Codice dell'Amministrazione digitale, dall'altro, creare nuovi diritti, che spesso si sovrappongono a quelli già pacificamente riconosciuti dalla Carta Europea dei diritti fondamentali, sebbene nella dimensione *on line*. Essa è documento politico, attraverso il quale l'UE mira ad esprimere la sua posizione sul tema della trasformazione digitale in atto, sprovvista di valore precettivo, ma che assume valore giuridico di *soft law*, in quanto fornisce materiale prezioso, funzionale alle strategie di argomentazione impiegate nell'interpretazione dei testi giuridici[44].

Conclusioni: Gli ETS quale strumento concreto del diritto privato per il superamento del digital divide e la promozione della persona nello spazio digitale.

A fronte delle innanzi esposte encomiabili dichiarazioni di intenti, ci si domanda di quali strumenti possa disporre il diritto privato per realizzare in concreto tali diritti digitali, attenuando il *digital divide* e preservando la persona in un mercato caratterizzato da un profondo clima di incertezza economica e sociale.

Un ruolo determinante potrebbe essere rivestito dalle organizzazioni aventi natura ideale (associazioni riconosciute e non, fondazioni e comitati), nonché dagli enti del terzo settore[45]. Enti che già rivestono nella Costituzione una posizione tutt'altro che marginale in virtù del principio di sussidiarietà orizzontale (*ex* art. 118 Cost.), e che sono il centro del sistema del d.lg. 3 luglio 2017, n. 117 (Codice del Terzo settore). Sono, infatti, enti del Terzo settore (ETS) le organizzazioni che svolgono attività di interesse generale in via esclusiva o principale per il perseguimento, senza scopo di lucro, di finalità civiche, solidaristiche e di utilità sociale (art. 4, comma 1, c.t.s.). Il legislatore, nel definire tali enti ed istituire il Registro unico nazionale del Terzo settore (su cui si annotano tutti gli eventi relativi all'ente, dalla costituzione all'estinzione), specifica quali siano le attività di interesse generale che caratterizzano gli enti del Terzo settore, fornendo, finalmente, una legislazione organica alle organizzazioni non profit. Il tutto si pone in linea con il principio di solidarietà sociale già espresso in àmbito costituzionale, che vede il favore dello Stato nei confronti delle iniziative dei privati che svolgano attività di interesse generale attraverso le formazioni sociali (artt. 2, 18 Cost.), più di altre adatte a soddisfare i bisogni del territorio, grazie alla conoscenza del contesto sociale e alla maggiore flessibilità organizzativa.

Dato che gli Ets hanno come elemento distintivo e qualificante lo svolgimento di attività di interesse generale, bisogna verificare se

[44] E N. FRAGALE, *La cittadinanza amministrativa al tempo della digitalizzazione*, in *Dir. amm.*, 2022, 2, 471.
[45] Per una trattazione esaustiva e recente in proposito, v. A. FUSARO, *Gli enti del Terzo settore. Profili civilistici*, in *Tratt. dir. civ. comm. Cicu Messineo*, Milano, 2022, *passim*.

l'alfabetizzazione digitale possa ricomprendersi nell'elenco delle diverse tipologie di attività tassativamente previste dall'art. 5 Cts, soggetto ad aggiornamento periodico ad opera del Presidente del Consiglio dei Ministri. Poichè non possono essere enti del Terzo settore le amministrazioni pubbliche, le formazioni e le associazioni politiche, i sindacati, le associazioni professionali, di categoria, le fondazioni bancarie, nonché gli enti sottoposti a loro coordinamento o controllo (fatti salvi gli enti di protezione civile), l'attività di alfabetizzazione digitale può essere compiuta dall'Ets in quanto rientra, senz'altro, nell'art. 5. In particolare, se pensiamo al *digital divide* di secondo livello, ossia all'esclusione generata dal mancato possesso delle competenze specifiche necessarie all'uso di tali tecnologie [46], l'insegnamento delle competenze digitali è rinvenibile nella lett. d), in riferimento all'educazione, istruzione e formazione professionale, nonché nelle attività culturali di interesse sociale con finalità educativa; nella i), relativamente all'organizzazione e gestione di attività culturali, artistiche o ricreative di interesse sociale, incluse attività, anche editoriali, di promozione e diffusione della cultura e della pratica del volontariato e delle attività di interesse generale di cui all'art. 5; nonché, infine, facendo riferimento al *digital divide* di primo livello (ossia alla già menzionata disparità tra le persone che hanno accesso a internet e le persone che ne sono prive), nella lett. w), in cui si promuovono e tutelano i diritti umani, civili, sociali e politici, se consideriamo l'accesso ad *internet* come un diritto sociale, ossia una pretesa soggettiva a prestazioni pubbliche, al pari dell'istruzione, della sanità e della previdenza, che siano in grado di ridurre i fattori culturali e tecnologici che determinano le disuguaglianze[47].

Il ruolo determinante che può essere svolto dagli Ets per il superamento del *digital divide*, alla luce del citato principio di sussidiarietà e del rapporto tra quest'ultimo e i principi di solidarietà ed uguaglianza, sembra ampiamente suffragato da una recente pronuncia della Corte costituzionale [48], che si sofferma ampiamente sul ruolo che assume l'art. 55 del Codice del terzo settore, il quale, «disciplinando i rapporti tra ETS e pubbliche amministrazioni, rappresenta dunque una delle più significative attuazioni del principio di sussidiarietà orizzontale valorizzato dall'art. 118, quarto comma, Cost.». In particolare, l'art. 55 CTS individua dapprima i principi cardine ai quali devono attenersi le amministrazioni pubbliche nell'esercizio delle proprie funzioni, in sede di amministrazione condivisa, avuto riguardo ai settori di attività che vedono il coinvolgimento degli enti del terzo settore e di poi, a séguito del riferimento iniziale al richiamato principio, delinea gli strumenti reputati idonei per rendere concreto il predetto coinvolgimento, espressione e attuazione del principio medesimo, identificandoli nella co-programmazione, nella co-progettazione e nell'accreditamento. Tali nuovi strumenti vengono rapportati a tutte le attività di interesse generale elencate nell'art. 5, tra cui, come

[46] V. G. PASCUZZI, *La cittadinanza digitale*, cit., p. 38.
[47] Per una articolata ricostruzione intesa a radicare nelle norme costituzionali un "nuovo diritto sociale" di accesso a internet, o meglio, di accesso alla conoscenza "tramite internet", v. M.T.P. CAPUTI JAMBRENGHI, *La funzione amministrativa neutrale*, Bari, 2017, 292-296. *A contrario* P. TANZARELLA, *L'accesso a Internet è fondamentale, ma è davvero un diritto fondamentale?*, in *Riv. dir. media*, 2021, 55, che considera l'accesso a *internet* come un servizio essenziale, e non come un diritto fondamentale.
[48] Corte cost., 26 giugno 2020, n. 131, in *Foro it.*, 2021, 365.

delineato, può essere annoverata, sebbene non esplicitamente prevista, anche l'attività di alfabetizzazione digitale, aspetto preminente per la soddisfazione di interessi generali con un modello di amministrazione condivisa, in grado di produrre effetti strettamente collegati ai valori fondanti della persona[49].

Si potrebbe sul punto affermare, in conclusione, che proprio perché la Corte costituzionale ha la funzione non solo di interpretare la legge, ma anche di scegliere tra i diversi significati del testo in sede di applicazione, la prospettata sentenza potrebbe rappresentare il riferimento interpretativo più coerente dal punto di vista sistematico alla soluzione *de iure condendo* prospettata.

A fronte, dunque, della consapevolezza dell'esistenza del *digital divide*, il giusprivatista, alla luce dell'art. 3 della Costituzione, ritrova i rimedi per attenuare gli effetti discriminatori che, di fatto, derivano dal fenomeno del massiccio uso delle tecnologie, negli Ets, che possono rivestire l'importante ruolo di restituire ad ogni persona, calata nell'attuale mondo digitale, il rilievo che le compete e assicurare a tutti pari dignità, obiettivo ineludibile in un sistema positivo preordinato alla tutela del pieno sviluppo della persona umana.

Gli enti del Terzo settore, potranno, dunque, contribuire in modo decisivo all'inclusione dei vulnerabili nelle città intelligenti, che dovranno diventare dimensione di condivisione e non di esclusione, appannaggio non solo di coloro che hanno accesso alle nuove tecnologie, ma anche delle categorie umane più deboli, con il superamento del *digital divide*, che costituisce una precondizione fondamentale nella prospettiva di riscrivere e rafforzare i diritti e le tutele dell'era digitale della società del futuro.

[49] V. M.C. PERCHIUNNO, *Enti del terzo settore, sussidiarietà e uguaglianza*, in *Contr. impr.*, 2021, 1048.

Di Lella F, 'Identità e destino degli embrioni soprannumerari. Ipotesi *de iure condendo*' (2022) 2 EJPLT, 84-98.
DOI : https://doi.org/10.57230/EJPLT222FDL

EJPLT
ISSN 2704-8012

Identità e destino degli embrioni soprannumerari. Ipotesi *de iure condendo.*

Identity and fate of supernumerary embryos. De iure condendo hypothesis.

FRANCESCA DI LELLA
Ricercatrice di Diritto privato, docente di Biodiritto
Università degli Studi di Napoli Federico II

Abstract

I progressi nel campo della medicina della riproduzione hanno portato al centro della scena una nuova entità: l'embrione in vitro. La ricostruzione della sua identità giuridica è preliminare alla ricerca di soluzioni per una delle questioni più delicate che attualmente animano il dibattito biogiuridico, e cioè quella concernente il destino degli embrioni in soprannumero. Il contributo ripercorre, in breve, gli apporti alla discussione forniti dalla dottrina e dalla giurisprudenza nazionale ed europea, per soffermarsi poi su alcune proposte oggetto di studio, esaminandone potenzialità e criticità.

Advances in the field of reproductive medicine have brought a new entity to centre stage: the in vitro embryo. The reconstruction of its legal identity is preliminary to the search for solutions to one of the most sensitive issues currently animating the biojuridical debate, namely the fate of supernumerary embryos. This essay briefly traces the contributions to the debate made by doctrine and national and European jurisprudence, and then dwells on some of the proposals under study, examining their potential and critical aspects.

© The author(s) 2022, 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: vulnerable subjects; reproductive technologies; human embryos.

Summary: Introduzione. – 1. La natura giuridica dell'embrione, tra *res* e persona. Il quadro legislativo. – 2. L'apporto al dibattito della giurisprudenza nazionale ed europea. Cenni. – 3. Gli embrioni crioconservati: le attuali categorie e le incertezze circa la sorte dei soprannumerari. – 4. Le prospettive *de iure condendo*: l'adozione per la nascita e la destinazione alla ricerca scientifica. – Conclusioni.

Introduzione.

L'ultima relazione del Ministro della Salute al Parlamento sullo stato di attuazione della legge n. 40 del 2004, presentata nel settembre del 2022[1], dà conto del numero degli embrioni formato nell'anno 2020, a séguito dell'applicazione di tecniche di procreazione medicalmente assistita di secondo e di terzo livello, quelle per le quali, cioè, l'unione dei gameti avviene al di fuori del corpo della donna. Del numero complessivo di essi, il 43,2% è stato trasferito a fini di gravidanza, mentre il restante 56,8% (pari a 42.532 embrioni) risulta crioconservato[2].

Invero, per un censimento completo della popolazione degli embrioni attualmente in stato di crioconservazione, al dato su riferito – che è preso in considerazione solo a fini indicativi – andrebbe addizionato quello degli anni precedenti. Tuttavia, è possibile effettuarne una stima soltanto approssimativa, sia per le difficoltà nel reperire informazioni precise nei centri di medicina della riproduzione, sia perché gli embrioni conteggiati negli anni passati potrebbero poi essere periti oppure essere stati utilizzati per nuove gravidanze. Non vi sono, dunque, dati ufficiali al riguardo, ma di certo il numero totale degli embrioni crioconservati è esponenzialmente cresciuto negli anni, in séguito a ben noti interventi della Consulta, modificativi di aspetti rilevanti della legge n. 40/2004. In ogni caso, non sarebbe possibile distinguere con precisione tra quelli ancóra vitali e destinabili a un impianto e quelli c.dd. soprannumerari, perché "abbandonati" dalla coppia di genitori o comunque "scartati", in quanto di qualità non buona ai fini di un positivo esito di gravidanza oppure affetti da patologie riscontrate tramite diagnosi genetica pre-impianto.

Al di là, dunque, dell'individuazione del numero esatto – certamente non esiguo – degli embrioni attualmente congelati, sembra non più eludibile la questione della sorte di quelli in soprannumero, soprattutto ove si consideri il riconoscimento, avvenuto in molteplici sedi, della ‹‹dignità umana›› della quale sono portatori. Nondimeno, il problema involge aspetti, certamente più prosaici, di sostenibilità dell'attuale sistema sotto un profilo non solo economico e organizzativo, ma anche ambientale, che si pongono in contrasto

[1] Consultabile in *www.salute.gov.it*.
[2] *Ivi*, p. 8. Le cifre sono riferite alle procedure con gameti della coppia richiedente, con esclusione delle tecniche con gameti donati.

con una preservazione *sine die* della vita nascente, racchiusa in ogni singolo embrione.

1. La natura giuridica dell'embrione, tra res e persona. Il quadro legislativo.

La messa a punto e il progressivo affinarsi di tecnologie mediche in grado di risolvere o, comunque, di superare patologie legate alla sfera riproduttiva[3] hanno fatto emergere nel tempo la necessità di comprendere quale fosse la natura giuridica dell'embrione umano e di definirne lo statuto[4].

Sul piano giusprivatistico, si è inizialmente impostato il confronto con le categorie della tradizione e, dunque, si è cercato soprattutto di verificare la tenuta della nozione di capacità giuridica rispetto alla nuova entità. La regola codicistica, ai sensi della quale l'acquisto della capacità giuridica è ancorato al momento della nascita, emanata in un'epoca storica in cui non esistevano le tecniche della procreazione assistita, non è in grado di riflettere la realtà degli embrioni *in vitro*[5]. Questi ultimi non risultano inquadrabili né nella nozione civilistica di soggetto di diritto dotato di capacità giuridica (art. 1, co. 1, c.c.), né in quella di concepito destinatario potenziale di diritti, l'acquisto dei quali è subordinato all'evento della nascita (art. 1, co. 2, c.c.), poiché le norme del codice civile che fanno riferimento a tale categoria chiaramente alludono al frutto del concepimento inserito nel grembo materno[6]. Né, tantomeno, possono essere accostati al nascituro non concepito, figlio di genitori individuati, essendo essi già il risultato dell'unione e della fusione dei gameti maschile e femminile, seppure avvenute in una provetta. Gli embrioni *in vitro* sembrano vivere, insomma, in una sorta di limbo definitorio ed essere – a voler forzare in qualche modo gli schemi della tradizione – dei concepiti non (necessariamente) nascituri.

La diffusione delle tecniche di procreazione assistita porta con sé, pertanto,

---

[3] Per uno sguardo d'insieme alle varie problematiche sollevate dall'impatto delle innovazioni della biologia e della medicina riproduttiva sul diritto, v. A. GORASSINI, *Procreazione (dir. civ.)*, in *Enc. dir.*, XXXVI, Milano, 1987, p. 957 ss.; M. FACCIOLI, *Procreazione medicalmente assistita*, in *Dig. Disc. priv.*, *Sez. civ.*, *Agg.*, III, Torino, 2007, p. 1051 ss.; più di recente, U. SALANITRO, *Procreazione assistita (dir. civ.)*, in *Enc. dir.*, *I Tematici*, IV, *Famiglia*, diretto da F. Macario, Milano, 2022, p. 1015 ss.

[4] Esigenza sentita su di un piano più complesso e interdisciplinare, attese le evidenti implicazioni bioetiche: cfr. il documento *Identità e statuto dell'embrione umano*, 22 giugno 1996, reso dal Comitato Nazionale per la Bioetica e reperibile in *bioetica.governo.it*. Per un approccio più strettamente inerente ai profili etici, v. L. LOMBARDI VALLAURI, *L'embrione e le vite diversamente importanti*, in S. RODOTÀ (a cura di), *Questioni di bioetica*, Roma-Bari, 1993, p. 361 ss.; v., inoltre, L. FERRAJOLI, *Diritti fondamentali e bioetica. La questione dell'embrione*, in S. RODOTÀ e M. TALLACCHINI (a cura di), *Ambito e fonti del biodiritto*, nel *Trattato di biodiritto*, diretto da S. Rodotà e P. Zatti, I, Milano, 2010, p. 241 ss.

[5] Invero, per vari decenni dopo l'emanazione del codice civile, finché le tecniche della procreazione un tempo definita "artificiale" erano state non ancóra concretamente attuate ma solo ipotizzate, lo sporadico interesse della dottrina si era focalizzato sul riscontro di un vuoto normativo rispetto al fenomeno di un concepimento scisso dall'unione sessuale della coppia, sulla liceità della pratica e sulla ricerca di soluzioni rispetto alle ricadute sul piano dei rapporti di filiazione: v. A. TRABUCCHI, *Inseminazione artificiale (Diritto civile)*, in *Novissimo Dig. It.*, VIII, Torino, 1968, p. 732 ss. Dai distinguo terminologici, che pure hanno interessato gli interpreti nella prima fase della riflessione, iniziò a profilarsi, sebbene in maniera assai sfumata, quell'‹‹embrione altrove determinatosi››, senza che però potessero essere ancóra colte le implicazioni della sua esistenza: le parole virgolettate sono di V. LOJACONO, *Inseminazione artificiale*, in *Enc. dir.*, XXI, Milano, 1971, p. 753.

[6] Le norme del codice civile, inoltre, fissano – a vari effetti – la presunzione di concepimento e distinguono il concepito dal nascituro non concepito, figlio di una determinata persona vivente.

l'esigenza di ricercare una disciplina per una realtà materiale del tutto nuova, da confrontare – per individuare le più opportune tutele da apprestare – anche con la distinzione tra *res* e persona. Il problema se l'embrione dovesse essere considerato alla stregua di un mero prodotto organico o essere tutelato come il frutto del concepimento, potenziale iniziatore della vita umana, ha così animato la discussione[7]. Fin dalle prime riflessioni al riguardo è dato registrare che esso non viene assimilato a puro materiale biologico, dunque a una *res*, della quale sia consentito disporre secondo la consueta ottica delle vicende circolatorie dei diritti sui beni[8].

Ad avvalorare quanto si è sinora osservato sono intervenuti provvedimenti legislativi che, pur senza elevare l'embrione alla qualifica di vero e proprio soggetto di diritto, lasciano intendere chiaramente la necessità di apprestare alla nuova entità forme di protezione adeguate alla condizione di estrema vulnerabilità in cui obiettivamente versa. In questa direzione, sono state lette, pur nella varietà delle opinioni espresse, le disposizioni contenute nella legge sulla interruzione volontaria della gravidanza e, poi, in quella sulla procreazione medicalmente assistita[9], laddove si ritrova – nei rispettivi *incipit*[10], ma anche

[7] Restano, al riguardo, scolpite le parole di C.M. Bianca, *Diritto civile*, I, *La norma giuridica - I soggetti,* II ed., Milano, 2002, p. 224 s., per il quale «in mancanza di una disciplina normativa della materia l'interprete deve attenersi al principio generale di tutela della vita umana fin dal suo inizio e adottare le soluzioni volte a salvaguardare l'embrione e la sua naturale destinazione».

[8] Cfr., tra i primi AA., A. Trabucchi, *Procreazione artificiale e genetica umana nella prospettiva del giurista*, in *Riv. dir. civ.*, 1986, I, p. 507 s., per il quale il rispetto della vita racchiusa nell'embrione, che già reca l'impronta dell'uomo, impone di escludere in radice la possibilità di distruzione, sperimentazione o manipolazione dello stesso, e richiede un regolamento che impedisca che possa essere considerato come ‹‹cosa di nessuno›› o come ‹‹oggetto di proprietà privata dei generanti››. Del resto, l'intersezione tra il piano dell'essere e quello dell'avere era inevitabile nell'approccio ai tentativi di individuazione della natura giuridica dell'embrione e della definizione del suo statuto: v. A. Gorassini, *Procreazione (dir. civ.)*, cit., p. 961 s. Per la collocazione dell'embrione tra le "persone", seppure *in fieri*, in quanto entità umana a prescindere dal grado di sviluppo, v., *ex multis*, G. Oppo, *L'inizio della vita umana*, in *Riv. dir. civ.*, 1982, I, p. 499 ss., spec. p. 512; P. Zatti, *Quale statuto per l'embrione?*, in *Riv. crit. dir. priv.*, 1990, p. 463; G. Oppo, *Scienza, diritto, vita umana*, in *Riv. dir. civ.*, 2002, p. 17 ss.; F. Santosuosso, *La procreazione medicalmente assistita. Commento alla legge, 19 febbraio 2004 n. 40*, Milano, 2004, p. 87; F. Gazzoni, *Osservazioni non solo giuridiche sulla tutela del concepito e sulla fecondazione artificiale*, in *Dir. fam. pers.*, 2005, p. 182 ss.; V. Scalisi, *Lo statuto giuridico dell'embrione umano alla luce della legge n. 40 del 2004, in tema di procreazione medicalmente assistita*, in *Fam. dir.*, 2005, p. 203 ss.; P. Schlesinger, *Il concepito e l'inizio della persona*, in *Riv. dir. civ.*, 2008, p. 247 ss.; di recente, P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, III, *Situazioni soggettive*, 4° ed. rived. e ampl., Napoli, 2020, p. 76, per il quale ‹‹potrà qualificarsi "embrione" solamente un complesso di cellule in grado di differenziarsi potenzialmente in tutti i tessuti e in tutti gli organi costitutivi». Per una prospettiva diversa, v. C.M. Mazzoni, *La tutela reale dell'embrione*, in *Nuova giur. civ. comm.*, 2003, II, p. 457 ss., che riconduce l'embrione al ‹‹mondo delle cose››, seppure viventi e umane, di giuridica rilevanza, negandone perciò l'appartenenza al mondo della soggettività giuridica, ma precisa che ciò non equivale a depotenziarne la tutela quale protezione effettiva e concreta dell'embrione nel suo significato ontologico. Tale tutela, a parere dell'A., si ricava dalle norme costituzionali, segnatamente dagli artt. 31 e 32, in un sistema nel quale la garanzia dei valori protetti può essere indipendente dalla titolarità dei diritti, sì che l'embrione – inteso come materiale umano vivente, come corpo che per un tratto fa parte del corpo della madre – può restare sul piano dell'oggetto della tutela (*ivi*, p. 465). Analoghe conclusioni in G. Cricenti, *Breve critica alla soggettività del concepito. I "falsi diritti" del nascituro*, in *Dir. fam. pers.*, 2010, p. 465 ss.

[9] Per le prime reazioni suscitate, cfr. *ex multis*, M. Marella, *Esercizi di biopolitica*, in *Riv. crit. dir. priv.*, 2004, p. 3 ss.; M. Sesta, *Dalla libertà ai divieti: quale futuro per la legge sulla procreazione medicalmente assistita?*, in *Corr. giur.*, 2004, p. 1407 s.; R. Villani, *Procreazione assistita*, in *Tratt. dir. fam.*, diretto da P. Zatti, VII, *Agg.*, Milano, 2006, p. 262 ss.

[10] La legge sulla interruzione volontaria della gravidanza (l. n. 194/1978) proclama la tutela della vita umana "dal suo inizio" (art. 1): in maniera più netta, la legge sulla procreazione medicalmente assistita (l. n. 40/2004) indica tra le sue finalità la tutela dei diritti di "tutti i soggetti coinvolti, compreso il concepito" (art. 1). Sul punto, cfr. F.D. Busnelli, *L'inizio della vita umana*, in *Riv. dir. civ.*, 2004, p. 533 ss. Per una lettura critica alla

nell'articolato normativo[11] – un richiamo forte all'esigenza di tutelare il frutto del concepimento e a favorire, per quanto possibile, la sua fisiologica evoluzione verso la vita[12]. Quanto al metodo, va notato che gli interventi del legislatore non prescindono da premesse di tipo assiologico circa la natura dell'embrione/feto, dalla quale fanno discendere le conseguenze sul piano giuridico; mentre rifuggono da un approccio di carattere più pragmatico, teso a ricercare soluzioni ragionevoli e applicabili in concreto più che a perseguire obiettivi ideali[13].

Sulla scorta delle suesposte premesse, si è aperta la strada a una rimeditazione della stessa "soggettività" come nozione più ampia, non combaciante con quella di capacità giuridica[14], e si è iniziato a vedere nella nascita l'evento dal quale dipende il riconoscimento, generale e egualitario, della titolarità dei diritti, patrimoniali e non, spettanti al soggetto, senza che ciò implichi *a contrario* una esclusione del non nato da taluni di quei diritti[15]. In verità, come è stato osservato, il dibattito finisce per confermare l'incapacità delle tradizionali categorie dogmatiche a cogliere la fisionomia giuridica dell'embrione umano, entità sospesa tra diritto e scienza e non inquadrabile nell'àmbito della rigida dicotomia tra *res* e *personae*[16], e si allinea a una

legge sulla p.m.a. e, in particolare, al suo art. 1, v. N. LIPARI, *Legge sulla procreazione assistita e tecnica legislativa*, in *Riv. trim. dir. proc. civ.*, 2005, p. 517 ss.

[11] Basti ricordare che l'interruzione della gravidanza è legata alla sussistenza di presupposti, cronologici e fattuali, in mancanza dei quali la tutela del feto deve prevalere, e che sussiste in capo al medico che esegue l'intervento l'obbligo di salvaguardia della vita del feto che manifesti una possibilità di vita autonoma. Vale, inoltre, la pena di richiamare tutte le misure di tutela dell'embrione contenute nel Capo VI della l. n. 40/2004. Invero, non è sfuggito il diverso approccio delle due leggi richiamate: v. G. FERRANDO, *La nuova legge in materia di procreazione medicalmente assistita: perplessità e critiche*, in *Corr. giur.*, 2004, p. 811 ss. Nella prima di esse – le cui norme sono riferite al frutto del concepimento già immesso nel processo della gravidanza – è riflesso un bilanciamento tra interessi che vede prevalere, nel conflitto, la salute della donna a scapito della vita del concepito (principio ribadito da note sentenze della Consulta: Corte Cost., 18 febbraio 1975, n. 75, in *Foro it.*, 1975, I, c. 515 ss., e Corte Cost., 10 febbraio 1997, n. 35, *ivi*, I, c. 672 ss.). Nell'impianto originario della legge sulla p.m.a., invece, la tutela dell'embrione, prima ancóra del suo impianto in utero, appare assoluta e disvela l'intenzione del legislatore di considerarlo un soggetto di diritto al pari dei nati. Per l'opinione secondo cui è irrilevante, ai fini della protezione giuridica, che l'embrione sia "costruito" in provetta o si formi nell'utero e, quindi, la presenza di un rapporto intersoggettivo attuale con la madre, v. F. GAZZONI, *op. cit.*, p. 182. Specifica G. OPPO, *Diritto di famiglia e procreazione assistita*, in *Riv. dir. civ.*, 2005, p. 332 s., che l'embrione concepito fuori dal corpo della donna ha accesso alla protezione della vita umana, che importa il dovere di fargli iniziare e proseguire il percorso di vita secondo la sua destinazione naturale, e che solo con l'inizio della gravidanza gli si applica la disciplina civilistica del figlio nascituro, poiché ‹‹per il codice il concepito coincide con *qui in utero est*››.

[12] Cfr. G. OPPO, *Diritto di famiglia e procreazione assistita*, cit., p. 332; B. MASTROPIETRO, *Procreazione assistita: considerazioni critiche su una legge controversa*, in *Dir. fam. pers.*, 2005, p. 1385 ss.

[13] Sul punto, v. P. ZATTI, *Diritti dell'embrione e capacità giuridica del nato*, in *Riv. dir. civ.*, II, 1997, p. 107 s. Sull'utilizzo disomogeneo del termine embrione nei testi normativi e sulla scelta tecnica del legislatore italiano, anche nel confronto con altri ordinamenti, cfr. V. DURANTE, *La ‹‹semantica dell'embrione›› nei documenti normativi. Uno sguardo comparatistico*, in *Riv. crit. dir. priv.*, 2012, p. 63 ss.

[14] La tendenza era già segnalata da M. BESSONE-G. FERRANDO, *Persona fisica (dir. priv.)*, in *Enc. dir.*, XXXIII, Milano, 1983, p. 204 ss. Per una ricognizione delle ricostruzioni che si profilavano a proposito della capacità del concepito, v. P. RESCIGNO, *Capacità giuridica*, in *Dig. Disc. priv., Sez. civ.*, II, Torino, 1988, p. 221 s. Cfr., nel senso indicato nel testo, V. SCALISI, *op. cit.*, p. 206, per il quale la soggettività è la ‹‹categoria giuridica idonea a rispecchiare l'evoluzione biologica dell'individuo››; più di recente, M.G. CABITZA, *Lo statuto dell'embrione: tra dignità umana e progresso scientifico*, in *Dir. fam. pers.*, 2018, p.628 s. *Contra*, ossia sulla difficoltà di slegare la soggettività dalla capacità giuridica, cfr. G. OPPO, *Scienza, diritto, vita umana*, cit., p. 15; F. GAZZONI, *op. cit.*, p. 184 s.; B. MASTROPIETRO, *op. cit.*, p. 1384.

[15] In tal senso, P. ZATTI, *Diritti dell'embrione e capacità giuridica del nato*, cit., p. 109.

[16] Cfr. M.G. CABITZA, *op. cit.*, 2018, p. 621 ss., ove un'analisi dei testi normativi, nazionali e non, più significativi per supportare la tesi di una compatibilità del concetto di soggettività con le peculiarità proprie

prospettiva di protezione della vita prenatale, emergente anche dal contesto europeo e dall'interpretazione delle Corti sovranazionali[17].

Le sollecitazioni provenienti dal suddetto dibattito sono state raccolte anche dalla giurisprudenza[18], che si è allontanata dalla logica della *res*, e hanno offerto lo spunto per proposte di legge rafforzative dell'identità dell'embrione quale soggetto di diritto, con ciò che questo comporta sul piano degli effetti e delle tutele[19].

2. L'apporto al dibattito della giurisprudenza nazionale ed europea. Cenni.

La giurisprudenza nazionale ha fornito un contribuito decisivo per ricostruire la figura dell'embrione, sia quello immesso nel processo della gravidanza che quello giacente in vitro[20].

In particolare, la Corte Costituzionale, nei vari interventi di riscrittura della legge n. 40/2004 finalizzati a bilanciare i diversi interessi in gioco[21], ha sì affievolito la tutela assoluta dell'embrione originariamente accordata dal legislatore[22], per armonizzarla con altri interessi costituzionalmente protetti[23], ma non ha mai mancato di mettere in risalto come l'embrione sia da considerare quale principio iniziatore della vita, portatore della dignità umana, quandanche se eventualmente malformato, e soggetto estremamente vulnerabile, come

dell'embrione; nonché U. SALANITRO, *op. cit.*, p. 1017 ss., per una chiara sintesi delle posizioni sviluppatesi nel tempo sullo statuto soggettivo del concepito.

[17] Cfr. I. BARONE, *Dignità e sorte degli embrioni soprannumerari*, in *Juscivile.it*, 2021, 5, p. 1450 ss.

[18] V. *infra*, § 2.

[19] Cfr. il più recente disegno di legge, presentato al Senato lo scorso ottobre 2022, recante il n. 165, che riprende analoga proposta del Movimento per la vita italiano (atto Camera n. 2922 del 1995), diretto alla modifica dell'art. 1 del codice civile, nel senso di ancorare il riconoscimento della capacità giuridica al momento del concepimento, fermo restando che l'acquisto dei diritti patrimoniali resti subordinato all'evento della nascita.

[20] Anche prima dei numerosi interventi della giurisprudenza sulla legge n. 40/2004, che sono quelli decisivi ai fini dell'indagine, è possibile ritrovare provvedimenti tesi alla protezione dell'embrione *in vitro*: al riguardo, v. Trib. Palermo, ord. 8 gennaio 1999, in *Nuova giur. civ. comm.*, 1999, I, p. 221 ss., con nota di F.D. BUSNELLI, *La sorte degli embrioni* in vitro*: in assenza di regole, il ricorso ai principi*, ove si riconosce, alla stregua dei principi ricavabili dalla Costituzione e dall'intero sistema, l'esistenza di diritti fondamentali, *in primis* di quello alla vita, in capo all'embrione. Differente la posizione di Trib. Bologna, 26 giugno 2000, in *Nuova giur. civ. comm.*, 2001, I, p. 475 ss., con nota di C. FAVILLI, *Autodeterminazione creativa e diritti dell'embrione*, in cui il Giudice opera una distinzione tra gli embrioni crioconservati e quelli già allocati nell'utero materno, per riconoscere solo a questi ultimi la tutela legale offerta dall'ordinamento.

[21] Per un ampio esame della genesi e delle principali tappe che hanno scandito l'evolversi della legge e della sua applicazione concreta, si rinvia a F. ANGELINI, *Procreazione medicalmente assistita*, in *Dig. Disc. pubbl.*, *Agg.*, VI, Torino, 2015, p. 341 ss.; F. AZZARRI, *I quindici anni della legge 40: nemesi e questioni aperte nella disciplina della fecondazione assistita*, in *Familia*, 2019, p. 561 ss.; U. SALANITRO, *op. cit.*, *passim*.

[22] Va ricordata, *in primis*, Corte Cost., 8 maggio 2009, n. 151, in *Corr. giur.*, 2009, p. 1213 ss., con nota di G. FERRANDO, *Diritto alla salute della donna e tutela degli embrioni: la Consulta fissa nuovi equilibri,* che ha abolito il limite dei tre embrioni, inizialmente fissato dalla legge n. 40/2004, dichiarando l'incostituzionalità dell'art. 14, co. 2 e 3: di tal guisa, ha restituito al medico la possibilità di valutare, caso per caso, in base alle condizioni cliniche della donna e a una serie di altre variabili (età, patologie, cause della sterilità/infertilità etc.), quanti embrioni produrre per il buon esito del programma di p.m.a., potendo – se lo ritiene opportuno a tali fini – superare il limite di tre. La statuizione ha introdotto, come conseguenza, una deroga al divieto di crioconservazione posto dalla legge, per la necessità di procedere al congelamento degli embrioni prodotti, ma non impiantati per decisione del medico.

[23] La salute della donna che ricorre alle tecniche e l'autodeterminazione della coppia nelle scelte relative alla vita privata e familiare.

tale bisognevole di protezione legale[24].

L'esigenza è stata avvertita maggiormente in séguito a ulteriori interventi della Consulta, aventi a oggetto questioni diverse, che, peraltro, hanno indotto un progressivo, notevole aumento della popolazione degli embrioni in stato di crioconservazione; la fragilità di questi ultimi risulta ancóra più evidente, non potendo essi godere neanche dello scudo protettivo del corpo della madre. Caduto il limite di produzione di tre embrioni per ciascun ciclo di applicazione delle tecniche di p.m.a.[25], difatti, è risultata allargata anche la platea delle coppie alle quali è consentito l'accesso alla p.m.a., poiché vi sono state incluse sia quelle che, per ragioni patologiche, necessitano di ricorrere a tecniche eterologhe[26], sia le coppie fertili, portatrici di malattie geneticamente trasmissibili, che solo attraverso una diagnosi genetica pre-impianto, possono "selezionare" un embrione sano da destinare a una gravidanza[27].

Scardinati così i divieti che, nelle intenzioni del legislatore, fungevano da presidio alla tutela dell'embrione e poi del nato a séguito dell'applicazione delle tecniche di p.m.a., permane in vigore, però, il divieto di soppressione degli embrioni, sancito e sanzionato dall'art. 14, commi 1 e 6, l. n. 40/2004, la cui legittimità è stata affermata dalla Corte Costituzionale[28]. La violazione del divieto integra, dunque, allo stato, gli estremi di un reato, confermando appieno la rilevanza del bene tutelato.

Su altro fronte, la giurisprudenza di merito e di legittimità, in pronunzie rese per lo più in materia di risarcimento danni da *malpratice* medica, allargando le maglie della soggettività, ha individuato nel concepito (embrione/feto) un centro di interessi giuridicamente rilevanti, ritenendolo titolare, ancor prima della nascita, di diritti personalissimi, quali quello alla vita, alla salute, all'identità genetica[29]. A sorvolare su alcune critiche che sono state mosse alle

---

[24] Sul valore e sulla dignità dell'embrione, che ‹‹quale ne sia il, più o meno ampio, riconoscibile grado di soggettività correlato alla genesi della vita, non è certamente riducibile a mero materiale biologico››, v. Corte Cost., 11 novembre 2015, n. 229, in *Foro it.*, 2015, I, c. 3749 ss. A corollario di siffatte statuizioni, la Consulta ha affermato che non è giustificabile un trattamento degli embrioni malformati deteriore rispetto a quelli sani, e che l'esigenza di tutelarne la dignità non può avere altra risposta che quella della procedura di crioconservazione. Medesima sensibilità si riscontra in Corte Cost., 13 aprile 2016, n. 84, in *Dir. fam. pers.*, 2016, p. 745 ss., che, nel dichiarare inammissibile la questione di legittimità del divieto di destinazione alla ricerca scientifica degli embrioni soprannumerari di cui all'art. 13, l. n. 40/2004, ribadisce il rispetto del principio della vita racchiuso nell'embrione, seppure affetto da patologie.

[25] Corte Cost., 8 maggio 2009, n. 151, cit.

[26] Corte Cost., 10 giugno 2014, n. 162, in *Europa dir. priv.*, 2014, p. 1105 ss., che ha dichiarato incostituzionale il relativo divieto, che era stato introdotto nel 2004.

[27] Corte Cost., 5 giugno 2015, n. 96, in *Foro it.*, 2015, I, c. 2250 ss., che ha appunto ammesso, a determinate condizioni, all'accesso a tecniche di p.m.a. e alla diagnosi genetica preimpianto le coppie fertili portatrici delle suddette patologie, al fine di consentire loro l'impianto dei soli embrioni risultati sani, destinando a una perenne crioconservazione quelli malformati.

[28] Corte Cost., 11 novembre 2015, n. 229, cit., che ha rigettato la questione di legittimità costituzionale della norma, con riferimento al delitto di ‹‹embrionicidio››. Peraltro, come fa osservare I. PELLIZZONE, *Dopo la sentenza costituzionale n. 229 del 2015: la rilevanza penale della selezione eugenetica e della soppressione degli embrioni malati*, in *Studium iuris*, 2016, p. 834, la sentenza valorizza anche un altro aspetto degno di rilievo, e cioè la qualificazione degli embrioni in termini di veicolo di un elemento fondamentale dell'identità biologica individuale: il patrimonio genetico delle persone dai cui gameti si sono formati.

[29] Cfr., tra le sentenze che hanno avuto maggiore risonanza, pur attestate su posizioni diversificate, Cass., 11 maggio 2009, n. 10741, in *Giur. it.*, 2010, p. 67 ss.; Cass., 2 ottobre 2012, n. 16754, in *Foro it.*, 2013, I, c. 181 ss.; Cass., Sez. un., 22 dicembre 2015, n. 25767, in *Giur. it.*, 2016, p. 543 ss. Sugli spunti che provengono dalla giurisprudenza in tema di tutela risarcitoria del concepito leso, v. F.D. BUSNELLI, *Il problema della soggettività del concepito a cinque anni dalla legge sulla procreazione medicalmente assistita*, in *Nuova giur. civ. comm.*, 2010, II, p. 185 ss.

decisioni indicate, non essendo questa la sede per darne conto[30], occorre qui notare che esse rivelano una certa incertezza innanzi alla vita nascente, quanto alla sua configurazione sul piano giuridico, a fronte del quale pare evidente lo sforzo di non tralasciare aspetti rilevanti sguarniti di tutela e di ricercare soluzioni, seppure discutibili, adattate alla peculiare conformazione del concepito. Sullo sfondo di tali ricostruzioni, si scorge la consapevolezza dei giudici del valore intrinseco che l'ordinamento assegna allo sviluppo della vita umana, per il tramite di norme che, in modi vari, mirano ad assicurare la prosecuzione di quel processo che evolve, senza soluzione di continuità, sino alla nascita[31].

Nondimeno, alla ricostruzione dell'«identità» dell'embrione umano ha concorso anche la giurisprudenza europea, che, in diverse sedi, ha inteso accordargli una speciale tutela in ragione dei suoi peculiari connotati.

In particolare, mentre la Corte europea dei diritti dell'uomo si è mantenuta più cauta in alcune note decisioni[32], sono assai rilevanti due pronunzie della Corte di Giustizia europea, rese in merito alla definizione di embrione ai fini dell'applicazione della Direttiva 98/44/CE, concernente le invenzioni biotecnologiche. In queste sentenze, il diritto dell'Unione è stato interpretato accogliendo una nozione molto ampia di «embrione umano», che, seppure riferita allo specifico àmbito disciplinare, evidenzia l'attenzione e, soprattutto, l'approccio precauzionale delle Istituzioni europee alla questione. Di fatto, le decisioni precludono una tutela giuridica per i trovati che hanno per oggetto o utilizzano cellule staminali embrionali e suoi derivati, perché il prelievo comporta la distruzione dell'embrione, cui la Corte UE annette la dignità di essere umano[33].

Invero, su un terreno disseminato da tante incertezze sul piano scientifico

---

[30] In argomento, per un'ampia ricognizione delle posizioni sviluppatesi, si rinvia, da ultimo, a E.A. EMILIOZZI, *La responsabilità medica*, in *Tratt. dir. civ. comm.* Cicu-Messineo, già diretto da L. Mengoni e P. Schlensinger, continuato da V. Roppo e F. Anelli, Milano, 2023, p. 598 ss.

[31] Processo la cui interruzione, peraltro, ha consentito alla giurisprudenza di enucleare uno specifico profilo di danno non patrimoniale, identificato nella sofferenza che deriva dalla recisione del rapporto che, innegabilmente, i genitori instaurano in modo progressivo con il feto in via di sviluppo: v. Cass., ord. 29 settembre 2021, n. 26301, in *Ridare.it*, con nota di F. TOPPETTI, *Il dolore dei genitori per la morte del feto*.

[32] Il riferimento è a Corte Edu, 10 aprile 2007, c. Evans c/The United Kingdom, in *Europa dir. priv.*, 2008, p. 225 ss. (s.m.), con nota di L. BOZZI, *Il consenso al trattamento di fecondazione assistita tra autodeterminazione procreativa e responsabilità genitoriale*, nella quale si nega agli embrioni *in vitro* la titolarità di un autonomo diritto alla vita, ma se ne riconosce la capacità di evolversi, in un processo contrassegnato da continuità temporale, in persona, come tale da proteggere; e a Corte Edu, 27 agosto 2015, c. Parrillo c/Italia, in *Foro it.*, 2015, IV, c. 453 (s.m.), con nota di G. CASABURI, *Ricerche embrionali: un'occasione perduta della Corte europea*, che recide ogni contiguità dell'embrione con il concetto di "bene", ma riconosce un ampio margine di discrezionalità agli Stati.

[33] V. Corte di Giustizia UE, 18 ottobre 2011, causa C-34/2010, in *Nuova giur. civ. comm.*, 2012, I, p. 289 ss., ed *ivi*, II, p. 237 ss., nota di R. ROMANO, *La brevettabilità delle cellule staminali embrionali umane*, nonché in *Fam. dir.*, 2012, p. 221 ss., con nota di A. SCALERA, *La nozione di "embrione umano" all'esame della Corte UE*, per la quale l'art. 6 della Direttiva va interpretato nel senso che ‹‹costituisce "embrione umano" qualunque ovulo umano fin dalla fecondazione, qualunque ovulo umano non fecondato in cui sia stato impiantato il nucleo di una cellula umana matura e qualunque ovulo umano non fecondato che, attraverso partenogenesi, sia stato indotto a dividersi e a svilupparsi››.
Cfr., poi, Corte di Giustizia UE, 18 dicembre 2014, causa C-364/2013, in *Giur. it.*, 2015, p. 1897 ss. (s.m.), con nota di R. ROMANDINI, *La brevettabilità del materiale biologico ottenuto da partenoti*, e, per esteso, in *Corr. giur.*, 2026, p. 23 ss., con nota di G. SPEDICATO, *Cellule staminali embrionali e limiti alla brevettabilità delle invenzioni biotecnologiche*, che ha ridimensionato sensibilmente la definizione resa in precedenza, nel senso di escludere dalla nozione i partenoti (cioè gli ovuli attivati mediante partenogenesi), qualora i medesimi siano privi della capacità intrinseca di svilupparsi in un essere umano.

prima ancóra che su quello giuridico, sembra più che mai pertinente il richiamo al principio di precauzione quale filtro e guida da seguire nelle scelte da operare. Da un lato, non vi sono dati precisi circa i limiti temporali oltre i quali la crioconservazione in azoto liquido osta ad un proficuo impianto dell'embrione; dall'altro, non esistono ancóra criteri e metodologie certe per diagnosticare la morte o una definitiva perdita di vitalità dell'embrione [34]. Peraltro, seppure siffatti accertamenti si rendessero possibili, tornerebbe a porsi il problema se considerare gli embrioni residui non più utilizzabili per nessuna delle finalità ipotizzate (v. *infra*, par. 4), a causa delle ragioni indicate – morte, cessazione di vitalità o di funzionalità –, alla stregua di materiale biologico, con il conseguente assoggettamento alla disciplina prevista per tali materiali, quando raccolti in àmbito diagnostico e terapeutico [35]: una conclusione siffatta avallerebbe una inaccettabile involuzione verso una reificazione dell'embrione, che mal si concilia con la invocata sua dignità di essere umano, emersa dal dibattito dottrinario e dall'elaborazione giurisprudenziale sin qui sinteticamente ripercorsi.

3. Gli embrioni crioconservati: le attuali categorie e le incertezze circa la sorte dei soprannumerari.

La categoria degli embrioni in stato di crioconservazione si presenta eterogenea, poiché in essa confluiscono sia gli embrioni che potrebbero ancóra essere destinati a un impianto, sia quelli in soprannumero, che, invece, non potrebbero, perché ultronei rispetto a uno specifico progetto procreativo di una coppia o ritenuti non idonei per cause di tipo organico o clinico oppure perché rifiutati, esplicitamente o implicitamente, in quanto affetti da patologie irreversibili riscontrate a séguito di diagnosi genetica pre-impianto, e, dunque, selezionati per favorire la nascita di quelli sani[36].

Con l'ausilio delle fonti di rango secondario, integrative del dettato della l. n. 40/2004, [37] è possibile distinguere due diverse tipologie di embrioni crioconservati: quelli in attesa di un futuro impianto, compresi quelli congelati prima dell'entrata in vigore della legge, e quelli in ‹‹stato di abbandono››, il cui accertamento è collegato al verificarsi di determinate condizioni[38]. L'anzidetta

[34] Sul punto, v. la *Relazione finale* della Commissione di Studio, all'uopo nominata con Decreto del Ministero del Lavoro della Salute e delle Politiche Sociali, sugli embrioni crioconservati nei centri di p.m.a., dell'8 gennaio 2010, in *www.salute.gov.it.*

[35] Essi sono equiparati a ‹‹rifiuti sanitari pericolosi››: v. D.P.R. 15 luglio 2003, n. 254, recante la disciplina della gestione dei rifiuti sanitari, attuativo dell'art. 24, l. 31 luglio 2002, n. 179, inerente allo smaltimento dei rifiuti sanitari.

[36] Per un'utile ricognizione delle tante situazioni di fatto che possono condurre alla crioconservazione degli embrioni, v. R. LANDI, *L'incerto destino degli embrioni soprannumerari*, in *Rass. dir. civ.*, 2017, p. 913 ss.

[37] V. le *Linee guida* di cui al D.M. 1° luglio 2015 (G.U. 14 luglio 2015, n. 161), che ha sostituito i precedenti Decreti del Ministero della Salute dell'11 aprile 2008 e del 21 luglio 2004, di tenore sostanzialmente analogo sul punto specifico; nonché il Decreto del Ministero della Salute 4 agosto 2004 (*Norme in materia di procreazione medicalmente assistita*, G.U. 26 agosto 2004, n. 200).

[38] Lo stato di abbandono di un embrione è accertato al verificarsi di una delle seguenti condizioni: a) il centro che effettua tecniche di p.m.a. acquisisce la rinuncia scritta al futuro impianto degli embrioni crioconservati da parte della coppia di genitori o della singola donna (nel caso di embrioni prodotti prima della entrata in vigore della l. n. 40/2004, con seme di donatore e in assenza di partner maschile); b) il centro che effettua tecniche di p.m.a. documenta i ripetuti tentativi eseguiti, per almeno un anno, di ricontattare la coppia o la

classificazione indirizza la sorte degli embrioni, che risulta ancor oggi regolamentata nel senso che quelli appartenenti alla prima tipologia devono essere crioconservati presso gli stessi centri dove le tecniche sono state effettuate[39], mentre quelli abbandonati avrebbero dovuto essere trasferiti – dopo l'attuazione di una serie di cómpiti e verifiche demandati all'Istituto Superiore di Sanità – alla Biobanca Nazionale, situata presso il Centro trasfusionale e di immunologia dei trapianti dell'Istituto di ricovero e cura a carattere scientifico "Ospedale Maggiore" di Milano, ove doveva essere attivato in maniera centralizzata un centro di crioconservazione degli embrioni stessi[40]. Cómpito del centro doveva essere quello di effettuare studi e ricerche sulle tecniche di crioconservazione dei gameti e degli embrioni "orfani" [41]. Tuttavia, nonostante la creazione della struttura, il trasferimento non è stato mai effettuato[42], sì che gli embrioni soprannumerari continuano ancóra oggi a restare presso i centri in cui sono custoditi e sono destinati al mantenimento in crioconservazione sino all'inevitabile deterioramento e alla conseguente estinzione naturale[43].

Il profilo più problematico, in una prospettiva *de iure condendo*, è costituito dalla assai labile definizione dello ‹‹stato di abbandono››, peraltro rimessa a una fonte di rango secondario. Sin d'ora è possibile affermare che essa appare inidonea a fungere da presupposto per eventuali destinazioni degli embrioni residuali[44].

La situazione di stallo in cui essi versano è, comunque, speculare al permanere del divieto di una loro soppressione, la cui violazione integra gli estremi di un reato[45]. D'altra parte, il riconoscimento della ‹‹dignità umana›› in capo a tutti gli embrioni, che riflette il lungo dibattito volto a ricostruirne l'identità, rende oltremodo difficile ipotizzare alternative a una perenne crioconservazione.

---

donna che ha disposto la crioconservazione degli embrioni; solo in caso di reale, documentata impossibilità a rintracciare la coppia, l'embrione potrà essere definito come ‹‹abbandonato››.

[39] Con oneri a carico della struttura sanitaria.

[40] Con oneri della procedura da far gravare su fondi oggetto di un finanziamento *ad hoc* a carico dello Stato.

[41] V., in part., il Decreto del Ministero della Salute 4 agosto 2004, cit., artt. 1, 2 e 5.

[42] Le ragioni che hanno reso inattuabile il trasferimento degli embrioni orfani presso la struttura centralizzata di Milano sono molteplici e da rinvenire in una serie di difficoltà pratiche, quali l'assenza di copertura finanziaria per le procedure di trasferimento e di una disciplina attuativa circa le modalità, la difficile individuazione dello stato di abbandono, la possibile insorgenza di contenziosi giuridici.

[43] Per questi embrioni, ha osservato C. PARDINI, *Libertà di ricerca scientifica e tutela dell'embrione*, in *Nuova giur. civ. comm.*, 2016, II, p. 795, il diritto alla vita pare trascolorare fatalmente in ‹‹una sorta di indefinibile diritto alla crioconservazione sino al deterioramento››.

[44] Esistono, al riguardo, diversi progetti di legge, alcuni dei quali risalenti, che tentano di individuare qualche soluzione al problema e contengono un primo, perfettibile, tentativo di normare l'adozione degli embrioni in stato di abbandono, e, in alcuni di essi, la destinazione alla ricerca scientifica. Cfr. la *Proposta di legge* n. 2058, presentata alla Camera dei Deputati il 12 gennaio 2009, la *Proposta di legge* n. 4800, presentata alla Camera dei Deputati il 25 novembre 2011, e la *Proposta di legge* n. 4831, presentata alla Camera dei Deputati il 6 dicembre 2011, poi abbinate per la discussione in aula. Più di recente, v. la *Proposta di legge* n. 2592, presentata alla Camera dei Deputati il 31 luglio 2014, e il DDL n. 1608, presentato al Senato il 9 settembre 2014. Tali proposte, reperibili sui siti istituzionali, si sono poi tutte arenate nelle secche parlamentari.

[45] Sottolinea G. DI ROSA, *Famiglia (bioetica e diritto)*, in *Enc. dir.*, *I Tematici*, IV, *Famiglia*, cit., p. 400 s., che è proprio la valutazione dell'embrione come entità che ha in sé il principio della vita a giustificare il divieto penale di soppressione di tutti gli embrioni, in coerenza con la logica conservativa e di forte tutela sposata dalla legge del 2004, senza, peraltro, che rilevino differenziazioni del processo di sviluppo dello zigote, che è già fornito dell'identità biologica di un nuovo essere umano.

4. Le prospettive de iure condendo: l'adozione per la nascita e la destinazione alla ricerca scientifica.

Da anni si discute in dottrina della necessità di trovare soluzioni allo stato di congelamento *sine die* degli embrioni soprannumerari, anche alla luce di considerazioni inerenti ai costi organizzativi, gestionali ed economici e all'utilizzo di energie che hanno un impatto sull'ambiente, connessi alla relativa procedura. Il problema, però, non può essere slegato dall'identità dell'embrione, dalla cui definizione dipendono le conseguenze sul piano della disciplina[46]. Nel tempo, sono state formulate diverse proposte, da inquadrare nella prospettiva di un intervento legislativo, che andrà innestato lungo le direttrici dianzi tracciate[47].

Invero, già all'indomani del profilarsi della questione con l'entrata in vigore della legge, gli interpreti si erano schierati su due fronti: alcuni a favore di una destinazione degli embrioni residui alla ricerca scientifica[48], in funzione solidaristica e subordinatamente al consenso della coppia che li ha creati[49], altri nel senso di prefigurare una sorta di loro adozione o donazione in favore di coppie, sterili o no, diverse dai generanti[50], senza che l'una soluzione escludesse necessariamente l'altra.

L'incremento esponenziale del numero di embrioni soprannumerari, dovuto – come si è rilevato in precedenza – agli interventi di riscrittura della l. n. 40/2004, ha favorito la ripresa del dibattito e una maggiore articolazione delle proposte da vagliare[51]. A supporto delle stesse, da un lato, si fa leva sulla

---

[46] Sull'incidenza, in particolare, della natura giuridica dell'embrione e degli interessi di cui è portatore sullo statuto da ricostruire, v. G. TOSCANO, *L'embrione tra ontologia e diritto*, in *Dir. fam. pers.*, 2018, p. 653 ss.

[47] Considerato l'elevato tasso di sensibilità che la connota, la questione non può che essere rimessa alla discrezionalità del legislatore, come sottolineato da Corte Cost., 13 aprile 2016, n. 84, cit., per la quale una scelta così ampiamente divisiva per i profili assiologici insiti, che, peraltro, non trova soluzioni uniformi neppure nella legislazione europea, attiene al piano degli interventi con i quali il legislatore, quale interprete della volontà della collettività, è chiamato a tradurre, sul piano normativo, il bilanciamento tra valori fondamentali in conflitto. La scelta tra il rispetto del principio della vita, racchiusa nell'embrione ove pur affetto da patologia, e le esigenze della ricerca scientifica, che potrebbe utilizzare gli embrioni residuati da procedimenti di p.m.a., tanto dibattuta sul piano etico e scientifico, si sottrae perciò al sindacato del giudice delle leggi, anche perché richiede la emanazione di norme che regolamentino nei dettagli le soluzioni ipotizzate.

[48] A. BELLELLI, *La sperimentazione sugli embrioni: la nuova disciplina*, in *Familia*, 2004, I, p. 989 ss.; I. CORTI, *La procreazione assistita*, in *Il nuovo diritto di famiglia*, *Trattato* diretto da G. Ferrando, vol. III, *Filiazione e adozione*, Bologna, 2007, p. 538 ss. A sostegno dell'idea, veniva fatto rilevare che la tutela assoluta dell'embrione, congegnata dal legislatore, finiva per attuare una scelta che escludeva il necessario bilanciamento tra dignità dell'embrione, diritto alla salute, solidarietà verso chi soffre, libertà della scienza.

[49] F. GAZZONI, *op. cit.*, p. 207; B. MASTROPIETRO, *op. cit.*, p. 1410 ss.

[50] Propenso a tale soluzione già F. SANTOSUOSSO, *op. cit.*, p. 103 ss.; G. OPPO, *Procreazione assistita e sorte del nascituro*, in *Riv. dir. civ.*, 2005, p. 105 s.; F. CAPOLUONGO, *Il problema degli embrioni residui*, in *Fam. dir.*, 2010, p. 1074 ss.; D. CARUSI, *In vita, "in vitro", in potenza. Verso una donazione dell'embrione sopranumerario?*, in *Riv. crit. dir. priv.*, 2010, p. 333 ss.; F.D. BUSNELLI, *Cosa resta della legge 40? Il paradosso della soggettività del concepito*, in *Riv. dir. civ.*, 2011, p. 466 ss. In questa direzione, cfr. i due pareri del Comitato Nazionale per la Bioetica, *L'adozione per la nascita degli embrioni crioconservati derivanti da p.m.a.*, del 18 novembre 2005, e *Destino degli embrioni derivanti da p.m.a. e non più impiantabili*, del 26 ottobre 2007, entrambi in *bioetica.governo.it*, e – più sfumatamente – la *Relazione finale* della Commissione di Studio, all'uopo nominata con Decreto del Ministero del Lavoro della Salute e delle Politiche Sociali, sugli embrioni crioconservati nei centri di p.m.a., cit.

[51] Cfr. C. PARDINI, *op. cit.*, p. 790 ss.; F.D. BUSNELLI, *Nascere (o anche "morire") con dignità: un traguardo problematico per l'embrione*, in *Nuova giur. civ. comm.*, 2017, II, p. 393 ss.; R. LANDI, *op. cit.*, p. 907 ss.; M.G. CABITZA, *op. cit.*, p. 620 ss.; R. CRISTIANO, *Gli embrioni soprannumerari: tutela e sperimentazione*, in *Rivista AIC*, 2018, p. 1 ss.; F. AZZARRI, *op. cit.*, p. 567 ss.; A. SPADARO, *Il "concepito": questo sconosciuto…*, in *Biolaw Journal* –

naturale destinazione alla vita dell'embrione, quale entità umana, titolare di diritti, di cui preservare la dignità; dall'altro, di fronte a un'obiettiva impossibilità di portarlo alla nascita, si apre alla possibilità di un utilizzo per la ricerca scientifica finalizzata al benessere della collettività[52]. Invero, le due proposte potrebbero in astratto convivere, come pure sostenuto[53], ed allora si tratta – nel bilanciamento dei valori costituzionali in gioco – di fissare le condizioni e di tracciare i percorsi per realizzarle, nonché di stabilire quale di esse debba essere rivestita di carattere prioritario rispetto all'altra. I nodi da sciogliere non sono pochi.

Per quanto riguarda l'istituto dell'adozione per la nascita, che aderisce maggiormente alla *ratio* ispiratrice della l. n. 40/2004[54], fortemente patrocinato dal CNB e sostenuto da gran parte della dottrina[55], i vuoti da colmare in via normativa attengono, innanzitutto, alla delimitazione del presupposto dell'"abbandono" definitivo dell'embrione da destinare a un progetto procreativo altrui, che andrebbe ancorato a criteri più certi e rigorosi di quelli fissati nelle fonti di rango secondario[56]; poi, all'individuazione dei requisiti che deve possedere la coppia adottante e del ruolo nella vicenda della coppia dei generanti.

Quanto ai requisiti soggettivi degli adottanti, si può ipotizzare che siano quelli risultanti dal combinato disposto di cui agli artt. 4 e 5, l. n. 40/2004,[57]

Rivista di BioDiritto, *Special Issue*, 2019, 2, p. 419 ss., spec. p. 429 ss.; S.P. PERRINO, *Fecondazioni postume e destinazione delle cellule riproduttive alla ricerca*, in *Biolaw Journal – Rivista di BioDiritto*, 2020, 2, p. 237 ss., spec. p. 246 ss.; I. BARONE, *op. cit.*, p. 1443 ss.; S.P. PERRINO, *Embrio-Adozioni: a brave new world?*, in *giustiziacivile.com.*, 2021, p. 2 ss.; G. DI ROSA, *op. cit.*, p. 400 ss.; G. GIAIMO, Cui prodest servare? *Due ipotesi di destinazione per gli embrioni crioconservati*, in *Dir. fam. pers.*, 2022, p. 254 ss.; R. SENIGAGLIA, *Quale* degno *destino per gli embrioni soprannumerati?*, in *Europa dir. priv.*, 2022, p. 421 ss.

[52] Al riguardo, è stata fatta anche notare la contraddittorietà del divieto di sperimentazione vigente in Italia con l'assenza di un divieto all'importazione di linee cellulari embrionali dall'estero, che sono pur sempre ottenute attraverso la distruzione dell'organismo di partenza, di cui, invece, possono avvalersi i centri di ricerca operanti sul territorio nazionale: v. C. PARDINI, *op. cit.*, p. 791. Si tenga in conto, però, che la questione è in continua evoluzione, perché se il valore della ricerca sulle cellule staminali embrionali per la comprensione e la cura di numerose patologie, stante le loro intrinseche caratteristiche, resta intatto, molti passi in avanti si stanno facendo nelle ricerche condotte da linee cellulari pluripotenti ricavate da staminali adulte (sul punto, v. G. DI ROSA, *op. cit.*, p. 402, e, per i riferimenti agli studi scientifici, *ivi* nt. 68); inoltre, nuove potenzialità paiono derivare dalla ricerca sui c.d. organoidi, colture cellulari tridimensionali in miniatura, tra i modelli di studio emergenti e più promettenti in campo bio-medico.

[53] Cfr., in particolare, F. CAPOLUONGO, *op. cit.*, p. 1075; F.D. BUSNELLI, *Cosa resta della legge 40? Il paradosso della soggettività del concepito*, cit., p. 468 s.; ID., *Nascere (o anche "morire") con dignità: un traguardo problematico per l'embrione*, cit., p. 402; M.G. CABITZA, *op. cit.*, p. 642 ss.; F. AZZARRI, *op. cit.*, p. 567 ss.; G. GIAIMO, *op. cit.*, p. 276 ss.; R. SENIGAGLIA, *op. cit.*, p. 446 ss.

[54] Invero, l'adozione era stata contemplata nel progetto di legge, ma poi non era confluita nel testo finale. Nelle more dell'approvazione, difatti, erano emersi forti dubbi, sia sul raccordo con la disciplina dell'adozione, sia per il rischio di una strumentalizzazione dell'istituto al fine dello smaltimento delle scorte di embrioni nei laboratori: sul punto, v. E. IORATTI FERRARI, *Tutela della vita prenatale nel contesto della gravidanza*, in S. CANESTRARI, G. FERRANDO, C.M. MAZZONI, S. RODOTÀ e P. ZATTI (a cura di), *Il governo del corpo*, t. II, in *Trattato di biodiritto*, diretto da S. Rodotà e P. Zatti, II, Milano, 2011, p. 1619 s.

[55] V. spec. F.D. BUSNELLI, *Cosa resta della legge 40? Il paradosso della soggettività del concepito*, cit., p. 466 ss.; D. CARUSI, *op. cit.*, p. 337 ss.; I. BARONE, *op. cit.*, p. 1443 ss.; G. DI ROSA, *op. cit.*, p. 404 s.

[56] Utili spunti al riguardo sono contenuti nei disegni di legge indicati in nt. 44. Suggerisce il ricorso allo ‹‹stato di abbandono›› delineato dall'art. 8, l. n. 184/1983 S.P. PERRINO, *Embrio-Adozioni: a brave new world?*, cit., p. 6.

[57] L'art. 5 consente l'accesso alla p.m.a. alle ‹‹coppie di maggiorenni di sesso diverso, coniugate o conviventi, in età potenzialmente fertile, entrambi viventi››. Ai sensi dell'art. 4, inoltre, per avere accesso alle relative tecniche, è necessario che sia accertata l'impossibilità di rimuovere altrimenti le cause impeditive della procreazione e che sia documentata da atto medico la sterilità o l'infertilità, nei casi sia di causa individuata che inspiegata. Va ricordato, difatti, che, nell'impostazione della l. 40/2004, il ricorso alle tecniche di p.m.a.

ovvero essere mutuati, in via analogica, dalla l. n. 184/1983 in tema di adozione di minori, in tal caso con un allargamento della cerchia degli aspiranti genitori anche a coloro che non siano affetti da una sterilità o da un'infertilità da certificare. L'istituto costituirebbe ulteriore applicazione del concetto di genitorialità sociale, sì che lo *status* acquisito dal nato andrebbe equiparato a quello del figlio adottato. I genitori genetici dell'embrione, invece, dovrebbero partecipare alla fattispecie *de qua* mediante un atto di autodeterminazione, volto a imprimere alla destinazione dell'embrione lo scopo della realizzazione di un progetto procreativo di altri, nell'ottica del ‹‹dono››, già sperimentata in altre realtà europee[58]. Un atto siffatto parteciperebbe delle caratteristiche di altre vicende dispositive del corpo umano, reputate lecite quando ispirate da finalità solidaristiche e improntate alla gratuità dell'atto di autonomia privata, onde prevenire qualsivoglia tipo di abuso[59]. Nelle proposte di legge delle quali si è fatto cenno in precedenza[60], la competenza sull'intero procedimento, come pare ovvio, spetta al Tribunale per i minorenni, chiamato a vagliare le domande e a vigilare sull'*iter* della procedura.

È fuori di dubbio che l'adozione per la nascita si adatti di più alla *ratio* della legge in materia di p.m.a., che intendeva limitare drasticamente il fenomeno della crioconservazione, poiché appare rispettosa della dignità di essere umano dell'embrione, al quale si offre una *chance* di vita. Nondimeno, le criticità annesse all'istituto possono essere individuate, innanzitutto, nella non semplice fattibilità della procedura, che necessariamente va scandita in una serie di passaggi che ne assicurino la legittimità, e nella circostanza che tale forma di adozione – peraltro praticabile solo con gli embrioni idonei a una gravidanza, e non con quelli che presentano anomalie irreversibili dello sviluppo – potrebbe essere richiesta in un numero limitato di casi, certamente tale da non coprire l'intera popolazione degli embrioni impiantabili; e ciò anche per questioni di carattere clinico, connesse, ad esempio, alla (in)compatibilità genetica con l'aspirante madre.

La destinazione degli embrioni soprannumerari alla ricerca scientifica, invece, che, per i motivi su esposti, dovrebbe rivestire carattere di soluzione subordinata rispetto a quella dell'adozione e riguardare solo gli embrioni non impiantabili[61], postula di rivedere *in primis* la scelta di campo del legislatore,

---

si colloca nell'alveo dei trattamenti sanitari volontari, come modo per realizzare il diritto alla salute dei soggetti coinvolti, e si configura, pertanto, come rimedio/terapia, di carattere residuale, per superare una patologia.

[58] Sul punto, v. R. LANDI, *op. cit.*, p. 922 ss.; S.P. PERRINO, *Embrio-Adozioni: a brave new world?*, cit., p. 13 ss.

[59] In argomento, in generale, v. G. RESTA, *Doni non patrimoniali*, in *Enc. dir.*, *Annali*, IV, Milano, 2011, p. 510 ss.; nello specifico, v. D. CARUSI, *op. cit.*, p. 339.

[60] *Retro*, nt. 44.

[61] Volendo accedere a questa prospettiva, risulta necessario, difatti, distinguere tra gli embrioni che possono ancóra essere destinati a una gravidanza e quelli che, a causa di alterazioni genetiche o malformazioni, non sono più impiantabili: v. G. GIAIMO, *op. cit.*, p. 257. La prospettiva non è condivisa già dalla Corte Costituzionale, che ha reputato discriminatorie differenziazioni di tal guisa (v. Corte Cost., 11 novembre 2015, n. 229, cit.), e da una parte della dottrina. Per tutti, v. diffusamente G. DI ROSA, *op. cit.*, p. 400 ss., per il quale deve prevalere la logica conservativa della vita embrionale rispetto alla logica della disponibilità appropriativa da parte dello Stato quale promotore della ricerca scientifica e tecnica di cui all'art. 9 Cost., e ciò anche quando vi sia il consenso dei genitori. Peraltro, in un'ottica di bilanciamento, fa notare R. SENIGAGLIA, *op. cit.*, p. 440, che la scelta delle Corti pare univoca nel senso della prevalenza della dignità di ogni embrione sulla libertà di ricerca scientifica, considerata l'evidente disparità valoriale dei princìpi in gioco. Piuttosto occorre interrogarsi sul ‹‹se la sua dignità, in presenza di talune circostanze e specifici casi, possa trovare realizzazione in quell'impiego e nell'orizzonte della solidarietà sociale, operando,

che, con l'art. 13, l. n. 40/2004, ha inteso vietare la sperimentazione e la ricerca sugli embrioni, a meno che non sia rivolta alla tutela della salute e allo sviluppo dell'embrione stesso, e qualora non siano disponibili metodologie alternative[62]. L'esistenza di tali limitazioni è il frutto di una scelta discrezionale del legislatore, che si coniuga con i ricordati obiettivi di tutela dell'embrione.

L'esistenza dei suddetti divieti costituisce, dunque, il primo scoglio all'accoglimento di una proposta in tal senso, che ne presuppone l'abrogazione, e che potrà, a volerla percorrere, poi essere sviluppata nella direzione suggerita da autorevole dottrina[63], e cioè come esito di un percorso che conduce l'embrione verso una "morte dignitosa": una fine concepita come una sorta di dono ‹‹che vale in qualche misura a "nobilitare" l'avvenuto "sacrificio"››[64]. Sulla scorta del modello francese, peraltro di recente in parte modificato[65], si potrebbe consentire la destinazione alla ricerca da realizzare nell'àmbito di un procedimento pubblico, ove la verifica del definitivo abbandono dell'embrione da parte dei generanti e della indisponibilità ad accoglierlo da parte di un'altra coppia fungano da presupposto per un provvedimento che metta fine, dopo un tempo da stabilire, alla durata dello stato di crioconservazione dell'embrione. Ciò dovrebbe avvenire mediante un accertamento pubblico della sua morte (così sottraendone la sorte alla pura volontà dei privati), cui consegue la destinazione a progetti di ricerca scientifica, da eseguire sulla base di protocolli debitamente autorizzati da un'apposita Autorità e improntati al

---

quindi, la valutazione *dall'interno* della sua dimensione ontologica, del suo essere il *fine* e non il *mezzo* delle scelte dell'ordinamento››.

[62] Tali divieti si pongono in linea con la Convenzione di Oviedo sui diritti dell'uomo e sulla biomedicina del 1997 (di cui l'Italia ha autorizzato la ratifica con la l. n. 145/2001), che, all'art. 18, vieta la clonazione di embrioni a fini riproduttivi e la creazione di embrioni per fini di ricerca, mentre richiede di assicurare un'adeguata protezione agli embrioni soprannumerari creati nel contesto della fecondazione assistita e utilizzati a fini di ricerca, ove quest'ultima sia ammessa nel singolo Stato aderente alla convenzione. Va osservato, inoltre, che alla deroga al divieto di cui all'art. 13, l. n. 40/2004, nel senso di consentire la ricerca clinica e sperimentale se rivolta a fini terapeutici e diagnostici in favore dell'embrione stesso, si aggiunge una ulteriore deroga, contenuta in una fonte secondaria (art. 5, Decreto del Ministero della Salute 4 agosto 2004, cit.), che permette studi e ricerche sugli embrioni ‹‹orfani››, che siano relativi alle tecniche di crioconservazione dei gameti e degli embrioni. Tale previsione è giudicata ‹‹sconcertante›› da R. VILLANI, *Procreazione assistita e Corte Costituzionale: presupposti e conseguenze (dirette ed indirette) del recente intervento della Consulta sulla disciplina della L. n. 40/04*, in *Nuove leggi civ. comm.*, 2009, p. 496 s. e *ivi* nt. 81, perché in contrasto con il disposto della legge. È indiscutibile che una simile disposizione avrebbe dovuto essere collocata diversamente sul piano gerarchico delle fonti; occorre notare che il suo scopo è probabilmente quello di affinare proprio quelle tecniche reputate, secondo una certa ottica, in grado di salvaguardare l'esistenza e la dignità degli embrioni abbandonati, evitandone la soppressione.

[63] F.D. BUSNELLI, *Cosa resta della legge 40? Il paradosso della soggettività del concepito*, cit., p. 468 s., e più ampiamente, ID., *Nascere (o anche "morire") con dignità: un traguardo problematico per l'embrione*, cit., p. 401 ss. *Adde*, nel senso che, a fronte di un inevitabile perimento dell'embrione o dell'impossibilità di svilupparsi e di nascere, una scelta rivolta a tutelare la salute collettiva e il valore della vita di milioni di uomini gli restituirebbe la dignità perduta in una conservazione *sine die*, v. G. DI ROSA, *op. cit.*, p. 405; nonché R. SENIGAGLIA, *op. cit.*, p. 444 ss.

[64] F.D. BUSNELLI, *op. ult. cit.*, p. 402.

[65] *Loi* n° 2021-1017 *du* 2 *août* 2021 *relative à la bioéthique*, che ha revisionato la precedente legge, introducendo modifiche significative, che non è possibile esaminare in questa sede (la legge è reperibile all'indirizzo https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043884384); per un commento alla genesi, ai contenuti e alle novità, cfr. T. PENNA, PMA pour toutes*, anonimato di donatori e donatrici di gameti e potenziali conseguenze discriminatorie dell'esclusione della GPA. Prime riflessioni sulla riforma della* loi de bioéthique *in Francia*, in *Biolaw Journal – Rivista di BioDiritto*, 2021, 3, p. 439 ss. Con riguardo alle cellule embrionali, risulta ampliato il campo delle ricerche che possono essere autorizzate: v., sul punto, D. BORRILLO, *Analisi dello sviluppo del biodiritto in Francia dall'ultima riforma legale*, in *Hal Open Science (id. 03746571)*, 2022, p. 11.

perseguimento di finalità mediche e al rispetto di princìpi etici[66].

La dottrina che sostiene l'ipotesi della destinazione alla scienza degli embrioni soprannumerari non impiantabili [67] promuove un'interpretazione ‹‹dinamica›› del concetto di dignità, più aderente alla nobiltà intrinseca all'essere umano, se rivolto al soddisfacimento di un rilevantissimo fine solidaristico[68]. In altri termini, il dono dell'embrione, la cui struttura si altera nel corso del tempo rendendolo inidoneo a evolversi e svilupparsi, può costituire un atto di solidarietà conforme, e non in contrasto, con la particolare dignità che gli compete[69].

Conclusioni.

A voler tirare le fila del discorso, emerge che le due proposte allo studio per gli embrioni residuali – l'adozione per la nascita e la destinazione alla ricerca scientifica – paiono ispirate da princìpi diversi; entrambe richiedono l'intervento del legislatore per poterne dare attuazione. Se l'ipotesi dell'adozione asseconda la naturale destinazione dell'embrione a un progetto di procreazione e alla soddisfazione del desiderio di genitorialità di una coppia, dunque tende alla vita, l'altra ipotesi valorizza un diverso interesse di rango costituzionale, quale quello della promozione della ricerca finalizzata alla tutela della salute umana, e può essere associata, in qualche modo, a un'idea di morte "dignitosa" e rispettosa dell'intima essenza umana dell'embrione.

La scelta, come tutte quelle eticamente sensibili, non può che essere il frutto del volere della collettività, che esprime la coscienza sociale e la cultura prevalenti in un dato momento storico. Si può solo osservare, in conclusione, che l'ordinamento ha già in sé le coordinate di sistema – princìpi, valori, norme – per supportare una decisione tanto delicata, quanto improcrastinabile.

---

[66] *Amplius*, v. F.D. Busnelli, *Nascere (o anche "morire") con dignità: un traguardo problematico per l'embrione*, cit., p. 402 s.

[67] Cfr., in part., A. Spadaro, *op. cit.*, p. 429 ss., il quale osserva che Corte Cost., 13 aprile 2016, n. 84, cit., in realtà non ha escluso, tra le righe, il possibile bilanciamento *pro* salute e ricerca scientifica, e ha fornito una sorta di "decalogo" per il legislatore per una futura regolamentazione. Per più puntuali osservazioni sul punto, v. Id., *Embrioni crio-congelati inutilizzabili: la Corte Costituzionale se ne lava le mani, ma qualcosa dice… (nota a C. cost., sent. n. 84/2016)*, in *Biolaw Journal – Rivista di BioDiritto*, 2016, 2, p. 253 ss.

[68] In tal senso, v. spec. G. Giaimo, *op. cit.*, p. 281 ss., a parere del quale il valore della solidarietà non è antitetico al rispetto comunque dovuto alle blastocisti, inevitabilmente destinate a una stasi criogenica potenzialmente perenne, laddove una eventuale disposizione per finalità dirette al benessere collettivo ne esalta, invece, la dignità, come già accade per gli atti relativi ai trapianti di organi (l. n. 91/1999) o per la destinazione delle spoglie mortali ad attività di didattica o di ricerca (l. n. 10/2020).

[69] Cfr., A. Bellelli, *op. cit.*, p. 989 s.; G. Ferrando, *La nuova legge in materia di procreazione medicalmente assistita: perplessità e critiche*, cit., p. 813. In senso contrario, G. Oppo, *Procreazione assistita e sorte del nascituro*, cit., p. 106, per il quale deve imporsi il rispetto dovuto alla vita nascente, anche nelle fasi estreme: l'Illustre A. fa rilevare che una cosa è lasciar morire, altra cosa è uccidere, e si domanda se la scienza, esauriti gli embrioni esistenti, si asterrebbe poi dal pretendere di poter continuare l'attività di ricerca su embrioni ‹‹nuovi››. Peraltro, come osserva G. Di Rosa, *op. cit.*, p. 401, risulterebbe ribaltata l'operatività del richiamato art. 18 della Convenzione di Oviedo, laddove vieta la creazione di embrioni a soli fini di ricerca, che risulterebbe aggirato, perché, indirettamente e surrettiziamente, si finirebbe per consentire siffatta pratica, stante la inevitabile creazione di embrioni eccedenti per la finalità procreativa.

Mollo A A, Napolitano D, Sicca L M, ' Il formalismo testamentario e le tecnologie assistive per le persone con disabilità: profili giuridici e organizzativi' (2022) 2 EJPLT, 99-118.
DOI: https://www.doi.org/10.57230/EJPLT222AAM

EJPLT
ISSN 2704-8012

Il formalismo testamentario e le tecnologie assistive per le persone con disabilità: profili giuridici e organizzativi.

Testamentary formalism and assistive technologies for people with disabilities: legal and organizational profiles.

ANNA ANITA MOLLO
Assegnista di ricerca in Diritto Privato, Scuola Superiore Meridionale

DOMENICO NAPOLITANO
Assegnista di ricerca in Organizzazione Aziendale, Scuola Superiore Meridionale

LUIGI MARIA SICCA
Professore Ordinario di Organizzazione Aziendale, Università degli Studi di Napoli Federico II

Abstract

Le tecnologie assistive, come da ultimo potenziate anche grazie all'intelligenza artificiale, vengono sempre più spesso impiegate dalle persone con disabilità per riuscire ad esprimere la propria volontà. Tuttavia, l'attuale impianto normativo non sempre consente l'utilizzo di strumenti tecnologici per la conclusione di validi negozi giuridici. Più in particolare, nel presente contributo l'attenzione sarà focalizzata sull'analisi delle norme che disciplinano le successioni a causa di morte per mostrare come il rigido formalismo testamentario che caratterizza il nostro ordinamento giuridico sia di ostacolo al perfezionamento di un valido testamento da parte di chi può esprimersi soltanto per il tramite di devices tecnologici. Saranno, inoltre, esaminate le ricadute sociali, nella prospettiva degli studi organizzativi, delle contraddizioni derivanti dalla mancanza di coordinamento tra sviluppo tecnologico, quadro normativo di riferimento ed esigenze specifiche delle persone con disabilità.

Assistive technologies, as most recently enhanced by artificial intelligence, are increasingly used by persons with disabilities to express their will. However, the current legal framework does not always allow the use of technological tools for the conclusion of valid legal transactions. More specifically, in this contribution, attention will be focused on the analysis of the rules governing succession law in order to show how the rigid testamentary formalism that characterizes our legal system is an obstacle to the finalization of a valid will by those who can only express themselves by means of technological devices. The social repercussions, from the perspective of organizational studies, of the contradictions arising from the lack of coordination between technological development, the legal framework and the specific needs of people with disabilities will also be examined.

© The author(s) 2022, 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: disabilità; vulnerabilità; diritto successorio; studi organizzativi.

Summary [1] : 1. Introduzione – 2. Il formalismo testamentario: tra ragioni storiche, stratificazioni normative e vuote formalità. – 2.1. Le ulteriori formalità in caso di testamento di persona con disabilità. – 3. Le persone con disabilità e l'autonomia testamentaria: quali limiti? – 4. Il possibile ruolo della tecnologia in materia successoria: brevi profili di comparazione. – 5. Il superamento del formalismo testamentario in conformità alla Convenzione delle Nazioni Unite sui diritti delle persone con disabilità. – 6. Conclusioni. – 6.1. Prospettiva organizzativa – 6.2. Prospettiva giuridica.

1. Introduzione.

L'accelerazione della trasformazione digitale e l'utilizzo delle tecnologie dell'informazione e della comunicazione (TIC), dell'intelligenza artificiale e della robotica favoriscono la progettazione di strumenti e di servizi per le esigenze specifiche delle persone con disabilità.

Tra queste, le tecnologie vocali meritano un'attenzione particolare, in quanto consentono di riprodurre artificialmente quella che è considerata una delle principali facoltà umane: la comunicazione per il tramite della parola[2]. Le tecnologie di sintesi vocale, infatti, oltre a vari usi commerciali (ad esempio, assistenti virtuali come Alexa), hanno interessanti applicazioni rivolte all'assistenza di persone con difficoltà di linguaggio. In particolare, tali device consentono alle persone di tornare ad esprimere oralmente la propria volontà grazie ad un "clone sintetico" della loro voce originale, ovvero una ricostruzione digitale delle caratteristiche della stessa prima che andasse perduta a causa di una malattia o di un incidente. Particolarmente interessante è, a questo proposito, la ricerca condotta da Google[3] con l'ex giocatore della NFL Tim Shaw, rimasto privo della sua voce dopo essere stato colpito dalla SLA (sclerosi laterale amiotrofica). Il progetto è consistito nel raccogliere le registrazioni vocali delle interviste di Shaw alla televisione nazionale americana per poi creare, grazie all'intelligenza artificiale (in particolare l'apprendimento automatico), un profilo vocale sintetico che imitasse il modo di parlare di Shaw in modo realistico e naturale. Attraverso una tecnologia chiamata clonazione vocale, Google ha dato a Shaw la possibilità di digitare frasi con un computer e di riprodurle con una versione sintetizzata del suono della sua voce così come era prima che la SLA gliela "portasse via".

[1] Il lavoro - frutto di un costante scambio tra gli autori - è stato sviluppato da Anna Anita Mollo per i §§ 2, 2.1, 3, 4, 5 e 6.2 e da Domenico Napolitano per i §§ 6.1. L'introduzione contenuta nel § 1 è il risultato di una stesura congiunta degli Autori.

[2] D. NAPOLITANO, *La voce artificiale. Un'indagine media-archeologica sul computer parlante*, Napoli, 2022.

[3] https://deepmind.com/blog/article/Using-WaveNet-technology-to-reunite-speech-impaired-users-with-their-original-voices (visitato il 30/06/2022). Un interessante esempio di questo progetto è riportato nel documentario "The Age of AI", disponibile online al sito: https://www.youtube.com/watch?v=V5aZjsWM2wo&ab_channel=YouTubeOriginals (visitato il 20/07/2022).

Nel presente lavoro cercheremo di mettere in evidenza diverse questioni che, sia in ambito giuridico che organizzativo, le tecnologie come quelle appena descritte pongono. Più in particolare, l'analisi giuridica sarà focalizzata sulle norme che regolano la successione a causa di morte nel nostro ordinamento giuridico, al fine di individuare quali limiti queste determinano per le persone con disabilità fisica rispetto alla possibilità di formalizzare un valido negozio testamentario. Successivamente, saranno illustrate le ricadute in ambito sociale di tale impianto normativo, con una riflessione critica sul modo di rappresentare la tecnologia come potenziante e migliorativa[4] per le persone con disabilità [5] nonostante l'attuale quadro normativo di riferimento non sempre consenta l'utilizzo di devices per l'espressione della volontà.

Ciò induce a riflettere sul rapporto tra diritto e tecnologia per valutare in che modo quest'ultima possa garantire la tutela dei diritti fondamentali delle persone con disabilità anche nell'ambito del diritto successorio.

Vi è, infatti, un vuoto di tutela in relazione alla possibilità di esprimere validamente la propria volontà per il tempo successivo alla morte per quelle persone che, a causa di patologie fortemente invalidanti abbiano perso alcune funzioni fisiche necessarie per esercitare la propria autonomia negoziale in una prospettiva *mortis causa,* sebbene siano capaci di agire o destinatarie di limitazioni che non rilevano dal punto di vista che qui si intende analizzare.

Tale ultimo aspetto è tanto più evidente in ambito successorio, dove il rigido formalismo che caratterizza sia gli ordinamenti di Civil Law che di Common Law[6], impedisce alle persone con disabilità di poter esprimere validamente la propria volontà.

Le ipotesi che vengono in rilievo sono molteplici: persone non più capaci di utilizzare gli arti superiori per apporre la propria firma o per redigere in forma olografa la scheda testamentaria; persone non più in grado di esprimersi con comunicazione verbale ma soltanto attraverso *devices* tecnologici.

In tutti questi casi, si intende valutare se sia ammissibile il ricorso ad una forma testamentaria, ancora non espressamente prevista in alcun ordinamento giuridico, che si potrebbe definire con espressione evocativa "testamento digitale", per fare in tal modo riferimento ad ogni ipotesi di testamento, scritto

---

[4] K. Richardson, *An Anthropology of Robots and AI. Annihilation Anxiety and Machines*, London, 2015.

[5] M. Alper, *Giving voice: Mobile Communication, Disability, and Inequality*. Cambridge, MA, 2017; K. Ellis, M. Kent, *Disability and New Media*, New York, 2011; I. Moser, *Disability and the Promises of Technology: Technology, Subjectivity and Embodiment within an Order of the Normal*, in *Information, Communication & Society*, 2006, vol. 9, III, 373–95; D. Napolitano, *Reuniting speech-impaired people with their voices: Sound technologies for disability and why they matter for organization studies*, in *PuntOorg International Journal*, 2022, vol. 7,I, 6-21.

[6] B.H. Mann, *Formalities and Formalism in the Uniform Probate Code*, in *University of Pennsylvania Law Review*, 1994, 1033; S.S. Boddery, *Electronic Wills. Drawing a Line in the Sand against their Validity*, in *Real Property Trust & Estate Law Journal*, 2013, 208; J. Banks, *Turning a Won't into a Will: Revisiting Will Formalities and E-Filing as Permissible Solutions for Electronic Wills in Texas*, in *Estate Planning and Community Property Law Journal*, 2015, 295; N. Banta, *Electronic Wills and Digital Assets: Reassessing Formality in the Digital Age,* in *Baylor Law Review*, 2019, 547-603; D. Horton, *Wills without signatures*, in *Boston University Law Review*, 2019, 1623-1685; M. Clark, *Avoiding Grave Consequences: Electronic Wills as a solution for Texas*, 2020 disponible online https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3534350 ; P.T. Wendel, *Testamentary Transfer and Intent versus Formalities Debate: The Case for a'Charitable' Common Ground*, in *Pepperdine University Legal Studies Research Paper,* 2020, 1-49; S.N. Gary, *The Electronic Wills Act: Facing the Inevitable*, 2020 disponible online https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3707246 ; A.J. Hirsch, *Models of electronic-will legislations*, in *Real Property, Trust and Estate Law Journal*, 2021, vol. 56, 163-235; J.C. Wilson , *Electronic Wills: why would Georgia choose to delay the inevitable?*, in *Mercer Law Review*, 2021, vol. 12, 337-364.

o orale, redatto con l'ausilio di strumenti tecnologici che consenta alle persone con disabilità di superare gli attuali limiti derivanti dal formalismo testamentario[7].

Dopo l'analisi del quadro giuridico si discuteranno una serie di implicazioni per le organizzazioni e la società, a partire dalle domande: l'innovazione tecnologica può da sola garantire un adeguato livello di autonomia alle persone con disabilità? Quale dovrebbe essere il tipo di interazione tra aziende tecnologiche, organizzazioni, individui e quadro giuridico di riferimento, che possa consentire un uso efficace delle tecnologie assistive nel rispetto della persona, evitando situazioni di vulnerabilità relazionale?

2. Il formalismo testamentario: tra ragioni storiche, stratificazioni normative e vuote formalità.

Il testamento è un negozio giuridico a causa di morte, ovvero ha la funzione di dare assetto ai rapporti della persona per quando questa avrà cessato di vivere (funzione successoria), ma anche di soddisfare il bisogno socialmente rilevante di disporre dei propri beni a favore di determinati beneficiari per il tempo successivo alla morte (funzione della liberalità successoria)[8].

Il negozio testamentario – oltre ad essere atto personalissimo, unilaterale, esclusivo, revocabile, patrimoniale – è atto formale[9] in quanto deve essere necessariamente fatto in una delle forme stabilite dalla legge.

Tutti gli ordinamenti giuridici, anche in diverse epoche storiche[10], hanno da sempre adottato quale principio cardine del diritto successorio quello del formalismo testamentario stante la cd. efficacia diacronica del negozio testamentario: in considerazione del fatto che gli effetti del testamento si produrranno soltanto dopo la morte del disponente, si vuole rende consapevole quest'ultimo dell'importanza delle conseguenze giuridiche che l'atto può determinare in un momento in cui egli non potrà più intervenire per modificarle[11].

---

[7] Sul punto I. SASSO, *Will Formalities in the Digital Age: Some Comparative Remarks*, in *The Italian Law Journal*, 2018, 171 utilizza l'espressione "*digital will*" in due distinti significati: come strumento per il trasferimento a causa di morte dei beni digitali; come documento redatto con l'ausilio di mezzi informatici ed elettronici e contenente disposizioni di ultima volontà.

[8] Così C.B. BIANCA, *Diritto civile*, *Le successioni*, Milano, 2022, 280.

[9] G. BRANCA, *Dei testamenti ordinari,* in *Comm. Scialoja e Branca, Artt. 601-608*, Roma, 1986, 60; C. CICALA, *Il formalismo testamentario. Il documento*, in G. BONILINI, *Trattato di diritto delle successioni e delle donazioni*, II, *La successione testamentaria*, Milano, 2009, 1253; P. BOERO, *Il testamento*, in R. CALVO E G. PERLINGIERI (a cura di) *Diritto delle Successioni*, Napoli, 2014, 773.

[10] Il formalismo trova origine nel diritto romano dove si ebbe il passaggio da riti arcaici tenuti in pubblico (il testamento *calatis comitiis*, ovvero dinanzi ai comizi curiati convocati due volte l'anno; il testamento *in procintu*, dinanzi all'esercito in partenza per una spedizione bellica; il testamento *per aes et libram*, con il quale attraverso la *mancipatio*, ovvero una vendita immaginaria, il testatore trasferiva il suo patrimonio ad un amico affinchè questi lo attribuisse secondo le disposizioni da lui impartite per il tempo successivo alla morte) a forme via via più semplificate tra cui nelle Istituzioni di Giustiniano (2.10.1 s.) si ricorda il testamento *ex edicto pretoris*, scritto ad opera del pretore su tavolette di cera con la firma di sette testimoni. Sul testamento romano E. VOLTERRA, *Istituzioni di diritto privato romano*, Roma, 1980, 738; M. TALAMANCA, *Istituzioni di diritto romano*, Milano, 1990, 716; M. AMELOTTI, *Testamento (diritto romano)*, in *Enc. Dir.*, 1992, XLIV, 459.

[11] Sulle ragioni del formalismo testamentario alcuni autori hanno affermato che esso sia funzionale alla tutela degli interessi degli eredi legittimi a conservare il patrimonio del testatore rispetto a possibili scelte avventate o sconsiderate; ciò sul presupposto della preminenza della successione legittima su quella

Il descritto formalismo, tuttavia, si pone come fonte di inaccettabili lesioni pregiudizievoli dei diritti delle persone con disabilità come è facile comprendere dalla lettura delle norme dell'ordinamento giuridico italiano, dove il formalismo appare essere particolarmente rigido e non diversamente superabile.

Si tratta di un impianto normativo particolarmente complesso anche in ragione delle diverse fonti, che devono essere tra loro coordinate, da cui deriva la disciplina:

- il libro secondo del codice civile
- la legge 16 febbraio 1913, n. 89, regolatrice della funzione notarile

Il principio fondamentale stabilito in tali testi normativi è quello della forma scritta *ab substantiam* del negozio di ultima volontà, non potendo il disponente redigere un testamento in forma orale[12]. Inoltre, il testatore deve (le norme sono inderogabili) utilizzare una delle seguenti forme:

- testamento pubblico (art. 603 c.c.) ricevuto dal notaio al quale il testatore, in presenza di almeno due testimoni, dichiara le sue volontà che sono ridotte per iscritto dal notaio. Il testamento deve poi essere sottoscritto dal testatore, dai testimoni, e dal notaio;
- testamento olografo (art. 602 c.c.) scritto per intero, datato e sottoscritto di mano del testatore;
- testamento segreto (art. 604 c.c.) che si compone di due parti: la scheda testamentaria (può essere scritta sia dal testatore che da terzi, anche con mezzi meccanici, ma sempre su supporto cartaceo) e l'atto di ricevimento da parte del notaio che sigilla la scheda (alla presenza necessaria dei testimoni).

Laddove non siano rispettate le formalità sopra indicate, il codice civile all'art. 606 stabilisce che:

- il testamento olografo è nullo quando manca l'autografia o la sottoscrizione

testamentaria. Così G. STOFLI, *Teoria del negozio giuridico*, Padova, 1947,172; P. RESCIGNO, *Ultime volontà e volontà della forma*, in *Vita not.*, 1987, 10. Secondo altra interpretazione, invece, più ampiamente condivisa in dottrina, il formalismo trova fonte nella duplice funzione del testamento, una di carattere sostanziale, attinente alla garanzia di una più accorta formulazione della volontà da parte del testatore; una di carattere processuale, ovvero la creazione di un documento che provi la reale volontà del disponente. In tal senso M. ALLARA, *Il testamento*, Padova, 1936, 232-233; F. SANTORO PASSARELLI, *Dottrine generali del diritto civile*, Napoli, 1997, 222.

[12] Anche detto "testamento nuncupativo", dal diritto romano che consentiva la proclamazione solenne e pubblica dell'erede testamentario. Nell'ordinamento giuridico italiano, secondo la tesi consolidata in dottrina e in giurisprudenza, il testamento redatto in forma orale non è nullo ma del tutto inesistente, in quanto la mancanza della forma scritta non può qualificarsi come un vizio che da luogo all'invalidità dell'atto ma rappresenta elemento che impedisce di rinvenire nel caso di specie qualsiasi requisito seppur minino che ne consenta la qualificazione giuridica in termini di negozio testamentario. Così F. SANTORO PASSARELLI, *Dottrine generali*, cit., 243; C. GANGI, *La successione testamentaria nel vigente diritto italiano*, I, Milano, 1964, 239; A. CICU, *Testamento*, Milano, 1951, 55-56. In giurisprudenza Trib. Trani, 28 luglio 1950, in *Dir. e giur.*, 1950, 419; Trib. Bergamo, 7 novembre 1994, in *Notariato*, 1996, 506 ss. Secondo la tesi minoritaria, il testamento orale, nullo per mancanza di forma, sarebbe convalidabile ai sensi dell'art. 590 c.c. In tal senso C.M. BIANCA, *Diritto civile. La famiglia. Le successioni*, 2, Milano, 640; A. VENDITTI, *Disposizione testamentaria orale e conferma*, in *Dir. e giur.*, 1988, 68 ss.; F. GAZZONI, *L'attribuzione patrimoniale mediante conferma*, Milano, 1974, 141 ss. Nello stesso senso anche alcune sentenze della Corte di Cassazione tra cui Cass., 16 maggio 1941, n. 1476; Cass, 5 maggio 1962, n. 888; Cass., 26 giugno 1964, n. 1689; Cass., 9 ottobre 1972, n. 2958; Cass., 11 luglio 1996, n. 6313, in *Notariato*, 1996, 509 ss.

- il testamento pubblico e il testamento segreto sono nulli quando manca la redazione per iscritto, da parte del notaio, delle dichiarazioni del testatore ovvero la sottoscrizione del notaio o del testatore

Si consideri inoltre che, in applicazione del principio di equipollenza delle forme testamentarie, queste sono tra loro autonome e distinte quanto ai requisiti ma anche equivalenti, perché producono tutte i medesimi effetti.

In altre parole, non essendovi una gerarchia il futuro *de cuius* può scegliere in totale autonomia, salvo i limiti di legge, in quale forma redigere il suo testamento.

Tale affermazione, tuttavia, pare essere smentita propria in considerazione della particolare fattispecie in cui a voler redigere il proprio atto di ultima volontà sia una persona con disabilità, come si cercherà di illustrare nei paragrafi che seguono.

2.1 Le ulteriori formalità in caso di testamento di persona con disabilità.

Per poter redigere un valido negozio testamentario occorre essere titolari della c.d. capacità di testare (art. 591 c.c.), quale espressione della capacità di agire (art. 2 c.c.), ovvero della idoneità a disporre delle proprie sostanze mediante testamento.

La capacità di testate spetta anche a chi ha una ridotta capacità di agire (come nel caso degli inabilitati e dei beneficiari dell'amministrazione di sostegno) e il relativo accertamento al momento della redazione del negozio testamentario spetta al notaio.

Pertanto, laddove ricorra la capacità di testare il disponente dovrebbe avere il diritto di perfezionare un valido negozio testamentario, anche in presenza di una disabilità fisica.

Al riguardo occorre precisare che sia il codice civile che la legge notarile prevedono regole ulteriori per consentire alle persone con disabilità fisica di poter regolarmente essere parte di un atto pubblico rogato da notaio.

Tuttavia, si tratta di una disciplina parziale, che tipizza alcune ipotesi che non sono idonee a ricomprendere tutte le fattispecie astrattamente possibili, impedendo in tal modo una tutela generalizzata del diritto del disponente di poter redigere un valido negozio testamentario prescindendo dalla sua disabilità fisica.

Si tratta delle ipotesi in cui la parte sia sorda, muta o cieca.

Più in particolare:

I. parte sorda, interamente priva dell'udito e che non può sentire quanto dichiarato dal notaio. L'art. 56, commi 1 e 2 L. Not. prevede al riguardo che
   - se la parte sorda *sa e può leggere*, deve personalmente leggere l'atto e di ciò ivi si farà menzione;
   - se la parte sorda *non sa leggere*, deve intervenire all'atto un interprete che sarà nominato dal Presidente del Tribunale tra le persone abituate a trattare con esso e che sappia farsi intendere dal medesimo con segni e gesti.

II. parte muta, l'art. 57 L. Not. oltre a richiamare la presenza dell'interprete di cui al precedente articolo 56 L. Not. distingue due ipotesi
   - se la parte *sa leggere e scrivere*, deve egli stessa leggere l'atto e scrivere alla fine del medesimo, prima delle sottoscrizioni, che lo ha letto e riconosciuto conforme alla sua volontà
   - se la parte *non sa o non può leggere e scrivere*, sarà necessario che il linguaggio a segni e gesti della parte sia inteso anche da uno dei testimoni o che intervenga all'atto un secondo interprete.

III. parte cieca, persona che non può leggere l'atto notarile sebbene in grado di leggere altri documenti con l'ausilio del codice Braille[13]. In questo caso, la legge 3 febbraio 1975, n. 18 richiede:
   - la necessaria presenza di un assistente del cieco scelto tra le persone di sua fiducia laddove questi ne faccia espressa richiesta;
   - la presenza obbligatoria di due assistenti del cieco quando questi non sia in grado di apporre la firma

Infine, tutte le formalità indicate debbono coordinarsi, nel caso del testamento pubblico, con l'art. 603 c.c. che prescrive il necessario intervento in atto di ben quattro testimoni laddove il testatore (sordo, muto o cieco) sia anche incapace di leggere, per qualsiasi motivo anche transitorio.

3. Le persone con disabilità e l'autonomia testamentaria: quali limiti?

All'esito della sintetica analisi di tutte le formalità richieste dalle norme di diversa fonte nell'ambito dell'ordinamento giuridico italiano, sembra emerge che:

- il testamento olografo non può essere fatto da chi *non sa o non può scrivere;*
- il testamento segreto non può essere fatto da chi non sa o può leggere e non può sottoscrivere la scheda testamentaria
- il testamento pubblico consente, rispettando le formalità previste dalla legge notarile, di superare sia l'impossibilità o incapacità di leggere sia l'incapacità di scrivere e sottoscrivere.

Pertanto, non solo nelle ipotesi di persona sorda, muta o cieca, ma in tutti i casi in cui il soggetto non riuscisse ad utilizzare gli arti superiori per scrivere e apporre la sua firma in calce alla scheda testamentaria non potrebbe che ricorrere unicamente al testamento pubblico.

Tale scelta diventa obbligata in quanto unica forma in cui è possibile esprimere la volontà pur senza apporre la sottoscrizione all'atto redatto dal notaio.

Tale dato rende già evidente che per le persone con disabilità non sia garantito il diritto di poter liberamente scegliere tra le varie forme di testamento previste, determinando in tal modo una diseguaglianza irragionevole. Ciò non può che qualificarsi come mera discriminazione fondata

[13] G. CASU, *L'atto notarile tra forma e sostanza*, Milano, 1996, 93.

sulla disabilità[14], che diventa tanto più evidente se si considera che pur essendo possibile formalizzare la propria volontà in un testamento pubblico senza apporre la sottoscrizione, dall'altro lato il notaio deve necessariamente in questo caso specificare in atto la causa che impedisce la sottoscrizione, in applicazione dell'art. 51, 2 comma n. 10 Legge notarile.

I limiti posti dal formalismo testamentario diventano macroscopici laddove si prendano in considerazione fattispecie in cui la disabilità è tale da impedire non solo la sottoscrizione dell'atto ma anche la stessa comunicazione verbale da parte del disponente.

Nel testamento pubblico, infatti, il testatore deve dichiarare la sua volontà al notaio. Tuttavia, il codice non specifica in che modo tale volontà debba essere dichiarata ovvero resa manifesta.

Sul punto appare evidente che una interpretazione evolutiva della norma, che tenga conto dello sviluppo tecnologico, si imponga proprio a tutela delle persone con disabilità.

Ciò è quanto fatto dalla giurisprudenza di merito di alcuni Tribunali italiani che in diverse occasioni hanno avuto modo di pronunciarsi in relazione alla particolare fattispecie di persone con sclerosi laterale amiotrofica (SLA) che avevano perduto l'uso della parola.

Le soluzioni proposte sono, tuttavia, diverse e per certi versi divergenti.

In una prima sentenza, infatti, il Tribunale di Varese[15] ha consentito alla persona con SLA di esprimere validamente la sua volontà testamentaria a mezzo di un comunicatore oculare (Eye tracking), autorizzando poi il curatore speciale nominato *ad hoc* di formalizzare tale volontà in un testamento olografo. Tale conclusione è stata motivata sulla base dell'esistenza per le persone affette da SLA di un vero e proprio diritto alla «*comunicazione non verbale*», non ritenendosi ammissibile che un soggetto perda la capacità di testare a causa della sua malattia in quanto ciò comporterebbe una discriminazione fondata sulla disabilità.

Successivamente, il Tribunale di Milano[16] ha in parte modificato tale approccio in quanto, pur confermando che debba essere sempre riconosciuto il diritto di fare testamento anche quando la persona con SLA non possa comunicare nelle forme convenzionali, ha ritenuto in tali casi necessario il ricorso al testamento pubblico, sulla base della maggior tutela della volontà e degli interessi del disponente che la figura professionale del notaio potrebbe garantire rispetto alla forma del testamento olografo.

Lo stesso orientamento è stato poi confermato anche dal Tribunale di Venezia[17] precisando che, per coloro che si esprimono per il tramite di un puntatore oculare, non è necessaria la nomina giudiziale dell'interprete ai sensi

[14] Ai sensi dell'art. 2 Convenzione delle Nazioni Unite sui diritti delle persone con disabilità per «discriminazione fondata sulla disabilità si intende qualsivoglia distinzione, esclusione o restrizione sulla base della disabilità che abbia lo scopo o l'effetto di pregiudicare o annullare il riconoscimento, il godimento e l'esercizio, su base di uguaglianza con gli altri, di tutti i diritti umani e delle libertà fondamentali in campo politico, economico, sociale, culturale, civile o in qualsiasi altro campo. Essa include ogni forma di discriminazione, compreso il rifiuto di un accomodamento ragionevole».

[15] Trib. Varese, 12 marzo 2019, in banca dati *Pluris*.

[16] Trib. Milano, del 24 febbraio 2015, provvedimento n.11965/2011 V.G., in banca dati *Pluris*.

[17] Trib. Venezia, del 11 aprile 2017, provvedimento n. 967/2017 in banca dati *Pluris*.

degli articoli 56 e 57 Legge notarile per essere parte di un atto pubblico, in quanto la funzione svolta dall'interprete nulla aggiungerebbe rispetto alla comprensione da parte del notaio della volontà in tal modo espressa, già resa intellegibile per il tramite del lettore oculare.

Le sentenze analizzate esprimono una posizione condivisibile rispetto al corretto bilanciamento di interessi che dovrebbe caratterizzare la materia successoria, specie con particolare riferimento alle persone con disabilità.

Se da un lato, infatti, i giudici hanno riconosciuto l'importanza ed il valore della tecnologia come mezzo di ausilio per agevolare l'espressione della propria volontà, dall'altro hanno posto l'attenzione sulla centralità della figura del notaio come garante della tutela effettiva e necessaria in tale ambito anche per le persone con disabilità.

Tale funzione, tuttavia, non pare possa essere effettivamente perseguita alla luce di un rigido impianto normativo che, nonostante la giurisprudenza innanzi analizzata, si basa ancora sul rispetto del formalismo testamentario che il notaio non può disattendere.

Una parziale apertura all'utilizzo della tecnologia per esprimere validamente la propria volontà si è avuta con la legge 22 dicembre 2017, n. 219, che al sesto comma dell'articolo 4, prevede espressamente che le disposizioni anticipate di trattamento – intese come le volontà espresse dal soggetto interessato in materia di trattamenti sanitari in previsione di un'eventuale futura incapacità di autodeterminarsi – possono essere espresse anche attraverso videoregistrazione o dispositivi che consentono alla persona con disabilità di comunicare nel caso in cui le condizioni fisiche del paziente non lo consentano più.

La tecnologia viene in questo caso presa in considerazione non in una prospettiva successoria ma con l'intento di tutelare adeguatamente il valore fondamentale della libertà di formazione ed espressione della propria volontà in relazione alla sfera personale e non patrimoniale, per dare così effettività a diritti di rango costituzionale (artt. 2, 13, 32 Cost.) e riconosciuti come diritti fondamentali dell'Unione Europea (art. 1,2 e 3 Carta diritti fondamentali UE) – vita, salute, dignità ed autodeterminazione – stabilendo che nessun trattamento sanitario possa essere iniziato o proseguito senza il consenso libero ed informato della persona interessata.

A questo primo passo fatto dal legislatore italiano, tuttavia, non è seguito un intervento riformatore più ampio del diritto successorio, nel senso di eliminare o almeno mitigare il formalismo testamentario.

Ciò crea una evidente lesione del principio di autodeterminazione che trova la sua più evidente espressione nell'autonomia privata, quale potere del soggetto di disporre dei propri diritti. Tale potere si esercita attraverso il negozio giuridico – categoria ampia della quale il testamento fa parte[18] - inteso quale autoregolamentazione di privati interessi.

Nel potere di autonomia privata, dunque, si ritrova lo stesso fondamento del diritto di testare (autonomia testamentaria).

[18] A. CICU, *Il testamento*, cit., 19; L. CARIOTA-FERRARA, *Le successioni per causa di morte*, Napoli, 1972, 180; L. MENGONI, *Successioni per causa di morte. Parte speciale (Successione legittima)*, Napoli, 1999, 20; C.M. BIANCA, *Diritto civile. Le successioni, 2.2.*, cit., 280 ss.

Non si comprende, pertanto, per quale ragione il diritto all'autodeterminazione delle persone con disabilità debba trovare tutela soltanto in relazione ad alcuni aspetti relativi alla sfera personale (di cui alla legge 22 dicembre 2017, n. 219), e non anche attraverso il negozio testamentario. Tale assetto del diritto successorio comporta una disparità di trattamento tra soggetti in considerazione delle precise caratteristiche fisiche di ciascuno. Per le persone con disabilità, infatti, il potere di autonomia privata trova un limite evidente nell'impossibilità di poter scegliere in quale forma esprimere la propria volontà per il tempo successivo alla morte. Ciò determina la lesione di principi fondamentali sui quali si fonda il nostro ordinamento giuridico, primo fra tutti il principio di uguaglianza.

4. Il possibile ruolo della tecnologia in materia successoria: brevi profili di comparazione.

La tecnologia si pone come elemento di forte progresso della società contemporanea ma per le persone con disabilità può rappresentare strumento necessario per consentire il recupero di funzioni fisiche utili al mantenimento di un adeguato grado di indipendenza ed autonomia.

Più in particolare, l'utilizzo di devices tecnologici, anche potenziati grazie all'intelligenza artificiale, può diventare rilevante in due distinti fasi del procedimento di formazione ed espressione della volontà testamentaria. L'attuale progresso della ricerca scientifica in campo medico ha infatti consentito di poter impiegare per la diagnosi ed il trattamento di patologie neurodegenerative gravemente invalidanti, che tolgono ogni possibilità di espressione alla persona, tecniche in grado di consentire percorsi di comunicazione diretti con il cervello umano per rilevare il segnale celebrale e, in tal modo, decodificare un determinato percorso di comunicazione della persona interessata con il mondo esterno (tecniche di BCI_fig. n. 1).

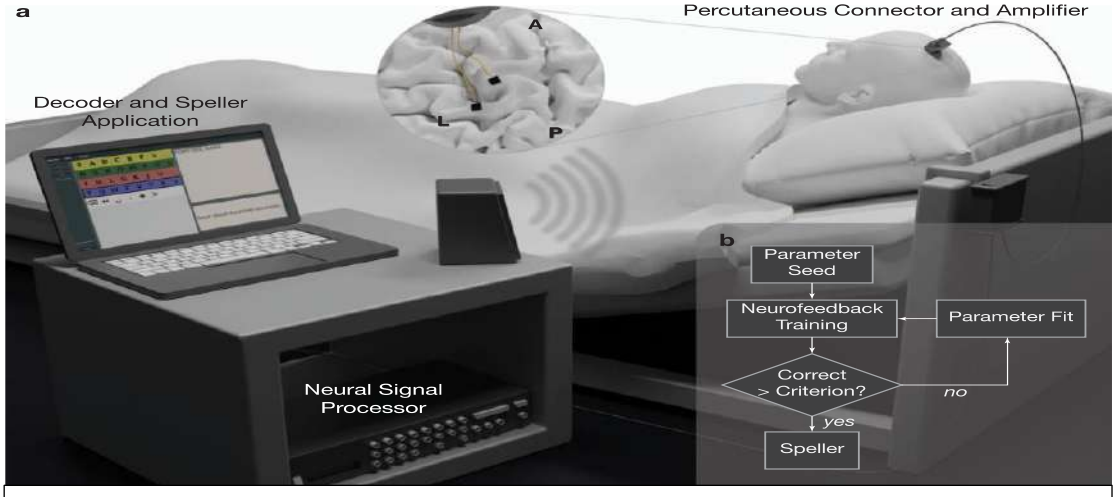


Fig. n.1 L'immagine rappresenta uno studio su un paziente con SLA sottoposto a tecniche di BCI per selezionare le lettere una alla volta e formare parole e frasi per comunicare i suoi bisogni e le sue esperienze. Questo caso di studio dimostra che la comunicazione volitiva basata sul cervello è possibile anche in uno stato di blocco totale.
CHAUDHARY, U., VLACHOS, I., ZIMMERMANN, J.B. *et al.*, "Spelling interface using intracortical signals in a completely locked-in patient enabled via auditory neurofeedback training", *Nature Communications*, 13, 1236, 1-9 https://www.nature.com/articles/s41467-022-28859-8



Fig. n. 2 Eye tracking usato dalle persone con sla

Il comunicatore a puntatore oculare (Eye tracking_fig. n. 2) è soltanto una delle possibilità oggi a disposizione delle persone con SLA per esprimersi e comunicare con il mondo esterno. Le fattispecie rilevanti possono essere tante, anche relative a patologie diverse e per le quali l'evoluzione tecnologica mette a disposizione tecniche in continuo perfezionamento e con diversi gradi di invasività.

Il secondo profilo, che è quello maggiormente rilevante ai fini del presente lavoro, attiene all'impiego di devices tecnologici non per la decodifica dell'attività celebrale utile ai fini della comunicazione – anche non verbale – quanto per la raccolta della volontà in tal modo espressa.

In altre parole, si potrebbe astrattamente immaginare un doppio livello di efficacia della tecnologia rispetto alle persone con disabilità: in un primo momento per favorire la manifestazione verso l'esterno della propria volontà naturalmente formatasi (evitando che questa sia eterodeterminata); in secondo luogo, come mezzo attraverso il quale "*conservar*e" la volontà, per poterle dare la forma di un testamento.

Il *focus* di quest'ultima riflessione si rinviene, dunque, nella possibilità di provare ad immaginare la compatibilità giuridica di un negozio testamentario redatto in una forma che non è quella dell'atto pubblico notarile così come attualmente disciplinata.

Gli spunti al riguardo nascono anche dalla lettura in chiave comparatistica dell'evoluzione in materia successoria in altri ordinamenti giuridici. Più in particolare, negli Stati Uniti quattro Stati - Nevada[19], Arizona[20], Florida[21], Indiana[22] - hanno adottato specifici atti legislativi per consentire la valida formazione di «electronic will» – testamento elettronico – che deve essere scritto e memorizzato su un disco elettronico, datato e firmato dal testatore, dal notaio e dai testimoni. Rispetto a questi ultimi, soltanto il Nevada, la Florida e l'Indiana prevedono che i testimoni possano trovarsi anche in luogo diverso da quello in cui si trovano il testatore ed il notaio a condizione che siano soddisfatti determinati requisiti[23].

In altri Stati, come in New Hampshire, Virginia, Washington D.C, sono state presentate proposte di legge ancora in discussione in cui è prevista la

[19] La prima legge sul testamento elettronico in Nevada risale al 2001 ma dal 1 luglio 2017 è stata sostituita da una nuova legge Nevada Electronic Wills Statute, Nevada Revised Statutes, § 133.085, 133.086 e 133.088 disponibile qui https://www.leg.state.nv.us/nrs/nrs-133.html. In dottrina sul punto G.W. BEYER E K.V. PETERS, *Sign on the electronic dotted line: the rise of the Electronic Will*, 2019, 1-12, disponible qui https://ssrn.com/abstract=3278363; sulla prima versione della legge G.W. BEYER E G.G. HARGROVE, *Digital Wills: has the time come for willa to join the digital revolution?*, in *Ohio Northen University Law Review*, 2007, 865.

[20] La legge adottata nel 2017 in Arizona è entrata in vigore il 1 luglio 2019, Ariz. Rev. Stat. Ann. § 14-2504, 14-2518 A 3(a) e 14-2519.

[21] F.S.A. § 117.265, 117.285, 732.502, 732.522 (2) e 732.522 entrata in vigore il 1 luglio 2020

[22] Ind. Code Ann. § 29-1-21-3(6). In Indiana la prova dell'integrità del documento prevede l'utilizzo di marcatori digitali per dimostrare che il testamento non è stato alterato dopo la sua esecuzione.

[23] Per l'Indiana *Indiana House Enrolled Act 1255*

necessaria firma elettronica di due testimoni e del notaio in presenza del quale il testatore deve aver apposto la sua firma.

Da ultimo, in considerazione del crescente proliferare di leggi e proposte di leggi sul testamento elettronico, nel 2019 The Uniform Law Commission[24] ha adottato una proposta di legge uniforme - The Uniforma Electronic Wills Act_Uniform Act[25] - che riconosce la possibilità di formalizzare i testamenti creati su un *computer* o su altro dispositivo portatile digitale non cartaceo, firmati elettronicamente dal testatore, alla presenza fisica o virtuale di testimoni (scelta quest'ultima rimessa agli Stati che promulgano la legge uniforme che attualmente sono tre: Colorado, North Dakota e Utah). Ciò senza la necessaria presenza di un notaio, ma anche rivolgendosi ad aziende specializzate che offrono servizi di archiviazione di testamenti elettronici.

Tale soluzione è certamente criticabile dal punto di vista della debole garanzia di tutela offerta, aprendo il campo al mercato dei testamenti online redatti senza alcuna assistenza giuridica sul punto e senza alcuna sicurezza della corretta conservazione dell'atto di ultima volontà in tal modo formato.

Tale timore pare confermato anche dalla lettura della decretazione d'urgenza durante il periodo pandemico[26].

Un approccio diverso, teso a valorizzare solo entro ristretti limiti l'impiego della tecnologia in materia successoria con l'intento di salvaguardare il più possibile l'espressione di volontà del disponente, è quello che caratterizza le scelte dei legislatori australiani e canadesi[27].

In entrambi i casi, infatti, non è stata promulgata alcuna legge che ritiene validi i testamenti elettronici ma si riconosce il principio - c.d. «harmless-error rule» - per il quale è il Tribunale che può dare effetto al testamento elettronico, ciò solo nella misura in cui il giudice ritenga che il testamento sia autentico, ovvero espressivo delle reali intenzioni del testatore senza alcuna interferenza esterna. Ciò come meccanismo correttivo per l'annullamento di testamenti elettronici formati in modo improprio.

Tuttavia, la harmless-errore rule, con il diverso nome di «dispensing power rule»[28], esiste anche in diversi Stati Americani e in versioni differenti, ma tutte hanno avuto origine dall' Uniforme Probate Code (section 2-503) che considera valido il testamento redatto senza rispettare le formalità richieste soltanto

[24] Si tratta di un'associazione americana senza scopo di lucro nata con l'intento di promuovere l'uniformazione legislativa nelle aree del diritto statale in cui maggiormente sarebbe auspicabile.

[25] In senso critico sulla legge uniforme J.A. HIRSCH, *Technology Adrift: In Search of a Role for Electronic Wills*, in *Boston College Law Review 827*, 2020, 846-851; A.J. HIRISCH E J.C. KELETY, *The Uniform Act versus Autralian and Canadian Alternatives*, in *Probate & Property*, 2020, 1-18.

[26] In ben diciassette Stati sono stati richiesti adempimenti ulteriori per consentire che l'attività notarile da remoto offrisse le stesse garanzie di quella svolta in presenza. Un elenco completo è stato elaborato dall'*American College of Trust and Estate Counsel* (ACTEC), un'associazione senza scopo di lucro di avvocati e professori esperti nella preparazione di testamenti e trust, nella pianificazione successoria e nell'amministrazione di trust ed eredità di deceduti, minori e incapaci. L'elenco è disponibile al seguente link https://www.actec.org/resources/emergency-remote-notarization-and-witnessing-orders/. Il caso indiano è trattoto da N. ANAND E D. ARORA, *Where there is a will, there is no way: covid-19 and a case for the recognition of e-wills in India and other Common Law jurisdictions*, in *ILSA Journal of International & Comparative Law*, 2020, 77-94.

[27] A.J. HIRISCH E J.C. KELETY, *The Uniform Act versus Australian and Canadian Alternatives*, cit., pp. 1-18.

[28] M. ZATUCKI, *Wills Formalities versus Testator's Intention. Functional model of effective testation for informal wills*, Baden, 2021, 85-95.

laddove esista una prova certa che il documento in questione contenga la reale volontà del disponente[29].

Spostando lo sguardo dal nord al sud degli Stati Uniti, si sottolinea come con la riforma del Codice Civile peruviano del 2012 in materia di successioni testamentarie, si è aperto un nuovo orizzonte per le persone ipovedenti, consentendo loro di poter perfezionare testamenti, sia segreti che olografi, utilizzando il codice Braille [30]. In relazione alla medesima fattispecie, nella recentissima sentenza della Corte Costituzionale della Colombia emessa lo scorso mese di marzo, si è affermato che dall'art. 1076 del Codigo Civil va espunto l'avverbio "solo" con riferimento al testamento innanzi al notaio come unica forma possibile per le persone ipovedenti. Al contrario, conformemente anche a quanto stabilisce la legge colombiana n. 1996 del 2019, gli adulti con qualsiasi tipo di disabilità devono avere accesso per esprimere la propria volontà a qualsiasi strumento di comunicazione a loro disposizione, incluso il sistema Braille e la lingua dei segni colombiana.

Quanto detto fino a questo momento si riferisce ad ipotesi in cui il testamento, sebbene in formato digitale, riproduca in ogni caso in forma scritta la volontà del disponente.

Tuttavia, il vero punto di svolta sarebbe riconoscere validità ad un testamento redatto in forma orale e con l'ausilio della tecnologia.

Allo stato nessun ordinamento ha adottato una legge in merito sebbene l'Australia, nella medesima – sebbene riduttiva – prospettiva della harmless-error rule ammette che i Tribunali possano riconoscere validi in quanto espressivi della reale volontà del disponente non solo i testamenti elettronici scritti ma anche quelli redatti per il tramite di una mera registrazione audio e/o video (anche se realizzata in proprio dal disponente con un semplice iPhone) [31].

Tale approccio, pertanto, per quanto complesso, ha il pregio rispetto all'Uniform Act americano prima analizzato, di evitare che le aziende commercializzino testamenti elettronici per consumatori vulnerabili poco consapevoli delle conseguenze connesse alle proprie dichiarazioni. Dall'altro lato, però, non riconosce una regola di generale validità del testamento in forma digitale.

Ciò che sembra emergere dall'analisi comparatistica è che, sebbene la fattispecie del testamento videoregistrato potrebbe garantire alle persone con disabilità la più ampia libertà dal formalismo testamentario, tale ipotesi necessita di una adeguata regolamentazione di fonte legislativa.

In ogni caso, il valore positivo che la tecnologia può apportare al diritto successorio sembra innegabile, così come lo sono le esigenze di riforma in tale ambito, confermate anche dal confronto con altri ordinamenti giuridici.

---

[29] Con particolare riguardo al profilo probatorio in giudizio e ai rischi che tale regola potrebbe determinare D. NORTON, *Partial Harmless Error for Wills: Evidence from California*, in *Iowa L. Rev. 2027*, 2018, 2058-2065, disponibile qui https://ilr.law.uiowa.edu/assets/Uploads/ILR-103-5-Horton.pdf .

[30] Sul punto L.P. PEREZ GALLARDO,Testamentos ológrafo y cerrado en braille en el derecho peruano, in *Revista de Derecho Privado*, 2017, 3-29.

[31] A.J. HIRISCH E J.C. KELETY, cit., precisano che la regola adottata nell'ordinamento australiano ha determinato dal 2020 ad oggi la pubblicazione, come validi, otto testamenti elettronici e undici testamenti audio e video.

5. Il superamento del formalismo testamentario in conformità alla Convenzione delle Nazioni Unite sui diritti delle persone con disabilità.

Un dato normativo molto forte che potrebbe supportare la validità giuridica di un "testamento digitale" è rappresentato dalla Convenzione delle Nazioni Uniti sui diritti delle persone con disabilità la cui *ratio* non si ritrova nel riconoscere "nuovi diritti" alle persone con disabilità, ma nel rendere queste ultime in grado di godere degli stessi diritti riconosciuti agli altri consociati in condizione di pari opportunità.

I principi ispiratori della Convenzione sono, infatti, quelli di autonomia, uguaglianza e non discriminazione delle persone con disabilità, che si riflettono in primo luogo nella libertà di poter compiere le proprie scelte in maniera autonoma (art. 3 lett. A).

Ciò comporta che nelle attività ufficiali debba essere garantito alle persone con disabilità il ricorso ad ogni mezzo di comunicazione che consenta di esprimere le scelte assunte, ricorrendo a tale scopo non solo alla lingua dei segni, al Braille o altre forme note di comunicazione ma anche «alle comunicazioni aumentative ed alternative e ad ogni mezzo, modalità e sistema accessibile di comunicazione di loro scelta» (art. 21, lett. b).

Appare evidente, tuttavia, come tale principio, che pure è stato recepito da una pluralità di Stati tra cui l'Italia con legge 3 marzo 2009, n. 18[32], resti ancora inattuato in sistemi che richiedono forme testamentarie non accessibili alle persone con disabilità.

Ciò rende gli ordinamenti in parola inadempienti rispetto a precisi obblighi giuridici che impongono espressamente di adottare tutte le misure legislative per attuare i diritti riconosciuti dalla Convenzione e per «abrogare qualsiasi legge, regolamento, consuetudine e pratica vigente che costituisca una discriminazione nei confronti delle persone con disabilità» (art. 4, lett. b).

Pertanto, l'attuale formalismo testamentario pare porsi come vera e propria «discriminazione fondata sulla disabilità» che va a ledere la dignità delle persone con disabilità, disattendendo il principio fondamentale della Convenzione (art.1).

Infine, appare necessario sottolineare che tra gli obblighi imposti dalla Convenzione vi sia quello di «promuovere la disponibilità e l'uso di nuove tecnologie […] dando priorità alle tecnologie dai costi più accessibili» (art. 4 lett. g).

Non si comprende allora quale sia il vero ostacolo all'accoglimento di una modifica legislativa che consenta di dare ingresso a nuove forme testamentarie che trovino nella dimensione tecnologica la principale modalità di perfezionamento (testamento digitale).

Osservando la questione da un diverso angolo prospettivo, appare evidente che un effettivo rinnovamento del diritto successorio grazie all'ausilio della tecnologia richieda un difficile bilanciamento di interessi tra diverse e complesse esigenze di tutela: da un lato, la necessità di garantire la piena autonomia alle persone con disabilità anche in materia successoria; dall'altro,

[32] Sulla «sostanziale indifferenza dell'ordinamento giuridico italiano» sulla Convenzione delle Nazioni Unite sui diritti delle persone con disabilità V. BARBA, *Persone con disabilità e capacità. Art. 12 della Convenzione sui diritti delle Persone con Disabilità e diritto civile italiano*, in *Rassegna di diritto civile*, 2, 2021, 419 – 449.

evitare fenomeni come il digital divide (mancata formazione sull'utilizzo dei devices, mancanza delle possibilità economiche per accedervi) nonché rischi tecnici pregiudizievoli (scarso livello di sicurezza nella conservazione della scheda testamentaria, possibile accesso indesiderato al testamento da parte di terzi prima dell'apertura della successione con conseguente possibile manomissione del relativo contenuto; futura inutilizzabilità del testamento a causa dell'obsolescenza del devices utilizzato).

Tali rischi, tuttavia, non sembrano dissimili da quelli che tradizionalmente caratterizzano il testamento in forma olografa: anche in questo caso la scheda testamentaria non custodita correttamente dal disponente potrebbe andare irrimediabilmente perduta; così come è noto che proprio i testamenti olografi sono la principale causa del contenzioso in materia successoria, in quanto redatti dal testatore senza l'ausilio ed il supporto giuridico del notaio, con conseguente formazione di voluti testamentari non sempre conformi ai principi su cui si basa il diritto successorio (si pensi alla disciplina a tutela dei legittimari e ad eventuali disposizioni lesive dei loro diritti redatte da chi non ha una conoscenza giuridica adeguata sul punto).

Eppure, questi stessi rischi, del tutto assimilabili a quelli sinteticamente elencati per il testamento digitale, non hanno mai messo in dubbio la legittima permanenza del testamento olografo all'interno degli ordinamenti giuridici.

6. Conclusioni.

6.1 Prospettiva organizzativa.

Quanto abbiamo analizzato sopra in merito alle norme sulla successione a causa di morte rispetto alle nuove sfide delle tecnologie avanzate ha importanti conseguenze dal punto di vista degli studi organizzativi. Le norme sulla successione a causa di morte, infatti, possono essere viste come parte di un progetto più ampio di inclusione delle persone con disabilità nella vita sociale, come quello proposto dalla Convenzione delle Nazioni Unite (2007). Le organizzazioni svolgono un ruolo decisivo nell'inclusione delle persone con disabilità, come sottolineato da un recente filone di letteratura. [33] Le tecnologie, invece, si trovano in una posizione di confine: sono considerate strumenti indispensabili per l'accessibilità e l'*empowerment* delle persone con disabilità[34]; tuttavia, la letteratura ha sottolineato come la tecnologia da sola non sia sufficiente a produrre un'adeguata inclusione e a garantire una vita

[33] E. JAMMAERS, *Theorizing Discursive Resistance to Organizational Ethics of Care Through a Multi stakeholder Perspective on Disability Inclusion Practices*, in *Journal of Business Ethics*, online first, 2022, doi: 10.1007/s10551-022-05079-0; E. JAMMAERS E P. ZANONI, *The Identity Regulation of Disabled Employees: Unveiling the "varieties of ableism" in employers' socio-ideological control*, in *Organization Studies* 2021, 42, 429-453; D. KNIGHTS E Y LATHAM, *Disabled People and Digitalization: Disruptive documents in distributing digital device*, in *Organization Studies,* 2021, 41, 855-872; K. VAN LAER, E. JAMMAERS, W. HOEVEN, *Disabling organizational spaces: Exploring the processes through which spatial environments disable employees with impairments*, in *Organization*, 2020, 1-18; J. WILLIAMS, S. MAVIN, *Disability as Constructed Difference: A Literature Review and Research Agenda for Management and Organization Studies*, in *International Journal of Management Reviews*, 2012, 14, 159-179.

[34] E. ELLCESSOR, *Restricted Access: Media, Disability and the Politics of Participation*, New York and London, 2016.

indipendente alle persone con disabilità[35], in quanto parte di una complessa rete di interdipendenze che comprende istituzioni pubbliche, produttori e aziende tecnologiche, servizi di dati e manutenzione, nonché quadro normativo[36].

Nel presente contributo abbiamo cercato di mostrare cosa succede quando i nodi di questa rete non comunicano tra loro, con il rischio di capovolgere le idee di potenziamento e di *empowerment* solitamente associate alla tecnologia avanzata e all'IA.

A tal fine, in questa sezione si intende richiamare il concetto di "tecnologie dell'umiltà" di Sheila Jasanoff[37], sostenendo la necessità di una conversazione più significativa tra il pubblico, le organizzazioni che sviluppano e gestiscono la tecnologia e le norme giuridiche.

Ciò in quanto, in primo luogo, la tecnologia non è un semplice strumento, ma è essa stessa una forza sociale che incorpora significati sociali – provenienti da idee, narrazioni, immaginari – e contribuisce a produrli[38]. In secondo luogo, la tecnologia è immaginata, progettata, gestita e trasformata nel contesto sociale delle organizzazioni, mentre è essa stessa ad avere un potere organizzativo[39]. In terzo luogo, perché la tecnologia viene utilizzata in modi non lineari e che possono essere non previsti sia dai progettisti[40] sia dai legislatori.

Tutto ciò è di grande importanza per le organizzazioni e la società, e diventa particolarmente urgente quando si ha a che fare con la disabilità, poiché in questo caso la tecnologia può diventare una questione di vita o di morte - oltre al libero arbitrio e al testamento, si pensi ai casi in cui la tecnologia media l'accesso al primo soccorso[41].

La tecnologia basata sull'IA è troppo spesso circondata da una sorta di aura mistica e associata acriticamente alle idee di miglioramento e di potenziamento[42]. Tuttavia, gli approcci tecnofili sono spesso informati da una sorta di determinismo tecnologico che è tipico delle ideologie transumaniste, secondo cui la tecnologia può, da sola, risolvere i problemi sociali, guarire le persone, dare accesso e opportunità. Si intende usare l'espressione "tecnologie di potenziamento" per fare riferimento non a tecnologie specifiche, ma a questo modo di intendere la tecnologia e il suo ruolo nella società. È stato notato come tale approccio sia ingenuo, in quanto trascura i più ampi fattori storici e sociali di emarginazione che colpiscono le minoranze, in particolare le persone con disabilità[43]. Inoltre, tale approccio soffre di una "ideologia

[35] T. Siebers, *Disability Theory*, Michigan, 2008; M. Alper, *Giving Voice: Mobile Communication, Disability, and Inequality*. Cambridge, MA, 2017.
[36] D. Napolitano, V. Lasala, S. Ripetta, *Limits of inclusion: multimodal action-nets and the challenge of communication technologies for disability*, in *Impresa Progetto* (in corso di pubblicazione).
[37] S. Jasanoff, *Technologies of Humility: Citizen Participation in Governing Science*, Minerva, 2003, 41, 223-244.
[38] W. Bijker, J. Law, *Shaping Technology, Building Society*, Cambridge (MA), 1997; S. Jasanoff, S.H. Kim, *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power*, Chicago and London, 2015.
[39] T. Beyes, R. Holt, C. Pias, *By means of which: Media, technology, organization*, in T. Beyes, R. Holt, C. Pias (eds.), *The Oxford Handbook of Media, Technology and Organization Studies*, Oxford, 2019, 498-513.
[40] A. Hamraie, K. Fritsch, *Crip Technoscience Manifesto*, in *Catalyst: Feminism, Theory, Technoscience*, 2019, 5, 1-34.
[41] E. Ellcessor, *In Case of Emergency: How Technologies Mediate Crisis and Normalize Inequality*, New York and London, 2022.
[42] D. Napolitano, *La voce artificiale. Un'indagine media-archeologica sul computer parlante*, Napoli, 2022.
[43] M. Alper, *Giving voice: Mobile Communication, Disability, and Inequality*, Cambridge, MA, 2017.

dell'abilità"[44], in quanto ritrae la tecnologia come qualcosa che permette agli individui di "superare" la loro disabilità - considerata come una limitazione individuale - e allo stesso tempo assume l'abilità come una condizione indiscussa e neutrale, poi corrotta dalla disabilità.

Oltre alle critiche a questa visione provenienti dal mondo degli studi sulla disabilità, si intende focalizzare l'attenzione sul mix di problemi organizzativi e giuridici legati alle tecnologie assistive. Il caso sopra analizzato del diritto successorio, infatti, mette in evidenza che un limite principale delle "tecnologie di potenziamento" non risiede nelle funzioni, ma nel contesto organizzativo in cui gli strumenti tecnologici sono inseriti. In particolare, evidenzia una mancanza di partecipazione alla progettazione e all'implementazione delle tecnologie sia da parte del legislatore che delle stesse persone con disabilità.

L'idea della Jasanoff di "tecnologie dell'umiltà" può essere vista come un quadro di riferimento per contrastare la condizione prodotta dalle tecnologie di potenziamento e, auspicabilmente, superarne i limiti. A suo avviso, le tecnologie dell'umiltà "*richiedono non solo i meccanismi formali della partecipazione, ma anche un ambiente intellettuale in cui i cittadini siano incoraggiati a mettere in gioco le loro conoscenze e competenze per la risoluzione dei problemi comuni*" [45] . L'autrice sottolinea come nelle moderne società industriali gli studi volti a stabilire la sicurezza o l'efficacia delle nuove tecnologie siano spesso delegati ai produttori. I processi di controllo della qualità per i test sui prodotti all'interno dell'industria includono l'imposizione e l'applicazione di buone pratiche di laboratorio, sotto la supervisione delle agenzie di regolamentazione e dei loro consulenti scientifici. Questo produce un'autoreferenzialità nel processo di creazione della conoscenza, da cui sono esclusi tutti gli altri attori sociali. Ma il crescente impegno a coinvolgere il pubblico nelle decisioni di carattere tecnico potrebbe non essere sufficiente, poiché le persone potrebbero non possedere conoscenze specialistiche e risorse materiali sufficienti per entrare nelle procedure formali e la partecipazione potrebbe avvenire troppo tardi per identificare alternative alle opzioni dominanti o predefinite. Per democratizzare la tecnologia, quindi, "*ciò che deve cambiare è la cultura della governance, sia all'interno delle nazioni che a livello internazionale; e per questo dobbiamo affrontare non solo la meccanica, ma anche la sostanza della politica partecipativa*"[46]. La questione, in altre parole, non è più se il pubblico debba avere voce in capitolo nelle decisioni tecniche, ma come promuovere un'interazione più significativa tra i responsabili politici, gli esperti scientifici, i produttori aziendali e il pubblico.

ll modo in cui Jasanoff suggerisce di raggiungere questo risultato si basa su una struttura composta da inquadramento, vulnerabilità, distribuzione e apprendimento. Una partecipazione attenta a questi quattro punti promette di non portare né a un indurimento delle posizioni, né a una decostruzione senza fine, ma piuttosto a una più ricca deliberazione sulla sostanza del processo decisionale. In particolare, la vulnerabilità sembra un punto cruciale quando si discute di tecnologie assistive. La partecipazione dei cittadini alle tecnologie democratiche, infatti, deve includere anche le persone con disabilità e tenere

[44] T. SIEBERS, *op. cit,* 8.
[45] S. JASANOFF, *op. cit.,* 227.
[46] S. JASANOFF, *op. cit.,* 238

conto della loro vulnerabilità senza nasconderla, anzi riconoscendo l'esposizione al rischio di subire pregiudizi, stigma e mancato riconoscimento.

Il tipo di partecipazione alla progettazione delle tecnologie assistive, quindi, può fungere da modello per il processo decisionale nel più ampio contesto tecnologico delle organizzazioni contemporanee. Si tratta di una partecipazione che coinvolge punti di vista plurali in cui il soggetto umano è visto come un agente attivo, immaginativo e vulnerabile, prodotto di una storia personale e collettiva che può essere fatta di potere o di ingiustizia e come tale è fonte di conoscenza, intuizione e memoria. Se questo tipo di partecipazione viene esteso anche alla formulazione delle leggi, può diventare la base per un progetto di inclusione effettiva, in grado di superare le visioni ingenuamente ottimistiche che troppo spesso si accompagnano alla retorica inclusiva[47].

6.2 Prospettiva giuridica.

Tutto quanto precede intende mettere in evidenza che le persone con disabilità, nel particolare ambito del diritto successorio, corrono il rischio di trovarsi in una condizione di vulnerabilità, intesa come possibile esposizione al rischio di subire un pregiudizio.

Ciò su cui si vuole richiamare l'attenzione, infatti, è che la vulnerabilità può essere determinata da molteplici fattori esterni o "di contesto", che ne individuano una dimensione "relazionale"[48].

Ciò implica che per le persone con disabilità la vulnerabilità non dipende da una condizione patologica ma da limitazioni determinate da una società non inclusiva, che pregiudica la piena espressione della personalità dell'individuo.

Recuperare il carattere relazionale della vulnerabilità, e quindi della persona, consente di non relegare la disabilità ad una dimensione individualistica e di comprendere che la stessa non rappresenta un assoluto della persona ma riguarda il rapporto tra la persona e il suo ambiente di riferimento.

Ciò induce a riflettere sull'opportunità che si costruisca una tutela effettiva basata sulla cooperazione tra persone con disabilità, giuristi ed aziende tecnologiche, affinché siano prodotti dispositivi che rispondano alle reali ed effettive esigenze delle persone.

A tal fine si potrebbe pensare ad un diritto successorio che consenta al notaio di porsi come figura garante del corretto utilizzo degli strumenti e servizi tecnologici prodotti da aziende in stretta collaborazione con le persone con disabilità al fine di consentire loro di regolamentare validamente la propria successione.

Si potrebbero immaginare al riguardo due distinti scenari idonei ad ispirare il legislatore con un intervento riformatore sul punto.

Prima proposta: creazione di una piattaforma digitale interamente gestita dal notariato cui poter facilmente dare accesso alle persone con disabilità, sia da

[47] L. DOBUSCH, H. LOTTE, S.L. MUHRE, *The im-/possibility of hybrid inclusion: Disrupting the 'happy inclusion' story with the case of the Greenlandic Police Force*, in *Organization*, 2021, 28, 311-333.

[48] I.A. CAGGIANO, *Minori d'età e GDPR*, in E. DE BELVIS (a cura di) *Family law and* Technology, Napoli, 2022, 189-214; L. GATT, *The vulnerability of the human being in a technological environment: the need for protective regulation*, in L. GATT (a cura di) *Social networks and multimedia habitats*, Napoli, 2020, 1-53; A. FUSARO, *L'atto patrimoniale della persona vulnerabile*, Napoli, 2019.

un punto di vista economico, prevedendo costi contenuti e sostenibili da tutti, ma anche da un punto di vista tecnico, attraverso la creazione di appositi tool che consentano ogni forma di comunicazione possibile.

In tal modo si potrebbero avere

- testamenti digitali redatti dalla persona con disabilità con il supporto del notaio
    - in forma scritta (con ogni mezzo possibile, incluso il codice Braille), superando con la tecnologia anche la necessaria sottoscrizione autografa dell'atto;
    - in forma orale dando modo alla persona con disabilità di poter realizzare un video in cui viene ripreso mentre esprime le sue ultime volontà.

In entrambi i casi, il testamento verrebbe redatto in piena autonomia dalla persona con disabilità ma alla presenza fisica o da remoto del notaio e di due testimoni (la cui storica *ratio* si ritrova nel garantire la spontaneità della manifestazione del testatore e la fedele riduzione in iscritto della stessa da parte del notaio) [49].

Pertanto, il notaio dovrebbe limitarsi ad assistere all'espressione della volontà da parte del disponente, dopo averlo adeguatamente informato e reso consapevole delle conseguenze connesse al suo testamento.



Fig. n. 3 *Eye-tracking* per la lettura del movimento oculare

- testamenti scritti redatti dal notaio, su espressa richiesta del testatore e non come scelta obbligata per mancanza di alternative ammissibili.
  In questo caso, il problema della sottoscrizione della scheda testamentaria da parte del testatore che ha perso l'uso degli arti superiori potrebbe essere diversamente risolto a seconda della forma da lui scelta:
    - testamento digitale: potrebbero prevedersi a tale scopo sistemi informatici che consentano al disponente di poter apporre la sua firma digitale, ad esempio tramite lettura dei dati biometrici come il movimento oculare[50] (fig. n. 3);
    - testamento cartaceo: avendo cura di eliminare dall'atto tutte quelle dichiarazioni che possano ledere la dignità del testatore perché discriminatorie.

[49] G. SANTARCANGELO, *La forma degli atti notarili*, Milano, 2006, 343.

[50] Il tutto conformemente alla normativa in tema di trattamento dei dati personali (Reg UE 679/2016 GDPR), di cui il testatore deve essere informato e prestare il relativo consenso firmando un apposito modulo. Con l'entrata in vigore del GDPR, infatti, anche i notai sono titolari del trattamento dei dati personali contenuti nei propri atti e sono tenuti a far sottoscrivere ai propri clienti l'informativa *privacy* che, nel caso di specie, verrebbe ad ampliarsi nel contenuto per ricomprendere anche i dati sopra menzionati. In dottrina sull'importanza dell'utilizzo di strumenti tecnologici anche per l'analisi giuridica del dato normativo, con *focus* specifico sul trattamento dei dati personali L. GATT, R. MONTANARI, I.A. CAGGIANO, *Privacy and consent. A legal and UX&HMI approach for data protection*, Napoli, 2021, 5-182.

Seconda proposta: riconoscere, in ogni caso, alle persone con disabilità il diritto di poter utilizzare, in alternativa rispetto alla piattaforma sopra descritta, «ogni altro mezzo, modalità e sistema accessibile di comunicazione di loro scelta», così rendendo effettivo il principio di uguaglianza e piena autonomia delle persone con disabilità espresso nella Convenzione delle Nazioni Unite (art. 21).

Aprire il diritto successorio alle innovazioni che la tecnologia mette a disposizione appare sicuramente un processo complesso e che investe profili molteplici e più ampi di quelli oggetto del presente contributo.

Ma volendo provare a fare il punto delle questioni di cui si è trattato fino a questo momento, il dato fondamentale che sembra emergere a supporto di quanto messo in evidenza è il seguente: tutelare i diritti delle persone con disabilità anche in ambito successorio non implica soltanto consentire un processo di ampliamento delle tutele immaginabili - aumentando il livello di fiducia delle persone verso lo strumento tecnologico e la figura professionale del notaio - ma implica anche modificare la percezione sociale della disabilità.

Si realizzerebbe in tal modo l'obiettivo fondamentale di garantire la piena autonomia delle persone con disabilità, finalmente libere di potersi esprimere con qualsiasi mezzo e di integrarsi in tal modo, compiendo valide attività negoziali, in un tessuto sociale in cui si possa riscontrare l'effettività del principio di uguaglianza giuridicamente tutelato. Ciò a dimostrazione della stretta connessione tra profili giuridici ed organizzativi delle questioni poste dall'utilizzo delle tecnologie da parte delle persone con disabilità.

Del Forno A, 'L'intelligenza artificiale nei processi gestori dell'impresa' (2022) 2 EJPLT, 119-135.
DOI : https://www.doi.org/10.57230/EJPLT222ADF

EJPLT
ISSN 2704-8012



L'intelligenza artificiale nei processi gestori dell'impresa.

Artificial Intelligence in business processes management.

ANDREA DEL FORNO
Ph.D.(c) Università degli Studi di Siena e Foggia

Abstract

Il contributo intende fornire un'analisi dello stato dell'arte in materia di intelligenza artificiale nei processi gestori dell'impresa, con un focus specifico sulla rilevanza che gli algoritmi potrebbero ricoprire in relazione alla corporate governance. In particolare, partendo da una disamina generale sull'intelligenza artificiale, si mira ad analizzare quelli che – ad oggi – sono i limiti che non consentono ad un algoritmo di ricoprire in maniera diretta il ruolo di amministratore all'interno di un consiglio di amministrazione. Infatti, nonostante la letteratura scientifica stia investigando in favore di aperture sul tema, tale possibilità è frenata sia da limiti di natura tecnologica, concernenti le modalità di sviluppo degli stessi algoritmi, sia da limiti di tipo soggettivo, riguardanti l'impossibilità attuale di riconoscere quantomeno uno status giuridico agli stessi. Lungo tali riflessioni – senza alcuna pretesa di esaustività – si considera anche la soluzione dottrinale della nomina indiretta di un'I.A. all'interno del board, nonché eventuali sviluppi derivanti dall'inclusione generica dell'I.A. nei contesti gestori.

The contribution wants to provide an analysis of the state of the art in the field of artificial intelligence in the management processes of the companies, with a specific focus on the relevance that algorithms could cover in the corporate governance. Especially, starting from a general examination of artificial intelligence, the aim is to analyze what – currently – are the limits that do not allow an algorithm to directly cover the role of director within a board of directors. In fact, although the scientific literature is investigating in favor of openings on the topic, this possibility is held back both by technological limitations, concerning the methods of development of the algorithms, and by subjective limitations, regarding the current impossibility of recognizing a legal status for them. Along these reflections – without any claim to exhaustiveness – it is considered the doctrinal solution of the indirect nomination of an A.I. within the board, and also some developments deriving from the generic inclusion of the A.I. in management contexts.

© The author(s) 2022, 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: intelligenza artificiale; consiglio di amministrazione; I.A.; consigliere amministratore; robodirector; roboboard.

Summary: 1. Introduzione. – 2. L'intelligenza artificiale. – 3. Algoritmo amministratore. – 4. Limiti tecnologici. – 5. Limiti connessi alla soggettività giuridica. – 6. Conclusioni.

1. Introduzione.

Negli ultimi decenni, il progresso informatico e lo sviluppo tecnologico hanno permesso di concepire strumenti tali da affiancare e sostituire l'attività umana in un numero sempre maggiore di settori, così da rendere quasi profetiche le parole di Douglas Adams in *"Guida galattica per gli autostoppisti"*, secondo le quali, per l'enciclopedia galattica al centro del romanzo distopico, la definizione di robot è quella di *"un apparecchio meccanico destinato a svolgere il lavoro di un uomo"*[1].

A tale progresso, tuttavia, sono conseguite una serie di riflessioni volte a plasmare la tenuta delle regole e delle categorie - nonché interrogativi circa la necessità o meno di crearne di nuove - di fronte a questi cambiamenti dirompenti apportati dalla tecnologia al mondo circostante, genericamente inteso, quindi non solo agli individui ed agli enti, ma anche a qualsiasi altro tipo di organizzazione, così come all'ambiente, ai mercati e così via.

In questo contesto, le imprese giocano un ruolo fondamentale in quanto sono i principali centri entro i quali vengono create e sviluppate le novità tecnologiche e, contestualmente, tra i primi soggetti a sperimentarle nella loro stessa organizzazione, in maniera tale da valutarne l'impatto pratico e le eventuali modifiche da effettuare dal punto di vista della tecnica.

Proprio alla luce di tali ragioni, il ruolo sempre più preponderante di queste nuove tecnologie nel cuore delle imprese[2], il presente contributo prende in considerazione lo strumento specifico dell'intelligenza artificiale, la quale assurge una funzione chiave in relazione agli impatti derivanti dallo sviluppo tecnologico applicato all'interno delle realtà societarie e ciò si configura come

[1] Tale citazione è ripresa dalla versione di "Guida galattica per autostoppisti" edita dalla Mondadori S.p.A. nel 1980 e tradotta da Laura Serra.

[2] Tra queste, a mero titolo esemplificativo, tutte quelle che fanno riferimento alla categoria delle *distribuited ledger technologies*, ovvero le tecnologie che si fondano su un sistema c.d. di "registro condiviso" tra più soggetti, come la *blockchain* e gli *smart contracts*. Più specificamente, volendo provare a definirle in poche parole e senza alcuna pretesa di esaustività, con il termine "*blockchain*" si intende quel registro contabile distribuito su cui vengono registrate le transazioni o le informazioni, le quali vengono aggregate in catene di blocchi di cui ogni blocco ha la propria capienza massima di dati, raggiunta la quale viene chiuso in maniera tale da renderlo immodificabile crittograficamente. Tale immodificabilità viene realizzata attraverso la c.d. funzione di *hash*, ovvero una funzione non invertibile, che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Invece, gli *smart contracts* sono una forma specifica di applicazione della tecnologia *blockchain* in quanto consistono in particolari istruzioni in linguaggio informatico tali da essere eseguite e registrate così da tenerne traccia per tutti i soggetti partecipanti. Per ulteriore approfondimento, a titolo esemplificativo si veda anche M. MAUGERI, *Smart Contracts e disciplina dei contratti - Smart Contracts and Contract Law*, Bologna, 2021; R. BATTAGLINI – M. GIORDANO, *Blockchain e smart contract. Funzionamento, profili giuridici e internazionali, applicazioni pratiche*, Milano, 2019; E. BASSOLI (a cura di), *Diritto di internet. Vol. 3: Smart Contract, criptovalute e blockchain*, Pisa, 2021; A. STAZI, *Automazione contrattuale e «contratti intelligenti». Gli smart contracts nel diritto comparato*, Torino, 2019;

un riflesso di una disamina, più generica, relativa al rapporto tra diritto, tecnologia e dinamiche del mercato.

La questione assume un rilievo sempre più essenziale in relazione alla tipologia di impiego per la quale l'impresa ritiene di far interagire l'intelligenza artificiale all'interno della propria organizzazione e gestione; in altre parole, a seconda delle modalità di interazione di tale tecnologia con la realtà societaria, si configura un'interferenza differente, la quale si può realizzare nei tre seguenti modi:

i) ricorso all'intelligenza artificiale come strumento di supporto e di *output* dell'attività di impresa;
ii) ricorso all'intelligenza artificiale con una prospettiva esterna del funzionamento societario[3];
iii) ricorso all'intelligenza artificiale con una prospettiva interna, quindi utilizzo degli strumenti di I.A. per l'organizzazione ed il funzionamento societario interno[4].

Tuttavia, il tema analizzato nelle prossime pagine è circoscritto, più specificamente, allo stato dell'arte attuale circa le ricadute inerenti al terzo profilo, dunque l'impatto dell'intelligenza artificiale sulla *corporate governance* della società per azioni, con un focus sull'eventuale utilizzo di sistemi di intelligenza artificiale nella funzione gestoria dell'impresa. In altre parole, quindi, l'intento di tale studio è quello di riassumere e definire la possibilità o meno di immaginare gli algoritmi come membri di un organo amministrativo composto anche da persone fisiche, se non addirittura di eventuali prospettive futuristiche di sostituzione degli amministratori in favore del c.d. *roboboard*[5].

2. Le intelligenze artificiali.

Prima di procedere alla disamina di quanto sopra, è fondamentale muovere dalla delineazione del concetto di intelligenza artificiale, posto che è sempre difficile relazionare in argomenti nei quali si evocano, in un contesto tecnologico, qualità umane così delicate, come proprio il concetto stesso di "intelligenza"[6].

Infatti, con tale espressione si fa riferimento a quelle tecnologie in grado di porre in essere attività che, se realizzate da una persona fisica, richiederebbero il ricorso a funzioni cognitive; più genericamente, pertanto, si può affermare come tali forme di tecnologia riescano a simulare i processi di intelligenza umana[7].

---

[3] Ad esempio, nelle imprese del settore finanziario tale funzione si estrinseca nella valutazione da parte dei sistemi di intelligenza artificiale dei mercati finanziari.

[4] N. ABRIANI, *La corporate governance nell'era dell'algoritmo – Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla corporate governance*, in *Il Nuovo Diritto delle Società*, 2020, 3, p. 261 ss.

[5] G. D. MOSCO, *Roboboard. L'intelligenza artificiale nei consigli di amministrazione*, in *AGE*, 1/2019, *Algoritmi. Se li conosci, li regoli…*, a cura di A. Nuzzo e G. Olivieri, p. 247 ss.

[6] S.J. RUSSELL, P. NORVIG, *Artificial Intelligence: A Modern Approach*, Harlow, 2021, p. 19 ss.

[7] A.M. TURING *Computing Machinery and Intelligence*, in *59 Mind*, 1950, p. 433 ss, secondo cui entro qualche decennio le macchine sarebbero apparse intelligenti, introducendo per la prima volta tale concetto. Turing, infatti, ha influenzato enormemente proprio la definizione del concetto stesso di intelligenza artificiale, attraverso l'idea di intelligenza della macchina sulla base della visione da parte dell'osservatore esterno. Detto in altri termini, una macchina per Turing può essere reputata intelligente se un soggetto esaminatore

A livello legislativo, poi, un'enunciazione generale del concetto di "sistema di intelligenza artificiale" è abbastanza recente e si rintraccia nella Proposta di Regolamento Europeo sull'intelligenza artificial[8], per la quale si deve intendere come tale qualsiasi *"software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I[9], che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono"*[10].

Già da queste premesse, si evince come esistano molteplici tipologie di I.A.; tuttavia, occorre precisare che uno dei principali sistemi di differenziazione si basa sul grado di autonomia dell'apprendimento da parte dell'algoritmo alla base dell'intelligenza artificiale: conseguentemente, si parla, di intelligenza *supervised* quando la stessa, a prescindere dal grado di autonomia, vede il governo del relativo procedimento coordinato dal programmatore; viceversa, quando questo manca ed è del tutto rimesso alla stessa I.A., si parla di intelligenza *unsupervised*.

Quest'ultima tipologia di tecnologia è definita "non supervisionata", poiché caratterizzata da un'autonomia totale: in questo caso, dunque, all'algoritmo vengono attribuiti sia un compito da realizzare sia un insieme di dati ed esso, attraverso un procedimento per tentativi ed in assenza totale di direzione da parte di qualsiasi figura di programmatore, identifica le regole da applicare oppure gli elementi comuni nell'insieme dei dati[11].

Ancora, poi, si deve precisare che ogni sistema di intelligenza artificiale necessita dell'uso di un algoritmo - dunque di un elemento che consta di istruzioni informatiche dettate per la realizzazione di uno specifico obiettivo[12] - a prescindere dal suo essere *supervised* o meno, poiché è proprio mediante gli algoritmi che si possono non solo estrarre informazioni o dati a supporto di determinate operazioni, ma anche procedere ad un'esecuzione automatizzata di procedimenti o decisioni mediante l'analisi degli stessi dati. In altre parole, quindi, gli algoritmi possono essere utilizzati sia come strumenti idonei a consentire di addivenire ad una determinata decisione, sia come elementi da

esterno, ponendo le stesse domande ad una macchina ed a una persona fisica, senza la consapevolezza di sapere quale delle due stia interrogando, non riesca a distinguere le risposte date dall'una o dall'altra categoria. Tale esame è il c.d. *imitation game*, o *Turing Test*.

[8] La prima versione dell'*Artificial Intelligence Act ("Proposta di Regolamento n. 2021/206 del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale – legge sull'intelligenza artificiale - e modifica alcuni atti legislativi dell'Unione"*), anche c.d. AIA, è stata presentata dalla Commissione Europea nell'aprile del 2021.

[9] Di seguito, il contenuto dell'ALLEGATO I di cui agli *Allegati della proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni legislativi dell'Unione*: *"TECNICHE E APPROCCI DI INTELLIGENZA ARTIFICIALE di cui all'articolo 3, punto 1)*

a) Approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (deep learning);

b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti;

c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione."

[10] Cfr. art. 3, par 1(1), *Artificial Intelligence Act Proposal* n. 216/2021.

[11] J. ARMOUR – H. EIDENMÜLLER, *Self - Driving Corporations?*, in 10 *Harvard Business Law Review*, 2020, p. 95 ss.

[12] Cfr. G. SARTOR – F. LAGIOIA, *Le decisioni algoritmiche tra etica e diritto*, in *Intelligenza Artificiale. Il diritto, i diritti, l'etica*, a cura di U. RUFFOLO, Milano, 2020, p. 64 ss, nel quale si rintraccia la definizione del concetto di algoritmo e la sua distinzione con l'intelligenza artificiale, genericamente intesa.

porre a fondamento di strutture o sistemi complessi così da agevolare l'interazione[13].

Relativamente alle modalità di apprendimento della macchina stessa - e dunque di formazione della sua intelligenza – si può porre in essere un'altra distinzione di I.A.: infatti, se il processo di apprendimento dell'algoritmo avviene in via automatica, si parla di metodo di apprendimento c.d. di *machine learning*; invece, se questo avviene in modo profondo, si parla di apprendimento dell'algoritmo mediante il c.d. *deep learning*[14].

A ben vedere, si parla di *machine learning* quando una macchina, servendosi dell'algoritmo di cui è stata dotata, impara attraverso l'analisi dei dati forniti durante la programmazione ed utilizza quanto apprende da questa stessa analisi per prendere decisioni che possono essere definite informate.

Di tale tipologia di I.A. esistono molteplici esempi, che si concretizzano come elementi pratici ai quali ci relazioniamo tutti noi quasi quotidianamente: tra questi, un esempio tra tanti può essere l'applicazione automatica di filtri *antispam* nelle caselle di posta.

Invece, in relazione al *deep learning*, invece, questo non è altro che una modalità potenziata di quello automatico nel quale la macchina, tuttavia, ricorre ad una rete neuronale – definita così proprio perché ha preso spunto da quella del cervello umano, dunque dall'interconnessione dei vari neuroni - tale da consentirgli di realizzare decisioni in via autonoma. Questa tipologia di algoritmi rintraccia un'ampissima applicazione nel contesto delle piattaforme *social*, oltre che in una moltitudine di altri servizi *online*, tra i quali si rinviene quelli concernenti la traduzione automatica di un testo da una lingua ad un'altra o il riconoscimento vocale.

Questi sistemi di I.A., pertanto, pur funzionando in maniera similare, si differenziano per il fatto che il *deep learning* riesce a verificare esso stesso, contrariamente al *machine learning*, se, sulla base di determinati dati, il risultato derivante risulta coerente con gli stessi, senza la necessità di un supporto umano.

Tuttavia, per raggiungere tale risultato, e conseguentemente essere autonomo, il modello di *deep learning* necessità di moltissimi dati, così da potersi allenare a consegnare le giuste risposte, e dunque a sbagliare fino a rilevare l'errore e correggerlo autonomamente nella propria sequenza[15].

Non potendo soffermarci ulteriormente in questa sede circa le ulteriori differenze tecniche ed il relativo sviluppo storico dell'I.A. e degli algoritmi[16], si riporta l'attenzione sul *machine learning* per delle considerazioni preliminari al tema in oggetto: infatti, proprio tale tipologia di apprendimento riveste nel

---

[13] A. NUZZO, *Algoritmi e regole*, in *AGE*, 2019, p. 40.

[14] In materia di *deep learning* e *machine learning*, a titolo esemplificativo si veda E. BASSOLI, *Algoritmica giuridica. Intelligenza artificiale e diritto*, Ancona, 2022; G. M. RICCIO – G. ZICCARDI – G. SCORZA (a cura di), *Intelligenza artificiale. Profili giuridici*, Padova, 2022; S. FARO – T. E. FROSINI – G. PERUGINELLI, *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020; U. RUFFOLO (a cura di), *XXVI lezioni di Diritto dell'Intelligenza Artificiale. Saggi a margine del ciclo seminariale "Intelligenza Artificiale e diritto*, Torino, 2020.

[15] M.G. PELUSO, *Intelligenza Artificiale e dati di qualità: la tecnologia come valido alleato*, in *Media Law - Rivista di Diritto dei Media*, 2/2022

[16] V. anche N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, Bologna, 2021, p. 20 ss; J. ARMOUR – H. EIDENMÜLLER, *op. cit.*, p. 87 ss; N. NILSSON, *The quest for artificial intelligence. A history of ideas and achievements*, Cambridge, 2009, p. 147 ss, nel quale è possibile rintracciare una ricostruzione storica completa in materia di intelligenza artificiale fino al XXI secolo.

mondo dell'I.A. un ruolo chiave già da diversi anni, poiché ha consentito di superare molte delle criticità tecnologiche precedenti permettendo, al tempo stesso, di sfruttare le potenzialità derivanti dalle funzionalità della moderna società dell'informazione.

Così, il *machine learning* ha consentito per primo un grande slancio nello sviluppo tecnologico: attraverso il suo metodo, la macchina apprende lavorando, correggendo gli errori e, conseguentemente, migliora continuamente le proprie prestazioni nel tempo proprio sulla base di tali passaggi. In altre parole, un programma con modalità *machine learning* impara inferendo regole a partire dagli *input* ricevuti, i quali a loro volta derivano dai dati osservati.

La capacità decisionale di tale strumento, pertanto, si ottimizza – proprio come negli esseri umani – attraverso l'esperienza: *nel machine learning*, come nei bambini appena nati, inizialmente le macchine sono scatole vuote con nulla al proprio interno se non le stesse regole per le quali impareranno ad apprendere a partire dai dati che gli verranno forniti.

Riconducendo lo studio alla tematica di cui in oggetto, posti tali cenni sugli algoritmi e sulle loro modalità di funzionamento, è possibile immaginare un consiglio d'amministrazione nel quale sieda, nelle vesti di amministratore, un algoritmo che si muove – per essa stessa configurazione – in questo modo?

Si può, riprendendo la celebre espressione concepita dal filosofo Kuhn [17] nella trattazione delle rivoluzioni scientifiche, introdurre un "cambio di paradigma" come questo all'interno del diritto societario e, più in generale, nei processi gestori dell'impresa, oppure il nostro sistema – ma non solo – non è ancora pronto a recepire tali novità?

3. Algoritmo amministratore.

Le diverse declinazioni dei doveri degli amministratori [18] sono state suddivise, alla luce della riforma del diritto societario del 2003 [19], in poteri -

[17] T.S. KUHN, *The Structure of Scientific Revolutions*, Chicago, 1962, nel quale il filosofo afferma la celeberrima "teoria del paradigma" in ambito scientifico, per la quale la scienza attraversa ciclicamente cinque fasi indicative della sua operatività, che ruotano tutte attorno ad un paradigma. Per Kuhn, la scienza cambia una volta giunti alla quinta fase del paradigma corrente, poiché successivamente il ciclo ricomincio dalla fase uno di un nuovo paradigma. Tale espressione sembra calzante rispetto al necessario cambio di paradigma, riguardante l'I.A., in seno al diritto societario.

[18] Si precisa che si prende a riferimento, nel trattare del ruolo e dei poteri degli amministratori e del consiglio di amministrazione, il modello della Società per Azioni, come già anticipato nel paragrafo precedente.

[19] Infatti, a partire da tale riforma, l'ordinamento italiano riconosce alle società la facoltà di scelta tra tre differenti modelli di *governance*, ciascuno dei quali idoneo a rispondere – in maniera differente – alle nuove esigenze e dinamiche del mercato: modello tradizionale, modello monistico e modello dualistico.
Il modello tradizionale, tipico della tradizione italiana ed anche detto "ordinario", prevede la presenza di un organo di controllo e di un organo di amministrativo. Quest'ultimo, che può essere costituito da un amministratore unico o da un consiglio di amministrazione, vede calato su di sé la funzione amministrativa – gestoria, per la quale si occupa di amministrare la società in maniera conforme all'oggetto sociale. L'organo di controllo, nelle vesti del collegio sindacale se previsto dallo Statuto, si occupa invece di svolgere attività di controllo sull'operato dell'organo amministrativo: più nello specifico, pone in essere il controllo sulla gestione ed il controllo contabile. Se, invece, lo statuto non attribuisce espressamente il controllo contabile al collegio sindacale o non concorrono le altre condizioni indicate, il controllo contabile è affidato ad un organo esterno (revisore o società di revisione), mentre al collegio sindacale è rimessa l'esclusivo controllo di legalità.

doveri di gestione in senso stretto (anche detti di *management*) e poteri - doveri di informazione e controllo (definiti pure di *monitoring*)[20].

Conseguentemente, si può evincere, come sostenuto da autorevole dottrina[21], che la gestione dell'impresa non deve essere intesa come un governo specifico e proteiforme degli affari societari e delle concernenti operazioni, ma, invece, come una coordinazione che afferisce all'organizzazione, alla supervisione ed all'indirizzo della realtà societaria, così che poteri e doveri si trovano ad essere in un delicato sistema di equilibri.

Tutto ciò premesso, potrebbe un algoritmo, assunte le vesti di consigliere di amministrazione, riuscire a coadiuvare gli altri membri ad esplicare i poteri gestori del consiglio stesso?

Uno studio effettuato nel 2017 da una grande società internazionale di consulenza strategica[22] ha affermato che circa un quarto delle attività realizzate dagli amministratori di società potrebbe essere alternativamente realizzato da idonei strumenti di intelligenza artificiale, quali gli algoritmi appunto. Tale dichiarazione, pure se apparentemente fantascientifica, in realtà si insinua nel solco di discussioni dottrinali di portata globale e di prime esperienze applicative.

In realtà, quando si parla di I.A. nei processi gestori dell'impresa si deve considerare che esistono tre livelli di coinvolgimento:

1) *"A.I. Assisted"*, cioè un'I.A. che supporta in maniera complementare l'attività amministrativa dei consiglieri di amministrazione;
2) *"A.I. Augmented"*, ovvero un'I.A. con un grado di coinvolgimento lievemente superiore, in quanto in tal caso la sua attività si interseca, comunque coadiuvando, i processi gestori degli amministratori;
3) *"A.I. Autonomous"*, quindi il livello ultimo dell'utilizzo delle tecnologie nel consiglio di amministrazione, per il quale la stessa I.A. è un autonomo amministratore.[23]

Il sistema monistico, invece, così come suggerito dallo stesso nome, prevede un unico organo amministrativo che si occupa sia dell'amministrazione che del controllo: in particolare, all'interno dello stesso consiglio di amministrazione viene costituito un comitato *ad hoc* per il controllo sulla gestione, formato da amministratori in possesso di determinati requisiti (onorabilità, professionalità e indipendenza). Relativamente al controllo contabile, questo deve essere affidato obbligatoriamente ad un revisore o una società di revisione esterna.

Il modello dualistico, tipico della tradizione tedesca e totalmente differente dagli altri due sistemi, prevede che l'assemblea dei soci elegga il consiglio di sorveglianza, dunque l'organo a cui spetta il controllo sulla gestione, al quale sono affidati alcuni dei compiti che nel modello ordinario sono prerogativa esclusiva dell'assemblea, come l'approvazione del bilancio d'esercizio. A sua volta, il consiglio di sorveglianza deve nominare il consiglio di gestione, dunque l'organo a cui spetta la gestione della società. Anche in tale modello il controllo contabile deve essere necessariamente esternalizzato ad un organo esterno, quale revisore o società di revisione.

Infine, occorre ricordare come, all'interno del nostro ordinamento, per l'adozione del modello monistico o dualistico è necessaria l'apposita indicazione statutaria.

[20] F. BONELLI, *Gli amministratori di s.p.a. a dieci anni dalla riforma del 2003*, Milano, 2013, 3 ss.

[21] V. anche, tra i tanti, P. FERRO – LUZZI, *L'esercizio d'impresa tra amministrazione e controllo*, in *AGE*, 2007, p. 231 ss.

[22] Tale società è McKensey e Company Inc. e, attraverso il proprio Osservatorio McKensey Global Institute, ha pubblicato questo studio a gennaio 2017, dal titolo *"A Future that Works: Automation, Employment and Productivity (Executive Summary)"*, reperibile all'indirizzo *https://www.mckinsey.com/~/media/mckinsey/featured%20insights/Digital%20Disruption/Harnessing%20automation%20for%20a%20future%20that%20works/MGI-A-future-that-works-Executive-summary.ashx*.

[23] A. RAO, *AI Everywhere/Nowhere part. 3 AI is AAAI (Assisted Augmented-Autonomous Intelligence)*, *http://usblogs.pwc.com/emerging-technology/ai-everywhere-nowhere-part-3-ai-is-aaai-assisted-augmented-autonomous-intelligence/*, 8 dicembre 2016; G. D. MOSCO, *op.cit,* p. 250 ss.

Ovviamente, il terzo e più alto livello di coinvolgimento, oltre ad essere quello di nostro interesse, risulta essere quello che ha – come predetto – maggiormente appassionato gran parte della dottrina.

Tuttavia, l'*A.I. Autonomous* si prospetta come una soluzione non (*rectius*: non ancora) attuabile per due limiti, di tipo e natura differente:

1) il primo è di tipo tecnologico e riguarda l'impossibilità odierna in capo agli algoritmi di replicare, nella sua totalità, la funzione gestoria *lato sensu*;
2) il secondo limite si ravvisa nella carenza di autonoma soggettività all'algoritmo.[24]

4. Limiti tecnologici.

Pur con l'avvento delle macchine connotate di intelligenza artificiale, ad oggi, nonostante i progressi raggiunti in campo scientifico e tecnologico, gli algoritmi non sono – almeno per adesso – in grado di replicare determinate caratteristiche intrinseche della natura umana e necessarie per talune delle funzioni alle quali un amministratore viene chiamato a dare il proprio contributo nel corso del mandato.

Esaminando tale limite più nel dettaglio, si deve precisare che la letteratura scientifica che ha analizzato la sostituibilità dei lavoratori e dell'apporto umano con quello tecnologico ha operato, tra le altre cose, una prima distinzione in seno ai compiti che un lavoratore può trovarsi a realizzare in "attività manuali" ed "attività cognitive", affermando allo stesso tempo, tuttavia, che rileverebbe un'altra distinzione, ovvero quella tra attività di *routine* ed attività non di *routine*[25].

Alla luce di tale distinzione, la connotazione routinaria di un compito deriverebbe dalla possibilità di descrivere una determinata attività attraverso regole esplicitabili. Pertanto, *a contrario*, le attività non routinarie sono quelle che non si prestano a tale tipologia di rappresentazione poiché i procedimenti sottesi alla loro realizzazione non si prestano ad essere circoscritti in un insieme di regole definito, esplicito ed idoneo ad essere eseguito da un computer; in altre parole, le attività non di *routine* richiedono capacità complesse.

Al riguardo, dunque, il contributo umano è – ad oggi – sostituibile con la tecnologia nelle sole attività di *routine*, a prescindere se di natura cognitiva o manuale: difatti, un sistema algoritmico, grazie allo sviluppo tecnologico, è in grado di rispondere con *performance* ottimali per compiti routinari anche di carattere cognitivo, come ad esempio l'effettuazione di una traduzione o di calcoli matematici.

Al contrario, per tutti quei compiti non routinari che necessitano di adattabilità rispetto alle circostanze concrete, per le quali l'apporto di natura umana deriva da elementi che difficilmente possono essere traslati in linguaggi

[24] C. Picciau, *Intelligenza artificiale, scelte gestorie e organizzazione delle società per azioni*, in *Il Nuovo Diritto delle Società,* 7/2022, p. 1253 ss.

[25] Si veda D.H. Autor, *Polany's Paradox and the Shape of Employment Growth, in Federal Reserve Bank of Kansas City: Economic Policy Symposium Proceedings. Reevaluating Labor Market Dynamics*, 2014, p. 129, ss.; D.H. Autor – F. Levy – R.J. Murnane, *The Skill Content of Recent Technological Change: An Empirical Exploration*, in *118 Q.J. Econ.*, 2003, p. 1279 ss;

di programmazione per l'algoritmo, le attuali tecnologie non si prestano alla concernente sostituzione.[26]

Considerando quanto finora riportato e riconducendolo ai fini della trattazione *de qua*, si palesa come l'attività di un consiglio di amministrazione non possa essere ricondotta nell'alveo delle attività di *routine* e, pertanto, la sostituibilità di un consigliere con un algoritmo è escludibile poiché ad oggi, proprio in ragione dei limiti di cui sopra, tale tecnologia non può elaborare o rimpiazzare né i singoli consiglieri, né tantomeno l'intero *board*.

Infatti, il *"managerial decision-making"* [27] non può, per sua stessa configurazione, rientrare nella categoria dei compiti routinari, proprio perché non traducibile in una connotazione di regole programmabili in un computer: l'attività degli amministratori necessita di flessibilità, prontezza e capacità di adattamento ai cambiamenti ed alle circostanze derivanti dal contesto di riferimento, oltre che di doti comunicative e relazionali, le quali non appaiono - ad oggi – replicabili nelle tecnologie algoritmiche.

Allo stesso tempo, però, nulla osta nel sostenere che l'intelligenza artificiale, così come ad oggi sviluppata, ben si confà ad un ruolo con funzione di supporto complementare – dunque non sostituivo – all'attività umana realizzata in un consiglio di amministrazione.

Ne consegue che, per gli attuali limiti operativi connessi alla struttura tecnica dell'I.A., questa si presta a ricoprire il ruolo intermedio di c.d. *A.I. Assisted*[28], dunque della tecnologia intesa a coadiuvare, senza interferire, gli amministratori nel processo gestorio.

Allo stesso tempo, tuttavia, il ricorso a questi strumenti tecnologici, pur con tale livello di coinvolgimento, comunque influenza, o perlomeno dovrebbe suggestionare, la composizione del consiglio di amministrazione: più specificamente, utilizzare l'I.A., pur se con un ruolo di supporto, si riverbera sull'*expertise* richiesta ai componenti stessi del *board*, per i quali deve – o comunque dovrà – essere tenuta maggiormente in considerazione il livello di conoscenze informatiche e di *data science*, ovvero competenze idonee alla supervisione dell'I.A. utilizzata.[29]

Nondimeno, la presenza di esperti di tecnologia, o addirittura la configurazione di uno o più comitati di esperti all'interno del consiglio di amministrazione, potrebbe divenire - nei prossimi anni - uno standard indefettibile – se non sintomatico – di *good governance*.[30]

Ribadendo quanto finora sostenuto, dunque, la nomina di un algoritmo, o comunque di un altro sistema di I.A., all'interno di un consiglio di amministrazione nelle vesti di autonomo consigliere non è ad oggi - ancora – possibile. Nonostante questo, però, pochi anni fa si era diffusa a livello

---

[26] D.H. AUTOR, *op. cit.*, p. 158 ss.
[27] V. anche, tra i tanti, J. SHANTEAU, *Encyclopedia of Psychology and Behavioral Science*, Kansas, 2002, p. 913 ss.
[28] A. RAO, *op. cit.*
[29] P. MÖSLEIN, *Robots in the Boardroom: Artificial Intelligence and Law*, in W. BARFIELD – U. PAGALLO (ed.), *Research Handbook on the Law of Artificial Intelligence*, 2017, p. 649 ss.
[30] N. ABRIANI, *op. cit.*, 273, che a sua volta cita R. FERACONE, *Good Governance, Do Boards Need Cyber Security Experts?*, in *Forbes*, 9 luglio 2019, *https://www.forbes.com/sites/robinferracone/2019/ 07/09/good-governance-do-boards-need-cyber-security-experts/#692766f61859.*

mondiale[31] la notizia che una *venture capital* di Hong Kong[32] aveva nominato come consigliere un algoritmo ribattezzato VITAL (*Validating Investment Tool for Advancing Life Sciences*).

Tale algoritmo, in realtà, non era un vero e proprio membro del *board*: esso, al contrario, aveva un esclusivo *status* di osservatore e, come tale, supportava gli amministratori nel valutare le opportunità di investimento attraverso l'analisi di un'enorme mole di dati, così da suggerire informazioni o raccomandazioni circa le decisioni da prendere in materia di investimento, le quali dovevano essere appunto corroborate da VITAL[33].

Detto in altri termini, quindi, VITAL non ricopriva in alcun modo il ruolo di consigliere, per cui non può essere portato come esempio di *A.I. Autonomous*: la sua funzione era, infatti, quella di supportare, attraverso analisi di livello informativo, i processi gestori dei consiglieri, i quali dovevano prendere decisioni avvalorate dai risultati elaborati da VITAL. La sua connotazione rispetto al grado di coinvolgimento è quella intermedia di *A.I. Augmented*, ebbene la sua attività si interseca con il processo gestorio dei membri del board, coadiuvando la loro funzione senza intervenire in via autonoma[34].

In conclusione, ad oggi, visti i limiti tecnologici derivanti dal programmare all'interno dell'algoritmo delle regole idonee a rendere la macchina dotata di tutti quegli aspetti concernenti la capacità di *managerial decision-making*, non essendo questa attitudine un'attività di *routine*, il ruolo al quale può aspirare un algoritmo – o una qualsiasi altra tecnologia – è quello di *A.I. Assisted* o di *A.I. Augmented*.

5. Limiti connessi alla soggettività giuridica.

L'altro limite che non consente di poter legittimare – per adesso - la configurazione di algoritmi come membri di un *board* societario è legato all'ambito soggettivo delle stesse tecnologie: infatti, come si potrebbe nominare amministratore uno strumento tecnologico non dotato di qualsivoglia soggettività giuridica?

Questo limite è particolarmente frenante rispetto ad un eventuale utilizzo in tal senso delle nuove tecnologie, sotto una moltitudine di aspetti e di profili connessi al ruolo di consigliere, basti solo pensare e prendere in considerazione quelli concernenti la rappresentanza e la delega.[35]

---

[31] Tale notizia, proprio in ragione dell'errato messaggio della nomina dell'algoritmo a membro del board, catalizzò l'attenzione mediatica internazionale. Si veda, tra i tanti, R. WILE, *A Venture Capital Firm Just Named An Algorithm To Its Board of Directors – Here's What It Actually Does*, in *Business Insider Australia*, 14 maggio 2014, *https://www.businessinsider.com.au/vital-named-to-board-2014-5*. In realtà, alla fine questa eco mediatica si è sostanzialmente risolta in una forte trovata pubblicitaria.

[32] La società è il fondo *Deep Knowledge Analytics*.

[33] V. M. PETRIN, *Corporate Management in the Age of AI*, in *Columbia Business Law Review*, 2019, p. 967 ss.; N. BURRIDGE, *Artificial Intelligence gets a seat in the boardroom*, in Nikkei Asia, *https://asia.nikkei.com/Business/Artificial-intelligence-gets-a-seat-in-the-boardroom*, 2017.

[34] M.L. MONTAGNANI, *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell'intelligenza artificiale*, in *Persona e Mercato*, 2020, p. 88 ss.

[35] L. ENRIQUES, D. ZETZSCHE, *Corporate Technologies and the Tech Nirvana Fallacy*, in ECGI *Working Paper Series in Law N° 457/2019*, p. 71 ss.

In particolare, volendo focalizzare l'attenzione sull'istituto della delega, questa non viene impattata tanto nell'ambito delle c.d. deleghe discendenti o funzionali, quanto in quello delle c.d. ascendenti - o comunque, deleghe in senso tecnico - per le quali il codice civile all'art. 2381 prevede l'esclusiva attribuzione ai soli soggetti qualificati come amministratori.

Infatti, rispetto al primo versante non si ravvisano particolari ostacoli in relazione al fatto che l'organo amministrativo possa realizzare un'attribuzione selettiva di funzioni in senso "discendente" direttamente allo strumento di intelligenza artificiale, così da assolvere una funzione di carattere pratico, non connessa al consiglio di amministrazione ma delegata dallo stesso.

Invece, relativamente alla delega c.d. "ascendente", è dubbia la configurabilità di una sua attribuzione da parte del board ad una "robot", poiché – alla luce dell'art. 2381 comma 2 cod. civ. – a sua volta presupporrebbe che il "soggetto" investito di funzioni delegabili – dunque lo stesso "robot" – sia esso stesso amministratore[36]; pertanto, l'assenza di soggettività giuridica si presenta come un limite in tal senso.

Ad oggi, il riconoscimento di uno *status* giuridico all'intelligenza artificiale è una questione aperta e che si presta ad essere affrontata sotto plurimi punti di vista: etico-filosofici, giuridici, economici e sociali.

Attenzionando l'aspetto giuridico, tale disamina si deve aprire[37] citando il paragrafo 59 lettera F) della Risoluzione del Parlamento Europeo 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, il quale invitava a prevedere *"l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi"*[38].

Da tale affermazione si evince come le istituzioni europee abbiano percepito la necessità di incanalare l'evoluzione tecnologica in modelli di imputabilità autonoma riconducibili alle macchine, le quali, essendo sempre più intelligenti ed indipendenti, difficilmente vedrebbero altrimenti riconducibili eventuali conseguenze derivanti dalla loro operatività a soggetti umani dal punto di vista della responsabilità giuridica.

Inoltre, questa specifica affermazione del Parlamento Europeo ha dato nuovo vigore ad una questione che aveva già allettato l'attenzione e l'interesse scientifico: infatti, la dottrina[39], attraverso i dogmi tradizionali di soggettività, capacità e personalità giuridica, aveva provato ad elaborare, in relazione alla creazione di un modello di imputabilità dei robot, molteplici soluzioni.

---

[36] N. ABRIANI, *op. cit.*, p. 270 ss.

[37] In realtà, il dibattito nella letteratura scientifica in materia di soggettività dei robot risale almeno al 1992 ed al saggio di L.B. SOLUM *"Legal Personhood for Artificial Intelligences"*, pubblicato per la prima volta in *North Carolina Law Review*, 70, 1992, n. 4.

[38] Tale proposta, ovvero la n. 2015/2103/(INL), è rimasta lettera morta, dal momento che lo stesso Parlamento Europeo in un secondo momento ha ritrattato tale ipotesi.

[39] V., tra i tanti, P. MORO, *Macchine come noi. Natura e limiti della soggettività robotica*, in U. RUFFOLO, (a cura di), *L'Intelligenza Artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020; G. TEUBNER, *Ibridi ed attanti. Attori collettivi ed enti non umani nella società e nel diritto,* 2015.

Partendo dal presupposto che soggettività giuridica e personalità giuridica non sono obbligatoriamente compresenti quando si tratta di imputazione giuridica a soggetti non umani[40], ciò ha consentito di procedere rimarcando la distinzione fondamentale tra l'attribuzione di personalità giuridica ed il semplice riconoscimento dello *status* di soggetto di diritto[41]. Tutto ciò è risultato di primaria importanza in relazione all'I.A. ed alla disamina concernente le esigenze pratiche sulla responsabilità per eventuali danni provocati dalle stesse.

È propria questa la ragione per la quale il Parlamento Europeo si auspicava la nascita delle "persone elettroniche", dunque di un criterio di imputazione autonoma riconducibile alle stesse, considerando che nella stessa Risoluzione invocava anche la necessità di una Carta etica della robotica[42], idonea ad affermare che lo sviluppo tecnologico venisse, comunque, guidato dalla volontà di salvaguardare la dignità, l'autonomia e l'autodeterminazione dell'uomo[43].

Tuttavia, lo stesso Parlamento ha, successivamente, fatto marcia indietro, rinnegando non solo l'idea di personalità elettronica, ma anche il riconoscimento di un qualsiasi *status* per l'I.A., affermando che *"qualsiasi cambiamento richiesto riguardante il quadro giuridico esistente dovrebbe iniziare con il chiarimento che i sistemi di IA non possiedono né una personalità giuridica né una coscienza umana e che il loro unico compito consiste nel servire l'umanità"*[44] e, da tale presa di posizione, l'argomento - pur rimanendo fortemente dibattuto nella letteratura scientifica – non è più stato affrontato a livello legislativo nazionale o internazionale[45].

---

[40] Infatti, le persone fisiche acquisiscono la soggettività giuridica al momento della nascita e, in tal modo, diventano astrattamente titolari di diritti e doveri; la capacità giuridica, invece, è l'effettiva titolarità delle posizioni di diritti e doveri. Per gli enti il legislatore ha previsto una disciplina differente: infatti, questi divengono soggetti giuridici solamente nel caso in cui, attraverso il riconoscimento, acquisiscono la personalità giuridica.

[41] Il nostro ordinamento non delinea esplicitamente una nozione di "soggetto". In dottrina ed in giurisprudenza si abbraccia la definizione classica elaborata da HANS KELSEN nella sua *"Dottrina pura del diritto"*, per la quale si deve intendere per "soggetto" il centro unitario di imputazione e, dunque, il titolare di situazioni giuridiche soggettive. In argomento si veda C.M. BIANCA, *Diritto Civile, La norma giuridica, i soggetti*, 2002, p. 137.

[42] Ancora oggi, tale appello è rimasto inascoltato nonostante su più fronti si richieda la formulazione di una Carta del genere, idonea a definire – in relazione allo sviluppo tecnologico – la centralità della persona e dei suoi diritti fondamentali.

[43] A.C. AMATO MANGIAMELI, *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 2019, p. 107 ss.

[44] Tale dichiarazione - volta a presentare alcune indicazioni pratiche per la Commissione Europea idonee a gettare le basi per un regime di responsabilità civile in materia di I.A. - è riportata nel considerando n. 6 della *"Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale"* - 2020/2014/INL.

[45] Infatti, dopo la predetta Risoluzione, la Commissione ha affrontato la materia dell'I.A. e ha, *in primis*, presentato – in data 21 aprile 2021 - il c.d. *"AI Act"*, ovvero una proposta di Regolamento *"del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Artificial Intelligence Act) e modifica di alcuni atti legislativi dell'Unione"*, attraverso il quale delinea una disciplina unitaria in materia di I.A., mirando ad affrontare i rischi generati da usi specifici dell'intelligenza artificiale, attraverso la previsione di un ventaglio di norme – di carattere generale – riguardanti la sicurezza ed il rispetto dei diritti fondamentali della persona. Tale Proposta ha avuto – e continua ad avere – un *iter* travagliato, dettato non solo dalla complessità di regolare una materia così viva, ma anche alle molteplici istanze da contemperare. In merito, a titolo esemplificativo si veda A. OTTOLIA, *Il 'nodo borromeo' dell'intelligenza artificiale e la sua regolazione*, in *Il Nuovo Diritto delle Società*, 12/2018; L. PARONA, *Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici, soft law e self-regulation*, in *Rivista della Regolazione dei Mercati*, 1/2020; F. DONATI, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza*

Occorre, altresì, precisare che il riconoscimento di uno *status* giuridico ai robot avrebbe come conseguenza diretta quella di affrontare un'ulteriore questione, ossia la responsabilità patrimoniale degli stessi: difatti, la dotazione di un patrimonio – o la costituzione di uno specifico fondo assicurativo – si palesa fondamentale nella misura in cui ai sistemi di I.A. venisse riconosciuto non solo un ruolo nella compagine societaria, ma – più in generale – qualora gli venisse riconosciuta una soggettività di sorta.

Pertanto, posta tale assenza di qualificazione, volendo provare a formulare un'ulteriore soluzione idonea a consentire la nomina di un algoritmo come consigliere di amministrazione, si potrebbe ancora, come suggerisce non solo autorevole dottrina [46] ma anche la prassi notarile [47], ricorrere allo stesso stratagemma realizzato per legittimare la nomina di una persona giuridica come amministratore in una società di capitali, ovvero designare per suo conto un rappresentante persona fisica [48] (così da effettuare un'applicazione analogica della disciplina del GEIE e della SE[49])[50].

In questo caso, dunque, non si avrebbe una nomina diretta dell'algoritmo all'interno del *board* societario, ma una nomina mediata – indiretta, la quale vedrebbe come *condicio sine qua non* la designazione di un rappresentante persona fisica capace di rispondere, alla pari degli altri amministratori persone

---

artificiale, in *Il diritto dell'Unione Europea*, 2/2021; F. SIBILLA – G. DI STEFANO, *L'Artificial Intelligence Act e il quadro giuridico in materia di intelligenza artificiale*, in *Diritto di Internet. Digital copyright e data protection*, 13 dicembre 2022.

In un secondo momento, ovvero il 28 settembre 2022, la Commissione ha presentato anche *l'Artificial Intelligence Liability Directive*, c.d. *"AILD"*, ovvero una proposta di Direttiva con la quale mira ad armonizzare le norme esistenti in materia di responsabilità civile extracontrattuale per i danni causati da sistemi di intelligenza artificiale derivanti da colpa, poiché per la Commissione le norme nazionali vigenti in materia di responsabilità per colpa non sono idonee a tutelare l'esercizio di azioni per responsabilità per danni causati da prodotti e servizi basati sull'IA. Inoltre, contemporaneamente alla Direttiva AILD, sono stati aperti i lavori sulla seconda Direttiva in materia di responsabilità per danno da prodotti difettosi, così da abrogare e sostituire quella vigente, cioè la direttiva europea 85/374/CEE. La disciplina di quest'ultima, infatti, è inidonea a ricomprendere le istanze derivanti dai nuovi sistemi tecnologici, intelligenze artificiali incluse, le quali al momento – proprio alla luce di tali limiti – non rientrano nel suo ambito di applicazione.

Entrambe le proposte sono ancora in fase di definizione ma in nessuna delle due è stato affrontato l'argomento dell'attribuzione, anche parziale, di una soggettività o di uno *status* specifica alla stessa I.A.

[46] A. CETRA, *La persona giuridica amministratore*, 2013, p. 70.

[47] CONSIGLIO NOTARILE DI MILANO, *Massime Commissione Società, Massima n. 100 del 28 maggio 2007, Amministratore persona giuridica e società di capitali (artt. 2380bis e 2475 c.c.)*, in *www.consiglionotarilemilano.it*, nella quale viene espressamente dichiarata la legittimità di una clausola statutaria di s.p.a. o s.r.l. che prevede la possibilità di nominare alla carica di amministratore una o più persone giuridiche o enti diverse dalle persone fisiche, dunque di realizzare la nomina di un "amministratore persona giuridica", salvi i limiti o i requisiti derivanti da specifiche disposizioni di legge per determinate tipologie di società. Inoltre, nella stessa massima il Consiglio Notarile di Milano stabilisce che ogni amministratore persona giuridica deve designare, per l'esercizio della funzione di amministratore, un rappresentante persona fisica appartenente alla propria organizzazione, il quale conseguentemente assume gli stessi obblighi e le stesse responsabilità civili e penali previsti a carico degli amministratori persone fisiche, ferma restando la responsabilità solidale della persona giuridica amministratore.

[48] V. F. PACILEO, *"Scelte d'impresa" e doveri degli amministratori nell'impiego dell'intelligenza artificiale*, in *Rivista di Diritto Societario*, 2022, p. 574.

[49] Infatti, il Consiglio Notarile di Milano, per affermare la massima – si veda la nota 47 – richiama, dal punto di vista sistematico, la già affermata configurabilità nel nostro ordinamento di un amministratore persona giuridica di un altro ente collettivo, anche di natura societaria. Più specificamente, cita a supporto della propria posizione la disciplina del Gruppo Europeo di Interesse Economico (G.E.I.E.), per il quale la disciplina italiana di attuazione del regolamento comunitario (art. 5 del d.lgs. 240/1991) contempla espressamente tale possibilità, e quella della Società Europea (art. 47.1 reg. UE 2157/2001), annoverabile nel quadro delle società azionarie, per le quali è espressamente sancita la possibilità di nominare quali amministratori anche le entità giuridiche diverse dalle persone fisiche.

[50] G. D. MOSCO, *op. cit.*, p. 248 ss.

fisiche, di qualsiasi responsabilità, inclusa quella penale, per conto dell'algoritmo.

Ancora, la nomina indiretta è consentita, alla luce di tale letteratura, anche nel caso in cui la stessa arrivi mediante una persona giuridica: infatti, non si ravvisano ostacoli alla nomina di amministratore a favore di una società specializzata in strumenti e servizi di I.A.[51]. Parimenti in questa ipotesi, la capacità giuridica delle azioni amministrative viene attribuita alla persona fisica rappresentante della persona giuridica, che a sua volta offre servizi basati sull'intelligenza artificiale.

Da tali premesse, ne consegue che gli azionisti potrebbero procedere a nominare consigli di amministrazioni composti esclusivamente da persone giuridiche controllate da società specializzate in servizi di intelligenza artificiale, andando così a configurare quello che in letteratura viene definito *Roboboard* a composizione esclusiva di *Robocompanies*, posto che resterebbe immutata, se non addirittura aumentata, la responsabilità dei rappresentanti di tali persone giuridiche[52], senza però che gli algoritmi siano effettivamente essi stessi membri del *board*.

Dunque, posto che - ad oggi - non esiste alcun tipo di soggettività riconosciuta in capo alle macchine, questi limiti finora illustrati sono condivisi con i principali ordinamenti giuridici stranieri[53]: prendendo ad esempio l'ordinamento francese, la norma di riferimento è l'art. L225-20 del *Code de commerce*, nel quale si stabilisce che le SA possono avere anche amministratori di tipo *personne morale*, a condizione che non siano il presidente del consiglio di amministrazione ed il direttore generale e che per queste sia nominato un *represéntant permanent*, il quale condivide le responsabilità secondo una solidarietà legale[54].

Un'altra soluzione paventata nella letteratura scientifica[55] è stata quella di richiamare l'istituto romanistico del *peculium* come *escamotage* per la loro carenza di soggettività e capacità in senso giuridico, così da equiparare l'intelligenza artificiale agli schiavi. Questa teoria, tuttavia, non è condivisibile perché, rimettendo la responsabilità in capo al proprietario, rischia di coinvolgere soggetti che non hanno influito in alcun modo nella formazione della macchina: l'esempio più attinente è quello dei veicoli a guida autonoma mediante un sistema di I.A..[56]

---

[51] N. ABRIANI, *op. cit.*, p. 270 ss.

[52] V., tra i tanti, V. M. PETRIN, *op.cit.*, p. 32 ss; G. D. MOSCO, *op. cit.*, p. 250; N. ABRIANI, *op.cit.*, p. 271.

[53] In realtà, negli Stati Uniti esiste una florida dottrina in materia di I.A. e *corporate governance*.
In particolare, si segnala *in primis* la teoria per la quale, dal momento che nell'ordinamento del Delaware – più specificamente nel *Delawere General Corporation Law* alla *section* 141(a) – è prevista una possibile derogabilità a favore delle *corporation* della regola generale di essere dotate di un *board*, se ne ricava che non debbano esserci necessariamente amministratori persone fisiche, si veda S. BAYERN, *The Implications of Modern Business-Entity Law for the Regulation of Autonomous Systems*, in *Stanford Technology Law Review*, 2015, p. 93 ss.
In secondo luogo, si segnala un filone scientifico a favore delle c.d. *Algorithmic Entities*, ovvero di costituire LLC destinate ad essere completamente controllate e gestite da algoritmi, attraverso una lettura volta a rendere flessibili le disposizioni di cui al *Revised Uniform Limited Liability Company Act* (c.d. RULLCA), si veda S. BAYERN, *op. cit.*, p. 101 ss.

[54] P. LE CANNU – B. DONDERO, *Droit des sociétés*, Parigi, 2022, p. 467 ss.

[55] H. ASHRAFIAN, *Artificial Intelligence and Robot Responsabilities: Innovating Beyond Rights*, in *Science and Engineering Ethics*, 2015, p. 325.

[56] M. RIZZUTI, *Il peculium del robot. Spunti sul problema della soggettivizzazione dell'intelligenza artificiale*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, p. 283 – 288.

La prospettiva del proprietario comporterebbe una responsabilità oggettiva proprio in capo al proprietario dell'autovettura per i danni cagionati da difetti di funzionamento dell'intelligenza artificiale, anche se lo stesso non ha avuto alcun tipo di ruolo in merito.[57]

Pertanto, nel solco di quanto finora affermato, si può concludere ribadendo che, mentre è possibile una nomina indiretta di algoritmo all'interno di un consiglio di amministrazione, in relazione alla nomina diretta ciò è tuttora impossibile e tale continuerà ad essere fintantoché non verrà posto in essere uno specifico ed esplicito riconoscimento di soggettività giuridica per gli stessi - oltre che uno sviluppo tecnologico idoneo a superare quei limiti di cui al paragrafo precedente.

6. Conclusioni.

A conclusione di questo breve percorso, si deve svolgere una considerazione di carattere generale volta ad interrogarsi circa la distinzione tra quello che è l'attuale presente dell'intelligenza artificiale e quello che potrebbe essere il suo futuro.

Rispetto al limite di tipo tecnologico riguardante l'impossibilità attuale per gli algoritmi di replicare la funzione gestoria in senso lato nella sua totalità, il progresso scientifico procede a ritmi talmente serrati che nulla vieta di immaginare – in un futuro neanche troppo lontano se si pensa agli ultimi utilizzi paventati per *i chatbot*[58] - che si possa arrivare a replicare anche quelle caratteristiche tipiche della natura umana che consentono di affrontare e gestire tutti quei compiti non routinari che necessitano di adattabilità rispetto alle circostanze concrete, nonché quelle componenti necessarie alla configurazuone del "*managerial decision-making*".

Ciò posto, quello che è di rilievo giuridico consiste nell'interrogativo circa la necessità o meno di concedere la personalità elettronica – o qualsiasi altro *status* – alle macchine, in maniera tale da renderle indipendenti dalle persone fisiche ed in grado di interagire con le stesse, attraverso la capacità giuridica e di agire.

Certamente, l'idea di attribuire capacità giuridica ad un algoritmo o, più in generale, a strumenti di intelligenza artificiale può sembrare stravagante; tuttavia, non può esserlo più di quanto dovesse apparire strano il riconoscimento di un'autonoma soggettività alle prime persone giuridiche.

---

[57] F. PACILEO, *op. cit.*, p. 575.

[58] I *chatbot* sono uno specifico strumento di intelligenza artificiale in grado di interagire, in maniera autonoma, durante una conversazione. Più specificamente, si tratta di un *software* in grado di rispondere a qualsiasi tipo di domanda che gli viene posta ed a prescindere da come gli viene formulata grazie ad una nuova variante di modello di previsione linguistica autoregressivo, cioè il Gpt-3.5, che – attraverso il *deep learning* – produce testi simili a quelli umani, attraverso un'interfaccia utilizzabile da chiunque. Questa nuova variante di *chatbot* sta avendo una diffusione capillare, in quanto è in grado di rispondere a molteplici esigenze: tra queste, si segnala il fatto che molteplici studi legali si stiano dotando di *software* con chatbot specifiche in grado di dare pareri legati immediati rispetto alle questioni sottoposte alla loro attenzione. Inoltre, è notizia di gennaio 2023 che la *startup* americana *DoNotPay* abbia programmato una *chatbot* idonea a ricoprire il ruolo di avvocato e che farà la sua prima comparsa in tribunale per aiutare un imputato in una causa legale per il ricorso contro una multa. Tale I.A., utilizzata attraverso uno *smartphone*, ascolterà in tempo reale le argomentazioni dei giudici e fornirà indicazioni all'imputato tramite cuffie.

Infatti, proprio come successe con le persone giuridiche, l'I.A. dotata di capacità giuridica costituirebbe un nuovo e contemporaneo soggetto di diritto; inoltre, alla stessa intelligenza si confà perfettamente la nota definizione elaborata nel 1819 per le società dal giudice Marshall: *"An artificial being, invisible, intangible and existing only in contemplation of the law"*[59].

Con il riconoscimento di uno *status* soggettivo le macchine potrebbero avere un ruolo diretto, e non mediato, all'interno dei processi gestori dell'impresa, anche se, nello sviluppo di questo percorso, deve comunque rimanere - come stella polare per l'elaborazione di tale progresso giuridico - una visione di natura antropocentrica[60].

Posta tale prospettiva, lo scopo perseguito con il riconoscimento di personalità elettronica non sarebbe il semplice ampliamento della sfera giuridica dell'I.A., quanto piuttosto la possibilità di creare maggiore tutela per la controparte umana che si relaziona con la stessa[61].

Questa soluzione, poi, potrebbe rispondere anche alla problematica principale che coinvolge l'utilizzo degli algoritmi in contesti gestori – o comunque decisionali -, ovvero la responsabilità patrimoniale diretta per danni derivanti dalle macchine. Infatti, pur essendo questa tematica e quella della personalità elettronica due questioni che non devono necessariamente essere affrontate insieme[62], potrebbero comunque avere un'unica soluzione, idonea a garantire esigenze attuali e concrete.

Inoltre, si sottolinea come l'utilizzo degli algoritmi nei processi gestori d'impresa, sia in un'ottica diretta sia in maniera mediata, necessita di uno specifico processo di trasparenza e di responsabilizzazione[63], in maniera da

---

[59] *Trustees of Dartmouth College v. Woodward*, 17 U.S. (4 *Wheat.*) 518 (1819).

[60] In tale ottica va letta l'indicazione di una Carta Etica della Robotica suggerita dal Parlamento Europeo nella sua Risoluzione del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica n. 2015/2013/(INL), si veda paragrafo 5.

[61] G. ZICCARDI, *Diritto, tecnologie del futuro e nuovi mercati: il pensiero di Alec Ross*, in *Diritto Mercato Tecnologia*, 2016, p. 11 ss; M. SCIALDONE, *Il diritto dei Robot: la regolamentazione giuridica dei comportamenti non umani*, in F. MARZANO, E. PIETRAFESA, T. MEDICI (a cura di), *La Rete e il Fattore C (Cultura, Complessità, Collaborazione)*, Stati Generali Innovazione, 2016, p. 76 ss.

[62] Come effettivamente sta avvenendo, visto che la Commissione ha presentato *l'Artificial Intelligence Liability Directive*, c.d. "AILD", senza preoccuparsi di disciplinare in alcun modo la personalità elettronica degli algoritmi, v. *infra* nota 45.

[63] Circa il cambio di paradigma rispetto alla percezione della necessità di prevedere idonee soluzioni di responsabilizzazione in merito alle intelligenze artificiali in generale, e non solo specificamente nei contesti di *corporate governance*, si deve segnalare come il Legislatore Europeo abbia stabilito una classificazione dei sistemi di I. A. in base ai rischi che questi pongono per i diritti fondamentali. Più specificamente, il titolo III dell'*A.I. ACT* (v. *infra* nota 45) disciplina specifiche regole per quelle intelligenze artificiali che creano un rischio reputato alto per la salute, per la sicurezza o per i diritti fondamentali delle persone fisiche. La classificazione di I.A. ad alto rischio può fondarsi sulla funzione svolta, sulla finalità e sulle modalità specifiche di utilizzo del sistema di I.A. stesso. Applicando un approccio *risk based*, il Legislatore Europeo subordina la circolazione nel mercato europeo di tali categorie di I.A. al rispetto di requisiti obbligatori e sulla base di una valutazione *ex ante* di conformità.
Il capo 1 del titolo III fissa – in merito – opportune regole di classificazione, individuando due categorie principali di sistemi di I.A. ad alto rischio:
• i sistemi di I.A. destinati ad essere utilizzati come componenti di sicurezza di prodotti soggetti a valutazione della conformità *ex* ante da parte di terzi;
• altri sistemi di I.A. indipendenti che presentano implicazioni principalmente in relazione ai diritti fondamentali esplicitamente elencati nell'allegato III dell'*A.I. ACT*.

rendere tracciabili i criteri di azione amministrativa derivanti dagli stessi ed in aderenza alla *Business Judgement Rule*[64].

Infatti, se in un'ottica di amministrazione indiretta, tali processi consentirebbero di addivenire alla tracciabilità degli strumenti algoritmici, così da individuare ed eventualmente valutare ipotesi di responsabilità delle I.A. amministratori, nonché profili in capo ai rappresentanti delle stesse, a maggior ragione in un contesto di amministrazione diretta ricoprirebbero un vero e proprio presupposto per l'attivazione della disciplina della società[65].

In conclusione, dunque, non si può non constatare che – ad oggi – non è ancora prefigurabile un algoritmo eletto consigliere di amministrazione algoritmo ed in grado di ricoprire tale incarico in totale autonomia, posti i limiti analizzati; allo stesso tempo, nulla osta alla possibilità di eleggere nel board societario un algoritmo in via indiretta, dunque mediante la nomina di un suo rappresentante.

In questo contesto, si deve sottolineare come sia fondamentale, non solo alla luce delle prospettive attuali ma soprattutto sulla base di quelle futuribili, che vengano predisposte – a livello generale – dettami normativi[66] capaci di consentire l'inserimento dell'intelligenza artificiale nella *governance* societaria, così da calibrarne le funzioni, contemperarne i rischi e, ancora, configurarli all'interno di una visione guidata da principi di natura antropocentrica[67].

Solo così – e, si aggiunge, anche con un riconoscimento, se non della personalità elettronica, di un qualche *status ad hoc* – sarà possibile ricorrere agli algoritmi in maniera diretta nei processi gestori societari; fino ad allora, il loro ruolo potrà essere solo quello di svolgere una funzione di supporto degli stessi amministratori, così come ci insegna l'esperienza citata di VITAL[68].

---

[64] Il c.d. principio della *Business Judgement Rule* prevede che, in caso di accertamento della responsabilità degli amministratori, il relativo giudizio sulla diligenza degli stessi nell'adempimento del proprio mandato non possa mai andare a sindacare o investigare nel merito le scelte di gestione o le modalità e circostanze di tali scelte (dunque elementi quali la convenienza, l'opportunità, la profittabilità e la remuneratività), anche qualora siano ravvisabili profili di rilevante alea economica, ma debba limitarsi alla verifica della sola diligenza circa la corretta procedimentalizzazione del processo decisionale seguito dagli amministratori.

[65] V. N. Abriani, *op. cit.*, 284; M. Petrin, *op. cit.*, p. 41.

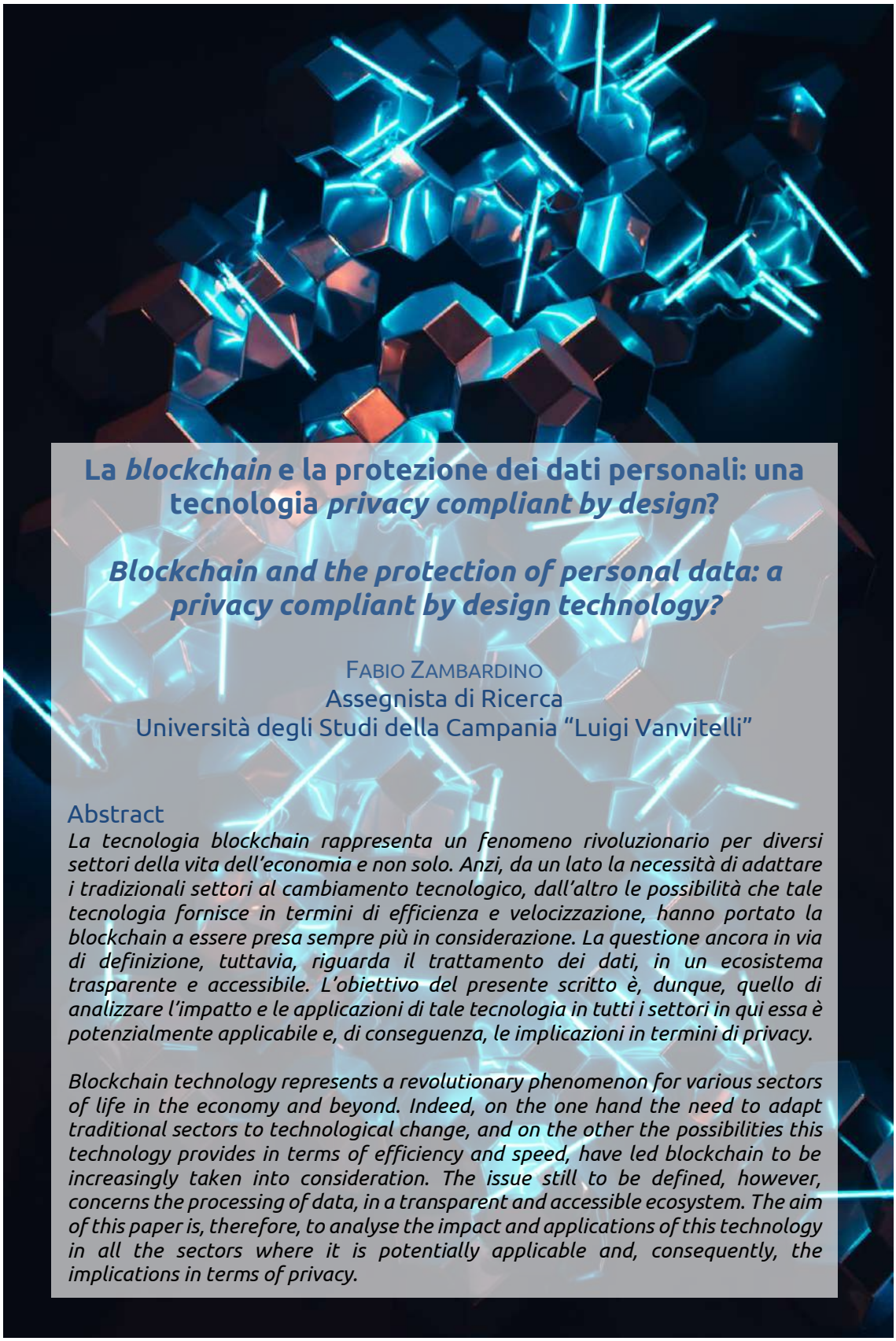
[66] A parere di chi scrive, sarebbe auspicabile che l'Unione Europa, la quale ha esercitato nel corso del tempo un ruolo primario per la modernizzazione del governo societario, fondamentale per consentire alle imprese del territorio europeo di rispondere alle nuove istanze del mercato e degli *stakeholder*, intervenisse in tal senso con la previsione di una disciplina comune ed idonea a gettare le condizioni necessarie a consentire non solo di cogliere tali istanze di cambiamento, ma – soprattutto – il corretto svolgimento dei processi di *governance* – alla luce di queste nuove istanze – in tutte le imprese degli Stati membri.

[67] In merito, si sottolinea che molte società, in assenza di predette linee guida generali, hanno realizzato dei *Corporate AI Principles*, ossia degli strumenti di autoregolamentazione concernenti l'utilizzo delle intelligenze artificiali nella propria realtà societaria, con specifiche ai fini della *corporate governance*. Tali strumenti sono paragonabili ai codici di condotta di cui all'art. 40 del Regolamento Europeo 2016/679 c.d. GDPR. Tra i principali esempi, si cita quello di *Microsoft*, reperibile all'indirizzo *https://www.microsoft.com/en-us/ai/our-approach-to-ai*, e quello di *Google*, reperibile all'indirizzo *https://blog.google/technology/ai/ai-principles/*.

[68] V. paragrafo 4.

Zambardino F, 'La blockchain e la protezione dei dati personali: una tecnologia privacy compliant by design?' (2022) 2 EJPLT, 136-152.
DOI: https://www.doi.org/10.57230/ejplt222FZ

EJPLT
ISSN 2704-8012



La *blockchain* e la protezione dei dati personali: una tecnologia *privacy compliant by design*?

Blockchain and the protection of personal data: a privacy compliant by design technology?

FABIO ZAMBARDINO
Assegnista di Ricerca
Università degli Studi della Campania "Luigi Vanvitelli"

Abstract

La tecnologia blockchain rappresenta un fenomeno rivoluzionario per diversi settori della vita dell'economia e non solo. Anzi, da un lato la necessità di adattare i tradizionali settori al cambiamento tecnologico, dall'altro le possibilità che tale tecnologia fornisce in termini di efficienza e velocizzazione, hanno portato la blockchain a essere presa sempre più in considerazione. La questione ancora in via di definizione, tuttavia, riguarda il trattamento dei dati, in un ecosistema trasparente e accessibile. L'obiettivo del presente scritto è, dunque, quello di analizzare l'impatto e le applicazioni di tale tecnologia in tutti i settori in qui essa è potenzialmente applicabile e, di conseguenza, le implicazioni in termini di privacy.

Blockchain technology represents a revolutionary phenomenon for various sectors of life in the economy and beyond. Indeed, on the one hand the need to adapt traditional sectors to technological change, and on the other the possibilities this technology provides in terms of efficiency and speed, have led blockchain to be increasingly taken into consideration. The issue still to be defined, however, concerns the processing of data, in a transparent and accessible ecosystem. The aim of this paper is, therefore, to analyse the impact and applications of this technology in all the sectors where it is potentially applicable and, consequently, the implications in terms of privacy.

© The author(s) 2022, 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: Privacy; Blockchain; GDPR; trasparenza; decentralizzazione.

Summary: Introduzione. – 1. Le origini e lo sviluppo del concetto di privacy. – 2. L'introduzione delle Distributed Ledger Technologies. – 3. I vantaggi in termini di privacy legati all'utilizzo della blockchain. – 4. Privacy contro trasparenza. – 5. Prime riflessioni. Quali implicazioni in termini di sovranità statale. – 6. Quale rapporto con il General Data Protection Regulation (GDPR).

Introduzione.

Nell'odierno scenario globale, le nuove dinamiche della raccolta e del trattamento delle informazioni e dei dati personali, la maggiore invasività del controllo sugli individui, sia da parte di soggetti pubblici che privati, hanno comportato una sempre crescente richiesta di tutela[1].

Infatti, il centro gravitazionale del diritto alla *privacy* è sempre più individuato, più che nel diritto ad essere "lasciati soli" (il c.d. *right to be let alone*), nella possibilità di ogni soggetto di controllare l'uso delle informazioni che lo riguardano e nel considerare i problemi della *privacy* «nel quadro dell'attuale organizzazione del potere, di cui appunto l'infrastruttura informativa rappresenta ormai una della componenti fondamentali»[2].

Considerate le premesse, il presente scritto, dopo avere brevemente analizzato le circostanze che hanno portato alla nascita, sviluppo e conseguente tutela del concetto di *privacy*, si concentrerà sul rapporto che intercorre tra il diritto alla tutela dei dati personali e le nuove tecnologie, con particolare riferimento alla *blockchain*[3].

[1] Si veda, sul punto, G. RESTA, in G. ALPA e G. RESTA, *Le persone e la famiglia. Le persone fisiche e i diritti della personalità*, in *Trattato di diritto civile*, diretto da R. SACCO, Torino, 2019, 145-632, in cui viene privilegiato, in particolare, una interpretazione «orientata ai valori», considerata la linea maggiormente appropriata alla trattazione dei temi concernenti la persona e i diritti della personalità. In tale scenario, la globalizzazione dei mercati e l'evoluzione delle tecnologie costituiscono, per gli autori, complesse sfide al ruolo del diritto.

[2] S. RODOTÀ, *Tecnologia e diritti*, Bologna, 1995, 19.

[3] Parte della dottrina afferma come, alla stessa stregua i diritti di proprietà intellettuale, anche il diritto alla privacy è strettamente connesso alla tecnologia. L'evoluzione del concetto di privacy è proficuamente letta in chiave di diritto e tecnologia. G. PASCUZZI, U. IZZO, M. MACILOTTI (a cura di), *Comparative Issues in the Governance of Research Biobanks. Property, Privacy, Intellectual Property, and the Role of Technology*, Heidelberg-New York-Dordrecht-Londra, 2013. In argomento, G. PASCUZZI, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, Bologna, 2003. Secondo autorevole dottrina, sono i mutamenti delle tecnologie dell'informazione, della riproduzione e dell'ingegneria genetica a muovere il cammino che porterebbe dal diritto alla riservatezza (il diritto ad essere lasciato solo) al diritto di mantenere il controllo sulle proprie informazioni personali. S. RODOTÀ, Repertorio di fine secolo, Roma – Bari, 1999, 201. T. E. FROSINI, *Tecnologie e libertà costituzionali*, in G. COMANDÉ e G. PONZALLI (a cura di), *Scienza e diritto nel prisma del diritto comparato*, Milano, 2004, 189, il quale, ancora in tema di rapporto tra tecnologia e *privacy* afferma come le nuove scoperte tecnologiche abbiano rappresentato e continuino a rappresentare uno sviluppo delle libertà; «anzi, le libertà si sono potute notevolmente accrescere ed espandere verso nuove frontiere dell'agire umano proprio grazie al progresso tecnologico». T. E. FROSINI, *Il diritto costituzionale di accesso ad Internet*, in M. PIETRANGELO (a cura di), Il diritto di accesso ad Internet, Collana ITTIG-CNR, Serie "Studi e documenti", n. 9, Napoli, 2011, 24. Tra i primi a introdurre tali tematiche, sebbene in chiave più generale, S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari 1997.

1. Le origini e lo sviluppo del concetto di privacy.

Storicamente, i concetti giuridici di riservatezza e di *privacy* risalgono alla fine del XIX secolo. Infatti, è con l'articolo "*The Right To Privacy*"[4] di Warren e Brandeis del 1890 che la nozione di *privacy* ha iniziato ad assumere la connotazione giuridica descritta nel paragrafo introduttivo[5].

Di conseguenza, il vero riconoscimento del diritto alla *privacy* si è avuto dopo un lungo processo in cui un ruolo fondamentale ha avuto, inevitabilmente, la giurisprudenza[6].

Infatti, a tal proposito, il giudice William O. Douglas, nel caso *Griswold v. Connecticut*, ha affermato che un diritto generale alla privacy si trova nelle c.d. "*penumbras*" create dalle garanzie specifiche di diversi emendamenti della Carta dei Diritti[7].

Tuttavia, dopo la pubblicazione del "*The Right to Privacy*", l'elaborazione dottrinale statunitense in materia fu piuttosto scarsa, se non addirittura inesistente. Tale circostanza ha contribuito a rafforzare il ruolo dei giudici, i quali, con una serie di decisioni, «chiarirono alcuni principi dell'ordinamento giuridico americano e, cosa più importante, attraverso una interpretazione evolutiva degli emendamenti del Bill of Rights, riuscirono a rintracciare il fondamento giuridico del diritto alla privacy»[8].

Una spinta innovatrice si è avuta a partire dagli anni Sessanta del '900, quando i cambiamenti che sono derivati dal passaggio da uno Stato liberale tradizionale ad uno Stato pluralistico di diritto accrebbero la sensibilità verso le questioni inerenti alla tutela della sfera privata.

---

[4] S. WARREN e L. D. BRANDEIS, *The right of privacy*, in *Harv. L. Rev.*, 1890, 193.

[5] Per un approfondimento in tema di riservatezza, S. RODOTÀ, *Riservatezza*, in Enciclopedia Treccani, 2000. Si veda, inoltre, R. PARDOLESI, *Riservatezza: problemi e prospettive*, in M. SPINELLI (a cura di), *Responsabilità civile*, Bari, 1974, vol. II, 316 ss. L'autore, sul punto, già anni fa ha sostenuto come «l'informatica […] ha introdotto, sia nella raccolta che nel trattamento e nell'impiego di dati, un cambiamento quantitativo così radicale da volgersi in qualitativo». *Ivi*, 381. Ancora, l'autore sostiene, in riferimento alla nascita del diritto alla *privacy*, che alla stessa stregua dei diritti di proprietà intellettuale, si tratta di un prodotto recente della tradizione giuridica occidentale. *Ivi*, 391.

[6] In particolare, il riferimento va ai casi *Griswold v. Connecticut*, 381 U.S. 479 (1965), *NAACP v. Alabama*, 357 U.S. 449 (1958), *Katz v. U.S.* 347 (1967). L'opera dei giudici, infatti, non solo ha sollecitato fortemente il dibattito dottrinale in materia di *privacy* ma ha portato all'attenzione del legislatore le tematiche relative alla protezione della sfera privata, contribuendo così alla piena affermazione del diritto e alla sua tutela. Questo è quanto accaduto non solo negli Stati Uniti d'America ove il formante giurisprudenziale ha un posto privilegiato all'interno dell'ordinamento giuridico, ma anche all'interno di ordinamenti giuridici di *civil law* come quello italiano.

[7] J. B. STONEKING, *Penumbras and Privacy: A Study of the Use of Fictions in Constitutional Decision-Making*, in *West Virg. L. Rev.*, 1985, 859. Le garanzie esplicite del *Bill of Rights*, considerate collettivamente, sono state definite "*penumbras*" o "emanazioni" che «help [to] give them life and substance». In altre parole, i tribunali possono derivare dei diritti impliciti che sono necessari per dare piena attuazione a quelli espliciti. Si vedano, in proposito B. HENLY, *"Penumbra": The Roots of a Legal Metaphor*, in *Hastings Const. L. Q.*, 1987, 81, 83–84; G. H. REYNOLDS, *Penumbral Reasoning on the Right,* in *U. Pa. L. Rev.*, 1992, 1334–36; J. C. RIDEOUT, *Penumbral Thinking Revisited: Metaphor in Legal Argumentation*, in *J. ALWD*, 2010, 155–56.

[8] L. MIGLIETTI, *Profili storico-comparativi*, *cit.*, 2014. L'atteggiamento della giurisprudenza così come quello della società nei confronti dell'esigenza *privacy* fu però altalenante. Mentre una parte del tessuto sociale americano e una minoranza dei giudici della Corte Suprema «propugnavano un approccio difensivo della libertà e, nello specifico, della privacy; l'altra parte della società e la maggioranza dei giudici della Corte Suprema erano ostili verso un atteggiamento liberale e soprattutto verso il riconoscimento di un autonomo diritto alla privacy». Il riferimento è ai già citati casi *Griswold v. Connecticut*, *NAACP v. Alabama*, *Katz v. U.S. Ibid.* Questa antiteticità di vedute ha rappresentato non solo un ostacolo per lungo tempo all'elaborazione di una teoria in materia ma, soprattutto, non ha permesso di chiarire la natura del concetto, lasciandolo così alla mercé degli oscillanti orientamenti giurisprudenziali che si alternavano nel tempo.

Infatti, se fino a quel momento la giurisprudenza aveva assunto posizioni ancora non del tutto definite per quanto concerne il riconoscimento di un diritto alla *privacy* costituzionalmente garantito, a partire dagli anni Sessanta vennero emesse una serie di sentenze fondamentali con le quali la Corte Suprema riconobbe la *privacy* come meritevole di tutela in rapporto tanto alla vita pubblica quanto a quella privata dell'individuo[9].

Successivamente, nel 1970, venne emanata una legge, il *Privacy Act*, che ancora oggi rappresenta un importante testo normativo di riferimento in materia di privacy.

È opportuno sottolineare, che la mancanza «di una legislazione federale a vocazione generale che possa impartire un indirizzo comune ai vari Stati membri ha portato a qualificare il sistema di tutela della privacy statunitense come un sistema di natura settoriale. Le leggi degli Stati Uniti perseguono l'obiettivo di regolamentare il trattamento dei dati in ambiti specifici di attività economica, nella misura in cui vi possano essere rischi per il cittadino considerato nel suo status di consumatore»[10].

Ne consegue che negli USA, differentemente dall'Europa, la privacy non si configura come un diritto fondamentale dell'individuo, ma come un diritto del consumatore, da bilanciare con le esigenze delle imprese. Ed infatti è la FTC (*Federal Trade Commission*), l'agenzia deputata alla tutela dei consumatori negli States, competente a vigilare anche sull'aderenza dei comportamenti delle aziende a quanto esse dichiarano nelle proprie privacy policy e sul rispetto delle leggi sulla privacy[11].

Nell'ambito dell'Unione europea, contrariamente, lo sviluppo e la tutela del concetto di *privacy* ha vissuto fasi molto differenti. In tale contesto, infatti, il trattamento dei dati personali [12] è considerato, oggi, uno degli elementi maggiormente qualificanti del sistema giuridico europeo, il quale conferisce a tale diritto il medesimo valore riservato ai diritti fondamentali dell'uomo[13].

Inizialmente pensato in chiave di integrazione economica, la materia della *privacy* all'interno del sistema giuridico comunitario non era stato adeguatamente considerato e regolato attraverso specifiche disposizioni

---

[9] Negli stessi anni anche il dibattito dottrinale riprese vigore e tra le varie teorie elaborate fra tutte W. PROSSER, *Privacy*, in *Cal. L. Rev.*, vol. 48, 1960. La teoria di Prosser si basava sulla negazione del concetto unitario di *privacy*– concezione che invece avevano difeso Warren e Brandeis – sostenendo, al contrario, una concezione pluralistica. Qualche anno più tardi, nel 1964, Edward Blounstein pubblicò un saggio nel quale, rifiutando di accogliere l'elaborazioni teoriche di Prosser, propugnava il ritorno ad una visione unitaria della privacy, concepita come valore essenziale dell'uomo e come diritto meritevole di tutela in tutti gli ambiti normativi. E. J. BLOUNSTEIN, *Privacy as an aspect of human dignity: an answer to Dean Prosser*, in NYU *L. Rev.*, 1964, 974, sostiene «I contend that the gist of the wrong in the intrusion cases is not the intentional infliction of mental distress but rather ablow to human dignity, an assault on human personality. Eavesdropping and wiretapping, unwanted entry into another's home, may be the occasion and cause of distress and embarassement but that is not what makes these acts of intrusion wrongful. They are wrongful because they are demeaning of individuality, and they are such whether or not they cause emotional trauma». *Ibid.*

[10] L. MIGLIETTI, *Profili storico-comparativi*, *cit.*

[11] *Ibid.*

[12] Sulla nozione di trattamento dei dati, si veda L. LAMBO, *La disciplina sul trattamento dei dati personali: profili esegetici e comparatistici delle definizioni*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 75.

[13] Si vedano, in merito, L. BOLOGNINI, E. PELINO, C. BISTOLFI (a cura di), *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; R. CASO, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano*, in *Dir. Internet*, 2008, 466- 472.

normative, essendo quello della riservatezza un tema appartenente alla sfera dei diritti umani[14].

Tuttavia, si è provveduto alla tutela dei principi fondamentali della persona – e, di conseguenza, con essi anche la *privacy* – per merito della giurisprudenza della Corte di Giustizia dell'UE[15].

In siffatto scenario, nel momento stesso in cui il concetto di *privacy* ha assunto maggiore rilievo in seno alle istituzioni, considerato come un diritto a cui riservare una garanzia giuridica, si è diffusa l'espressione "*data protection*", ed è stato trasformato l'originario diritto alla riservatezza in un vero e proprio controllo specifico dei dati[16].

L'inizio della lunga e travagliata evoluzione normativa in materia di trattamento dei dati personali che ha avuto luogo in Europa è stato segnato dall'adozione della direttiva 95/46/CE del Parlamento Europeo e del Consiglio (cosiddetta "*Data Protection Directive*" o anche direttiva "madre")[17]. Con essa il legislatore europeo, oltre a prevedere un'accurata definizione di dati personali[18], ha recepito il nuovo profilo assunto dalla *privacy* al fine di tutelare i diritti e le libertà delle persone fisiche con specifico riferimento al trattamento dei dati e alla libera circolazione degli stessi, stabilendo altresì i principi relativi

[14] Per una attenta ricostruzione del dibattito sul tema, che ha animato la dottrina a partire dai primi decenni del Novecento, si veda S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, 39 ss. In Italia, per esempio, a ridosso della riforma del Codice civile, alcuni giuristi cominciarono a interessarsi al tema della "riservatezza", inquadrandolo nel contesto più generale dei diritti della personalità. A partire da quel momento in tema di diritto alla riservatezza si sviluppò un ampio dibattito dottrinale che vide coinvolti illustri giuristi e che trovò causa, anzitutto, nella mancanza di una norma esplicita e di portata generale che si ponesse a fondamento giuridico del sopraddetto diritto. In argomento, si vedano *ex multis* G. GIAMPICCOLO, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza nel quadro dei diritti della personalità*, in *Riv. Dir. Civ.*, 1963; A. DE CUPIS, *Teoria generale, diritto alla vita e all'integrità fisica, diritto sulle parti staccate dal corpo e sul cadavere, diritto alla libertà, diritto all'onore e alla riservatezza*, Milano, 1959; F. CARNELUTTI, *Il diritto alla vita privata*, in Rivista trimestrale di diritto pubblico, 1955; A. RAVÀ, *Istituzioni di diritto privato*, Padova, 1938.

[15] Per un approfondimento A. TERRASI, *Il rapporto tra diritto alla privacy e protezione dei dati personali tra Corte di giustizia dell'Unione europea e Corte europea dei diritti dell'uomo*, in M. DISTEFANO (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, 2017, 127-149; R. CASO, *Misure tecnologiche di protezione: cinquanta (e più) sfumature di grigio della Corte di giustizia europea*, Trento Law and Technology Research Group. Research Papers, 2014. È interessante, a tal proposito, osservare la ricostruzione fatta da Gambaro, il quale, con riferimento alla libera circolazione dei dati personali, sottende la concezione di questi ultimi come beni giuridici oggetto di scambio. Per un approfondimento di tale pensiero si rimanda a A. GAMBARO, *I beni*, in *Tratt. dir. civ. e comm.*, già diretto da A. CICU e F. MESSINEO, continuato da L. MENGONI, Milano, 2012.

[16] In tema, si rimanda a G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012. L'autrice, in particolare, ben sintetizza l'evoluzione del termine. Infatti, comunque lo si pronunci, «è oramai polisenso e indica una molteplicità di beni giuridici e di interessi suscettibili di differente tutela». Il bene della riservatezza in senso stretto, ossia la tutela della vita privata, la segretezza, la privatezza dello spazio, la protezione delle informazioni. La pluralità e la diversità dei beni giuridici considerati «si riflettono anche nella scelta del legislatore europeo di disciplinare in maniera distinta la tutela della vita privata e la protezione dei dati personali, rispettivamente nell'art. 7 e nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea». G. FINOCCHIARO, *Il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, in Il *trattamento dei dati personali in ambito giudiziario*, Scuola Superiore della Magistratura, Roma, 2021, 21.

[17] F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 6.

[18] Art. 2, lettera a) della direttiva n. 95/46/CE definisce dati personali «qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale».

alla legittimazione degli stessi[19].

Nonostante le successive modifiche alla "direttiva madre" apportate con l'obiettivo di fronteggiare le nuove sfide derivanti dal crescente sviluppo della tecnologia delle comunicazioni che hanno richiesto, nel tempo, una maggiore tutela dei dati personali, l'impianto normativo europeo in tema di tutela della *privacy* è rimasto alquanto obsoleto, almeno fino all'entrata in vigore del *General Data Protection Regulation*[20].

2. L'introduzione delle Distributed Ledger Technologies.

L'utilizzo di *Distributed Ledger Technologies*, come la *blockchain*, si è esteso dal mercato delle criptovalute ad altri campi, incluso, per esempio, il settore della *privacy*[21].

In particolare, la necessità di decentralizzazione risiede nella crescente preoccupazione da parte degli utenti per la perdita di controllo in relazione ai propri dati personali registrati su Internet[22].

A questo proposito, la stessa struttura della tecnologia *blockchain* consentirebbe di preservare la riservatezza dei dati; tuttavia, tali architetture possono dimostrarsi talvolta vulnerabili all'analisi dei metadati. Di conseguenza, se non adeguatamente progettate, «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»[23].

---

[19] L. BOLOGNINI e PELINO (a cura di), *Codice della disciplina privacy*, Milano, 2019. Sulle medesime tematiche, anche F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016. Gli autori, in particolare, propongono una lettura organica della vigente disciplina in materia di privacy e protezione dei dati personali, oggi estremamente frammentata e vasta in UE e in Italia, consentendo così un'immediata interpretazione della materia attraverso l'analisi combinata della normativa europea e di quella nazionale, nonché dei provvedimenti dell'Autorità Garante.

[20] F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH, *Il codice dei dati personali*, *cit.*, 9.

[21] Per una disamina dei diversi utilizzi della *blockchain*, A. BORRONI, *Blockchain: Uses and Potential Value*, in *Legal Perspective on Blockchain Theory, Outcomes, and Outlooks*, A. BORRONI (ed.), Pubblicazioni del Dipartimento di Scienze Politiche Jean Monnet dell'Università degli Studi della Campania Luigi Vanvitelli, ESI, 2019. Per un'analisi, invece, relativamente a possibili scenari regolamentari, si rinvia a A. BORRONI e M. SEGHESIO, *Bitcoin e Blockchain: Un'analisi comparatistica dalla nascita alla potenziale regolamentazione*, in *La relazione tra intermediari e clienti nel diritto dell'economia*, G. GIMIGLIANO (ed.), *IANUS Diritto e Finanza*, no. 19, 2019.

[22] Taluni autori, in proposito, fanno riferimento alla nascita di una vera e propria identità virtuale in quanto parlare di identità personale, nel contesto attuale, significa fare i conti anche con una nuova dimensione, ossia quella informatica, in cui l'identità personale risulta indispensabile per il compimento di una serie di azioni, per lo più di carattere patrimoniale – si pensi all'utilizzo delle carte di credito sul web, alle varie transazioni commerciali, fino ad arrivare ai social network. Su questo punto, S. RODOTÀ, *Quattro paradigmi per l'identità*, in *Vivere la democrazia*, Bari, 2018, 20 ss; G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, CONTR. IMPR., 2017, 725; G. RESTA, *Identità personale e identità digitale*, in *Dir. Infor.*, 2007. Per un primo approfondimento relativamente al rapporto tra *privacy* e *blockchain*, V. DEVI, V. SABARESHWARAN, R. SARAVANA KUMAR, M. SIVASANKAR, *Privacy-Preserving Healthcare Architecture Using Blockchain*, IJCSMC, vol. 9, 2020, 116-120; S. SAKHO *et al.*, *Privacy Protection Issues in Blockchain Technology*, IJCSIS, vol. 17, 2019, 124-131; R. DE LA CRUZ, *Privacy Laws in the Blockchain Environment*, in *Annals of Emerging Technologies in Computing*, vol. 3, 2019, 34-44; G. ALPA, *Tecnologie e diritto privato*, in *Rivista italiana per le scienze giuridiche*, 2017.

[23] P. DE FILIPPI, *The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies*, Paris, 2016, 1. Prima di approfondire la propria analisi, l'autore sottolinea come nonostante gli ovvi vantaggi che offrono per quanto riguarda la sovranità dei dati, le architetture decentralizzate presentano anche caratteristiche che, se non tenute in debita considerazione, potrebbero, in ultima analisi, compromettere la

In questa prospettiva, non va dimenticato che la natura pseudonima di molte reti che si basano sulla *blockchain* consente agli individui la possibilità di condurre le proprie transazioni su base *peer-to-peer*, senza la necessità di rivelare la propria identità alle controparti[24].

Allo stesso tempo, per converso, la trasparenza derivante dalle *distributed ledger technologies* è tale che chiunque ha la possibilità di accedere alla cronologia di tutte le transazioni memorizzate sulla *blockchain*, affidandosi così all'analisi dei dati in essa contenuti per ricavare informazioni potenzialmente sensibili[25].

In questo senso, tuttavia, laddove il sistema non sia progettato accuratamente, la trasparenza potrebbe finire per interferire con la *privacy* degli utenti[26].

Di conseguenza, a meno che non si utilizzino ulteriori mezzi tecnici per proteggere la riservatezza delle comunicazioni online, potrebbe risultare che le infrastrutture decentralizzate – progettate per promuovere la *privacy* e l'autonomia – finiscano per essere più vulnerabili alle agenzie governative o al controllo delle imprese rispetto alle loro controparti centralizzate[27].

Innanzitutto, il rapporto tra *privacy* e registri decentralizzati potrebbe, almeno all'apparenza, non risultare immediatamente calzante. In effetti, potrebbe sembrare più logico affermare che la *blockchain* sia meglio costruita al fine di preservare i dati e la *privacy* degli utenti[28].

A ogni modo, permane ancora un elevato livello di incertezza sulla potenziale predisposizione di soluzioni alternative – e decentralizzate – che siano in grado di affrontare adeguatamente il problema della riservatezza dei dati[29].

Indipendentemente da ciò, i sistemi decentralizzati, come la *blockchain*, hanno attirato crescente attenzione da parte della dottrina, che sta esaminando in maniera attenta come le DLTs potrebbero essere applicate in

---

privacy degli utenti. Infatti, «[w]hile they are capable of preserving the confidentiality of data, decentralized architectures cannot easily protect themselves against the analysis of metadata». *Ibid.*

[24] M. CROSBY, P. PATTANAYAK, S. VERMA, P. KALYANARAMAN, *Blockchain Technology Beyond Bitcoin*, Sutardja Center for Entrepreneurship & Technology, Berkeley University of California, 2015, 13-19. Mentre il bitcoin in sé è molto controverso, la tecnologia blockchain sottostante ha funzionato in modo impeccabile e ha dimostrato di poter trovare un'ampia gamma di applicazioni, sia nel mondo finanziario che in quello non finanziario. Tuttavia, tale tecnologia crea una situazione che, come avrebbe detto Rodotà, rappresenterebbe una realtà caratterizzata da un controllo permanente (ovvero di sempre maggiore ed indiscriminata identificazione ed identificabilità) dei singoli, come parti di un "gregge". Sul punto, si vedano S. RODOTÀ, *Il mondo nella rete: quali i diritti, quali i vincoli*, Roma-Bari, 2014; S. RODOTÀ, *Repertorio di fine secolo*, Roma-Bari, (1992-) 1999; S. RODOTÀ, *Tecnopolitica*, Bari, 1997.

[25] B. MARR, *A Very Brief History of Blockchain Technology Everyone Should Read*, Frobes, 2018. Disponibile al sito https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read. Consultato il 08 giugno 2022.

[26] D. BRADBURY, *The Problem with Bitcoin*, Computer Fraud and Security, 2013, 5-8.

[27] P. DE FILIPPI, *The Interplay, cit.*, 2.

[28] C. TRONCOSO, M. ISAAKIDIS, G. DANEZIS, H. HALPIN, *Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments*, De Gruyter Open, Proceedings on Privacy Enhancing Technologies, Losanna, 2017, 307-308. Sul punto, si afferma come sia possibile, in tal modo, una maggiore *privacy* dell'utente e, allo stesso tempo, un controllo autonomo dell'infrastruttura. In quanto tali, rappresentano una possibile soluzione tecnologica alle richieste delle leggi sulla protezione dei dati, vincolanti dal punto di vista giuridico ma spesso non applicate dal punto di vista tecnologico.

[29] Si consulti, inoltre, in tema di diritto alla riservatezza dei dati R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003; R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.

relazione alla *privacy*[30].

Considerate quanto affermato finora, nelle pagine che seguono sarà analizzata la relazione che intercorre tra *privacy* e DLTs, il loro impatto in termini di vantaggi e svantaggi, e il rapporto tra trasparenza e *privacy* quando viene applicata la tecnologia crittografica.

3. I vantaggi in termini di privacy legati all'utilizzo della blockchain.

Quanto scritto in precedenza è principalmente riferito agli aspetti collegati alla sicurezza e alla privacy. In particolare, quando si fa riferimento a sistemi decentralizzati si fa riferimento a casi in cui non vi è alcuna entità che possa agire come una c.d. *Trusted Computing Base* (TCB) e che, in tale contesto, possa imporre degli standard di sicurezza o una politica di *privacy*[31].

Al fine di meglio comprendere le problematiche collegate alla protezione dei dati personali, è necessario considerare due aspetti rilevanti. *In primis* (i) l'identificazione del soggetto che si occupa della determinazione delle modalità in cui vengono trattati i dati personali e, in secondo luogo, (ii) l'individuazione del soggetto che si occupa di controllare il modo in cui i dati sono conservati e gestiti[32].

La decentralizzazione che caratterizza la *blockchain* non comporta solo più alti livelli di protezione per i dati personali degli utenti ma, al contempo, comporta un maggiore "potere" nelle mani degli stessi, in quanto gestiscono e hanno un completo controllo sulle informazioni che vengono scambiate tra di loro[33].

Infatti, la tecnologia *blockchain*, in questo senso, è stata definita da parte della dottrina come un «decentralized cloud computing system»[34].

In un siffatto scenario, il principale vantaggio che deriva dall'utilizzo di un sistema decentralizzato risiede nel fatto che viene data agli individui / utenti la possibilità di gestire e controllare in prima persona i propri dati.

Inoltre, i dati che vengono condivisi, generati e raccolti dagli stessi individui potrebbero essere resi disponibili e venduti per scopi comuni e, conseguentemente, utilizzabili anche da soggetti terzi, non diversamente da quanto accade con gli *open data* ma, ovviamente, con logiche e meccanismi differenti[35].

---

[30] C. TRONCOSO, M. ISAAKIDIS, G. DANEZIS, H. HALPIN, *Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments*, De Gruyter Open, Proceedings on Privacy Enhancing Technologies, Losanna, 2017, 308. Gli autori, in questo senso, forniscono anche la propria definizione di *distributed ledger technologies* asserendo che con tale concetto si fa riferimento a «[a] distributed system in which multiple authorities control different components and no single authority is fully trusted by all others». *Ibid.*

[31] J. RUSHBY, *A Trusted Computing Base for Embedded Systems*, Computer Science Laboratory, SRI INT'L, 1984, 294-311. Dal punto di vista definitorio, un *Trusted Computing Base* (TCB) si riferisce a tutti i componenti del computer che si combinano per fornire un ambiente sicuro nel sistema stesso per garantire lasicurezza delle sue informazioni.

[32] W. MAXWELL e J. SALMON, *A Guide to Blockchain and Data Protection*, Hogan Lovells, 2017, 10-11.

[33] *Ibid.*

[34] C. BRIDGE, *Blockchain's Next Frontier: Cloud Computing?*, in *Inv. Mark't Bus. Res.*, 2018. Concettualmente, in particolare, «[c]loud storage allows the user to store data and information online. This serves as a backup in case the data is lost and could be used to secure large amounts of data». *Ibid.*

[35] Si veda, sul punto, T. W. BELL, *Copyrights, Privacy, and the Blockchain,* in *Ohio North'n U. L. Rev.*, 2016, 461-466.

In aggiunta, per quel che concerne la struttura, la maggior parte delle architetture decentralizzate a disposizione degli utenti hanno lo scopo specifico di promuovere la *privacy* concentrandosi su almeno uno dei due paradigmi seguenti: riservatezza dei dati e la "sovranità" degli stessi[36].

Così analizzata, la decentralizzazione di cui è caratterizzata la *blockchain* ha il potenziale per ridurre effettivamente le asimmetrie informative che, generalmente, forniscono dei vantaggi agli operatori in sistemi centralizzati[37].

Proprio quest'ultimo aspetto merita di essere approfondito in maniera sostanziale; soprattutto se si considera che, al giorno d'oggi, ogni volta che un utente naviga in rete accetta innumerevoli *cookie* che monitorano le proprie attività *online*, le ricerche effettuate, le preferenze dei singoli individui[38].

La conseguenza di ciò risiede nel fatto che tutte le informazioni vengono profilate senza un adeguato e consapevole consenso[39].

4. Privacy contro trasparenza.

Tuttavia, va sottolineato come permangano, allo stato attuale, molteplici complessità per comprendere appieno il modo in cui *privacy* e trasparenza possano interagire tra essi.

Da un lato, in una società "trasparente", qualsiasi parte interessata può facilmente avere accesso alle informazioni. Ciò implica che la trasparenza sociale comporta la compromissione del diritto alla *privacy*. Di conseguenza, «è ragionevole associare alla crescente trasparenza delle informazioni un decrescente rispetto del diritto alla privacy»[40].

In siffatto scenario, quindi, la trasparenza che le DLTs sono in grado di offrire non è né assoluta né incondizionata. Infatti, le diverse tipologie di *blockchain* possono garantire diversi livelli di trasparenza[41].

In particolare, esistono due tipologie di *blockchain*, ossia vero le c.d. *permissionless* – che non necessitano di un'autorizzazione – e *permissioned* – che, al contrario, necessitano di autorizzazione. Soprattutto con riferimento a quest'ultima tipologia, le transazioni (o, comunque, gli scambi, la "scrittura"

---

[36] P. De Filippi, *The Interplay*, *cit.*, 4. Si veda, sul punto, anche S. Jin Kim, *An Impossible Trinity in Blockchain-based Transactions: Decentralization, Privacy, and Lower Transaction Costs*, Shanghaitech Sem Working Paper Series No. 2020-010, ShanghaiTech University, 2020.

[37] *Ibid.* Sul medesimo punto, si veda per un approfondimento anche A. T. Themelis, *Information and Intermediation, Abuse of Dominance and Internet 'Neutrality': 'Updating'Competition Policy under the Digital Single Market and the Google Investigations (?)*, *EU. J. L. & Tech*, Vol. 4, no 3, 2013.

[38] Per quel che concerne la fruizione di servizi in rete, G. Resta e V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, *Riv. Trim. Dir. Proc. Civ.*, fasc. 2, 2018; S. Rodotà, *Il mondo della rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014.

[39] S. Goldfeder, H. Kalodner, D. Reisman, A. Narayanan, *When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies*, Sciendo, Proceeding on Privacy Enhancing Technologies, Vol. 2018, issue 4, 2018, 189-191. Per una disamina della fattispecie della revoca del consenso, si veda, G. Resta, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*; *Riv. Crit. Dir. Priv.*, 2000.

[40] Sia consentito riferimento a F. Zambardino, *La blockchain nel mercato del lavoro italiano con particolare enfasi sulla questione privacy e il rapporto con il General Data Protection Regulation*, in TSL, 2022, 23-38. Si veda, inoltre, G. R. Mayes, *Privacy and Transparency*, Sacramento State University, Department of Philosophy, 2018, 125-129.

[41] M. Seghesio, *Blockchain and Privacy,* in *Legal Perspective on Blockchain Theory, Outcomes, and Outlooks,* A. Borroni (ed.), Pubblicazioni del Dipartimento di Scienze Politiche Jean Monnet dell'Università degli Studi della Campania Luigi Vanvitelli, ESI, 2019, 138.

delle informazioni) avvengono all'interno di un ecosistema chiuso, in cui tutti i dati registrati rimangono, in un certo modo, riservate e le identità dei partecipanti sono note[42].

Da un punto di vista pratico, i problemi di *privacy* derivanti dal livello di trasparenza della *blockchain* possono essere mitigati «dalla crittografia della comunicazione "end-to-end", la quale richiede chiavi private e pubbliche, anziché utilizzare una chiave unica per la crittografia e la decrittografia»[43].

Il principio afferma che, laddove possibile, le operazioni del protocollo di comunicazione devono essere definite per essere effettuate ai punti finali di un sistema di comunicazione, o il più vicino possibile alla risorsa da controllare[44].

In particolare, crescono le aspettative sociali per quel che concerne la trasparenza e la supervisione degli algoritmi e nel rendere i sistemi decisionali automatizzati responsabili, più trasparenti e governabili, eventualmente dotandoli di nuovi strumenti tecnologici in grado di verificare che le decisioni automatizzate siano conformi a standard chiave di equità giuridica. Garantire la responsabilità attraverso valutazioni d'impatto degli algoritmi (AIA), audit e certificazioni dovrebbe essere parte integrante di tutte le iniziative politiche e legali in questo campo, considerando che la *blockchain* allo stato attuale non è stata ancora compiutamente implementata[45].

5. Prime riflessioni. Quali implicazioni in termini di sovranità statale.

Uno dei problemi principali legati all'utilizzo di una simile tecnologia – così come, in generale, anche per Internet – è rappresentato dalla crescente tensione «fra il bisogno di una rete aperta e autenticamente globale e l'affermazione di diritti di sovranità sul proprio territorio e sui propri cittadini richiede, per risolverla, più della semplice buona volontà»[46].

Il primo punto da considerare è di natura ideologica. Per lungo tempo, l'idea dominante è stata che la *blockchain*, alla stessa stregua dell'IoT, in quanto globale, sia essenzialmente aterritoriale e, di conseguenza, può "esistere" grazie a regole auto-determinate.

---

[42] PARLAMENTO EUROPEO, *What if blockchain offered a way to reconcile privacy with transparency?*, Unione Europea, 2018. Disponibile al sito europa.eu/RegData/etudes. Consultato il 08 giugno 2022.

[43] F. ZAMBARDINO, *La blockchain nel mercato del lavoro italiano*, *cit.*, 25-26. Per un approfondimento del concetto di comunicazione *end-to-end*, si veda L. ZHANG, *End to end architecture and mechanisms for mobile and wireless communications in the Internet*, Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS, Institut National Polytechnique de Toulouse, Université de Toulouse, 2009, 7.

[44] Con riferimento ai rischi, si veda B. GARDELLA TEDESCHI E S. THOBANI, *Innovazione, diritto e tecnologia: temi per il presente e il futuro. Introduzione*, in *Rivista di Diritto dei Media*, 2020, secondo cui i rischi derivanti dall'automatismo, in particolare, sono acuiti dall'invasività delle nuove tecnologie, che consentono un elevato grado di intrusione nella vita privata delle persone. L. ZHANG, *End to end architecture*, *cit.*, 7-8. Il principale vantaggio di sistemi di comunicazione "end-to-end" è rappresentato dal fatto che consente di integrare «efficient and intelligent mechanisms at the end systems and doesn't require the modifications to the intermediate system, which make the de- ployment easier and much more flexible». *Ibid.*

[45] L. ZHANG, *End to end architecture*, *cit.*, 3. Si vedano, per un approfondimento sul tema, D. REISMAN, J. SCHULTZ, K. CRAWFORD, M. WHITTAKER, *Algorithmic Impact Assessment: A Practical Framework for Public Agency Accountability,* AINOW Institute, 2018. Disponibile al sito https://ainowin- stitute.org/aiareport2018.pdf. Consultato il 08 giugno 2022.

[46] V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. RESTA e V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Consumatori e Mercato, Roma, 2016, 14.

Volendo osservare la questione da una prospettiva della sovranità degli Stati, la *blockchain* può essere considerata alla stessa stregua di un protocollo utilizzato al fine di per trasferire pacchetti di dati, utilizzando reti pubbliche (*i.e.* aperte al pubblico). È chiaro che un protocollo di questo tipo ha consistenza giuridica nel settore della proprietà intellettuale e dal punto di vista regolamentare, «ma essendo interamente non materiale esso non può formare oggetto di sovranità più di uno standard di telecomunicazione o di un sistema di misurazione metrico decimale»[47].

In aggiunta, il fatto che le informazioni che vengono trasmesse in un ecosistema di questo tipo siano intangibili e vengano inviati sulla base di una entità non materiale (come il protocollo Internet) non significa necessariamente che la rete sia immateriale. Anzi, piuttosto essa è composta in larga misura da elementi fisici, collocati quasi interamente sul territorio sovrano dello Stato[48].

Tuttavia, è innegabile come l'epoca contemporanea abbia presentato dei casi sempre più frequenti di regimi che operano senza essere necessariamente contenuti all'interno di un sistema incentrato sugli ordinamenti statali, «pur mantenendo per lo più qualche rapporto con esso, oppure ponendosi con esso, in vario modo, addirittura in contrasto»[49].

Tuttavia, da lì ad affermare che in questi casi si possa considerare l'esistenza di un unico ordinamento giuridico "globale" o "universale" sarebbe quantomeno improprio, soprattutto in considerazione del fatto che i diversi sistemi di regole statali e transnazionali interagiscono al fine di dare vita a una regolamentazione anche in relazione alle attività condotte nelle reti digitali[50].

6. Quale rapporto con il General Data Protection Regulation (GDPR).

Nelle pagine precedenti è stato osservato come, per definizione, la *blockchain* è un archivio distribuito; come naturale conseguenza, anche il controllo sui dati personali non può che essere decentralizzato, demandato a

[47] *Ibid.* ancora, l'autore, con riferimento specifico a Internet – ma per analogia il medesimo discorso è applicabile anche alla *blockchain* – afferma come non possa esservi sovranità sul protocollo Internet più di quanta ce ne possa essere sui protocolli utilizzati per i servizi Skype o WhatsApp.

[48] *Ibid.* L'autore ben esemplifica come l'unico caso di comunicazione extra-territoriale non-materiale è «quella di un messaggio proveniente da un satellite ricevibile direttamente dall'utente (ad es. con un telefono mobile satellitare) senza bisogno di una infrastruttura terrestre che lo distribuisca». Sul punto, V. M. MEJIA-KAISER, *Space Law and Unauthorised Cyber Activities*, in K. ZIOLKOWSI (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 349.

[49] C. PONCIBÒ, *Il Diritto Comparato e la Blockchain*, Memorie del Dipartimento di Giurisprudenza dell'Università di Torino, Napoli-Torino, 2020, 226. Del medesimo autore, anche C. PONCIBÒ, *Blockchain and Comparative Law*, in B. CAPPIELLO e G. CARULLO (eds.), *Blockchain, Law and Governance*, 2020,137-156.

[50] *Ibid.* Del medesimo avviso, G. PASCUZZI, *Il diritto dell'era digitale*, V ed., Bologna, 2020; O. POLLICINO, L. LIGUORI, G. BUSIA (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali*, Roma, 2016. Sul punto, uno spunto di riflessione è fornito da G. TEUBNER, *Ordinamenti frammentati e costituzioni sociali*, in *Rivista giuridica degli studenti dell'Università di Macerata*, 2010, 45-57, il quale afferma come sia opportuna, se non anche auspicabile, «una dilatazione semantica del nostro concetto di diritto, in modo tale che esso possa includere anche le norme operanti a prescindere dalle fonti giuridiche dello stato o del diritto internazionale».

tutti i partecipanti della *blockchain*. Tuttavia, una sorta di controllo centralizzato è prevista nel testo del GDPR[51].

Infatti, al fine di perseguire il duplice obiettivo della protezione dei dati e, al contempo, della libera circolazione degli stessi nel mercato interno, l'Unione europea ha optato per un ambizioso quadro di protezione dei dati, il *General Data Protection Regulation* (di seguito, GDPR), sostituendo la Direttiva 95/46/CE[52].

Il GDPR, specificamente, si prefigge come obiettivo cardine quello di garantire «un elevato livello di protezione dei dati personali, ponendo un freno alla frammentazione normativa in materia prodotta dalla diversa attuazione, nei vari Stati membri, della precedente Direttiva»[53].

La strada attraverso la quale il Regolamento si propone di giungere a tale obiettivo si muove lungo due direttrici fondamentali: da una parte, attraverso la "responsabilizzazione" maggiore dei soggetti attivi del trattamento; dall'altra, fornendo agli interessati strumenti specifici tesi ad innalzare il livello di consapevolezza sull'uso dei propri dati[54].

A partire dal 25 maggio 2018, tale Regolamento è divenuto direttamente applicabile in tutti gli Stati membri dell'Unione europea[55].

In particolare, il GDPR, come indicato dalla stessa Commissione Europea, ha lo scopo, tra gli altri, di garantire la certezza e l'armonizzazione del diritto in materia di protezione dei dati personali nonché una maggiore semplificazione delle norme sul medesimo punto.

In tale prospettiva, il Regolamento si pone come una risposta necessaria e propositiva alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di protezione dei dati personalità sempre più sentite dai cittadini dell'UE[56].

---

[51] M. FINK, *Blockchain and Data Protection in the European Union*, in *Eur. Data Prot. L. Rev.*, 2017, 9. Per un approfondimento, si veda anche G. ALPA, *La "proprietà" dei dati personali,* in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, Milano, 2019.

[52] *Ibid.* In particolare, per 'dato personale', nello specifico contesto del GDPR si intende qualunque tipo di informazione che possa ricondurre a uno specifico individuo. Analizzando questa definizione è possibile evincere fin da subito che la questione è piuttosto complessa. Infatti, la *blockchain*, sempre in quanto sistema distribuito, rappresenta uno strumento potenzialmente incontrollabile e, quindi, può non garantire appieno la tutela dei dati personali così come stabilito dal GDPR. R. TEPERDJIAN, *The Puzzle of Squaring Blockchain with the General Data Protection Regulation*, in *Jurimetrics J.*, 2020, 293-294.

[53] A. M. GAMBINO e C. BOMPREZZI, *Blockchain e protezione dei dati personali*, in *Dir. Infor.*, 2019, 620. Ancora in tema di rapporto tra GDPR e tutela dei dati personali G. ALPA, *La "proprietà" dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, N. ZORZI GALGANO (a cura di), Milano, 2019, 17 ss.

[54] *Ibid.* Entrambe le linee d'azione, nello specifico, se complessivamente considerate, producono «come effetto quello di un innalzamento del livello di controllo sui dati, come già auspicato dal Garante europeo della protezione dei dati». *Ibid.* Sul punto, anche A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (Artt. 32-39)*, in G. FINOCCHIARO, (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, 2017, 287 ss.

[55] 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. Disponibile al sito https://eur-lex.europa.eu/legal-content/IT/TXT. Consultato il 08 giugno 2022.

[56] *Ibid.* Si vedano, sul punto, anche S. SATER, *Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows*, Tulane University, 2017, 4-7; C. SALMENSUU, *The General Data Protection Regulation and Blockchains*, University of Helsinki, Tieto, 2018.

Il cuore del GDPR risiede nella protezione dei dati degli utenti. Più specificamente, il regolamento riconosce «(i) il diritto alla portabilità dei dati[57], (ii) il diritto all'oblio[58] (il quale, prima dell'entrata in vigore del regolamento, era riconosciuto solo dalla giurisprudenza), (iii) il diritto di essere informato in un modo trasparente, corretto e dinamico sul trattamento dei dati, (iv) il diritto di essere informati in maniera tempestiva su qualsiasi violazione dei dati personali (*data breach*)»[59].

Il fatto che le trasmissioni siano intangibili non significa che lo Stato non possa, di fatto o di diritto, impedire la circolazione di taluni contenuti, l'accesso a siti stranieri, o l'accesso dall'esterno a siti interni, e in generale non possa legittimamente. Tutti questi interventi evidenziano come gli Stati – o nel caso dell'UE, entità sopra-nazionali – esercitano i loro poteri sulle reti di telecomunicazioni, da aspetti di poco rilievo fino a interventi assai più complessi e profondi. In tale ottica, stabilire come i dati personali raccolti «attraverso le reti di telecomunicazioni debbano e/o possono essere elaborati e a quali condizioni essi possano essere trasferiti in altri paesi costituisce semplicemente l'espressione dell'esercizio di poteri sovrani da parte e secondo uno stato di diritto»[60].

Tenendo presenti le importanti distinzioni tra le varie forme di DLTs e la necessità di un'analisi caso per caso che ne deriva, di seguito il tentativo di fornire una panoramica generale dell'applicazione del GDPR alla *blockchain*, «con focus sulla questione se i dati relativi a una persona fisica archiviati in un registro decentralizzato possano essere qualificati o meno come dati personali ai sensi del diritto europeo»[61].

---

[57] Per un'analisi sul diritto alla portabilità dei dati, si rinvia a L. BIANCHI, *Il diritto alla portabilità dei dati*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Reg. UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003*, Milano, 2019.

[58] Art. 17 del GDPR. Tale disposizione prevede che il titolare dei dati ottenga dal controllore «the erasure of personal data concerning him or her without undue delay». I titolari del trattamento sono obbligati a cancellare i dati personali soggetti a una serie di condizioni, come «(i) that personal data is no longer necessary for the purposes it was collected or otherwise processed; (ii) that the data subject withdraws consent on which the processing is based or where there is no other ground for processing; (iii) that the data subject objects to the processing and that there are no overriding legitimate grounds for processing; that (iv) data has been unlawfully processed; (v) that personal data has to be erased for compliance with national or supranational law to which the controller is subject; or that (vi) personal data has been collected in relation to the offer of an information society service to a child under 16 years of age». M. FINK, *Blockchain and Data Protection*, *cit.*, 23. Per una disamina del concetto giuridico di oblio, si vedano A. PALMIERI e R. PARDOLESI, *Polarità estreme: oblio e archivi digitali*, FORO IT., 2020, parte I, 1570 (nota a Cass., sez. I, 27 marzo 2020, n. 7559); R. PARDOLESI, *Oblio e anonimato storiografico: «usque tandem...»?*, in *Foro It.*, 2019, parte I, 3082 (nota 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*, DIR. INFOR., 2017; R. PARDOLESI, *Diritto all'oblio, cronaca in libertà vigilata e memoria storica a rischio di soppressione*, in *Foro It.*, 2016, parte I, 2734 (nota Cass., sez. I, 24 giugno 2016, n. 13161).

[59] F. ZAMBARDINO, *La blockchain nel mercato del lavoro italiano*, *cit.*, 27. Si veda anche Regolamento (UE) 2016/679, *cit.* Si vedano, sul punto, A. LONGO e R. NATALE, *GDPR, tutto ciò che c'è da sapere per essere in regola*, Agenda Digitale, 2018. Disponibile al sito https://www.agendadigitale.eu. Consultato il 08 giugno 2022. N. BOLDRINI, *Blockchain e GDPR: le sfide (e le opportunità) per la protezione dei dati*, Blockchain4Innovation, 2018. Disponibile al sito https://www.blockchain4innovation.it/sicurezza/blockchain-gdpr/. Consultato il 08 giugno 2022.

[60] V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems*, *cit.*, 10. L'autore afferma come, «il problema […] non è quello di stabilire quale diritto privato debba applicarsi al rapporto giuridico e chi sia il giudice competente. Quel che è in gioco in questi casi, invece, è la regolazione pubblica delle reti, che non può essere risolto attraverso le regole applicabili ai soggetti privati». *Ibid.*

[61] F. ZAMBARDINO, *La blockchain nel mercato del lavoro italiano*, *cit.*, 27-28. Sul medesimo punto, anche M. FINK, *Blockchain and Data Protection*, *cit.*, 9.

Pertanto, proprio in tale ottica, l'analisi dell'interazione tra la *blockchain* e il GDPR trova giustificazione. In particolare, se da un lato sarebbe utile valutare se tale tecnologia possa effettivamente essere utilizzata per facilitare la tutela della *privacy*, dall'altro lato è pur vero che la tecnologia *blockchain* non viola nessuna delle disposizioni del regolamento[62].

In siffatto scenario, l'art. 25 del GDPR, relativo alla *data protection by design* richiede al titolare del trattamento di mettere in atto «misure tecniche e organizzative adeguate […] volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e tutelare i diritti degli interessati»[63].

Pertanto, si può dedurre che si prediligono soluzioni volte a favorire (i) la minimizzazione dei dati contenuti, (ii) la trasparenza, in relazione all'utilizzo dei dati raccolti, nonché (iii) il permesso all'interessato di esercitare un adeguato controllo sui propri dati[64].

Da quanto fin qui emerso, pare che le caratteristiche della *blockchain* possano soddisfare i desiderata del GDPR circa la necessità di una protezione dei dati sin dalla progettazione. Pertanto, è possibile affermare che, a questo proposito, la *blockchain* può essere considerata ideale per la protezione dei dati personali in quanto ha intrinsecamente il compito di «data protection by design»[65].

Per quel che concerne la *compliance* tra Regolamento e *blockchain* è necessario analizzare sia quelli che sono i punti di conflitto che di convergenza; in questo senso, infatti, sebbene il GDPR e la *blockchain* condividano diversi

---

[62] *Ibid*. Secondo le previsioni annunciate all'ultimo *World Economic Forum*, entro il 2025 ben il 10% del PIL mondiale sarà prodotto da attività e servizi che saranno prodotti e distribuiti attraverso le tecnologie blockchain. Uno scenario, questo, che dovrà fare i conti con le normative, prima fra tutte il GDPR, appunto.

[63] Le caratteristiche che la tecnologia adottata dovrebbe avere a tal fine sono meglio specificate al considerando n. 78 del Regolamento, per cui si prevede che le misure «potrebbero consistere nel: ridurre al minimo il trattamento dei dati personali; pseudonimizzare i dati personali il più presto possibile; offrire trasparenza per quanto riguarda le funzioni ed il trattamento di dati personali; consentire all'interessato di controllare il trattamento dei dati; consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza». A. M. Gambino e C. Bomprezzi, *Blockchain e protezione dei dati personali*, *cit.*, 624-625.

[64] . Zambardino, *La blockchain nel mercato del lavoro italiano*, *cit.*, 29. Sottolineano tale elemento positivo, tra gli altri, M. Berberich e M. Steiner, *Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?*, in *Eur. Data Prot. L. Rev.*, 2016, 425 ss.

[65] Su questo punto, si veda C. Lima, *Blockchain-GDPR Privacy by Design. How Decentralized Blockchain Internet will Comply with GDPR Data Privacy*, Blockchain Engineering Council, IEEE Blockchain Standards, 2018, 2-5. Disponibile al sito https://blockchain.ieee.org. Consultato il 08 giugno 2022. Secondo l'autore, considerando che la tecnologia *blockchain* non consente agli utenti di ripercorrere i propri passi ed eliminare o modificare i dati in essa inseriti, è più che mai indispensabile applicare il principio della *privacy by design*.
Quanto appena affermato, in particolare, trova conferma sotto 3 aspetti fondamentali: (i) le *blockchain* sono decentralizzate e distribuite, aspetto che rende molto più difficile che un attacco di *cybercrime* possa andare a buon fine; (ii) le *blockchain* sono pubbliche e trasparenti per l'utente, il che significa che le informazioni sulle transazioni sono pubbliche ma l'identità e i dati personali sono "mascherati" da una chiave pubblica il cui contenuto è noto solo al diretto interessato; (iii) le *blockchain* fanno un ampio ricorso alla crittografia e sfruttano il meccanismo degli incentivi garantendo, almeno a livello teorico, un metodo sicuro per archiviare e gestire le informazioni (compresi, ovviamente, anche i dati personali). Si vedano, per un approfondimento sul punto, B. S. Jiménez-Gómez, *Risks of Blockchain for Data Protection: A European Approach*, in *Santa Clara High Tech. L. J.*, 2020, 281-343; A. Mirchandani, *The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR*, in *Fordham Intell. Prop. Media & Ent. L. J.*, 2019, 1201-1241.

aspetti, va sottolineato che il Regolamento europeo non è stato redatto *ad hoc* per essere compatibile con un sistema decentralizzato[66].

Pertanto, l'estensione efficace ed efficiente delle disposizioni del GDPR alla tecnologia *blockchain* è subordinata alla previa interpretazione di giudici e regolatori[67].

In particolare, se si considera l'applicazione del GDPR su *blockchain* pubbliche e, quindi, *permissionless*. Nei confronti di tale tipologia di *blockchain*, infatti, l'applicazione del Regolamento può rivelarsi di non agevole realizzazione, dato che la semplice idea di un diritto alla cancellazione si pone in netto contrasto tutto ciò che rappresenta la *blockchain*[68].

In questo contesto, infatti, dopo che una chiave pubblica e le transazioni associate sono state identificate, non c'è modo di "cancellare" le informazioni, che fanno parte della *blockchain* e, quindi, di dominio pubblico.

Sono state anche sollevate questioni su come sarà possibile per le *blockchain* aderire al principio di minimizzazione dei dati, dato che i dati vengono continuamente aggiunti alla catena senza possibilità di cancellazione o modifica e le *blockchain* sono in continua crescita[69].

Sul punto, in particolare, uno degli elementi di contrasto maggiormente evidenti con il GDPR risiede nel fatto che la *blockchain* si basa su un sistema di registro distribuito, decentralizzato e immutabile[70].

Questa funzionalità significa che (i) i dati inseriti nella *blockchain* sono pubblici e accessibili da chiunque partecipi alla rete, (ii) non vi è alcuna

---

[66] K. SWAMINATHAN, *Blockchain Versus GDPR and Who Should Adjust Most*, Finextra, 2018. Disponibile al sito https://www.finextra.com/blogposting/16102/blockchain- versus-gdpr-and-who-should-adjust-most. Consultato il 08 giugno 2022. La tematica in questione è, sicuramente, pertinente se si considera che la tecnologia *blockchain*, per sua propria natura, non consentirebbe la cancellazione dei dati. Infatti, «[w]ithout entering the technical specifications, as soon as a data is entered and shared in the network it cannot be deleted without compromising the reliability, security and validity of the Blockchain system itself. The entry of the data is, therefore, an irreversible process». *Ibid.*

[67] M. FINCK, *Blockchains and Data Protection in the European Union*, EDPL, 2018, 21-26.

[68] M. KRITIKOS, *What if blockchain offered a way to reconcile privacy with transparency?,* European Parliament Research Service, Scientific Foresight Unit (STOA), 2018, 2. Disponibile al sito https://www.europarl.europa.eu/RegData/etudes. Consultato il 08 giugno 2022. In merio al diritto alla cancellazione, si approfondisca con A. BERTI SUMAN, *Il diritto alla cancellazione*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Reg. UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003*, Milano, 2019.

[69] *Ibid.* in particolare, «[t]he spirit of data minimization is profoundly at odds with data storage on a DLT». M. FINK, *Blockchain and Data Protection*, *cit.*, 20. Inoltre, il GDPR prevede che i dati personali siano «collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes». Art. 5, comma 1, let. b), del GDPR. Inoltre, un altro aspetto importante evidenziato da tale articolo è che i dati pesrsonali devono essere «lawfully, fairly and transparently processed in regards to the data subject». Il principio di correttezza, in particolare, va ritrovato in tutto il Regolamento, a partire dai diritti dell'interessato e passando per elementi importanti come l'operatore e l'incaricato del trattamento, i trasferimenti di dati verso Stati terzi o organizzazioni internazionali, il ruolo dell'Autorità nazionale, in particolare per quanto riguarda l'applicazione di sanzioni. D. M. SANDRU, *The fairness principle in personal data processing*, in *Law Review*, vol. 10, 2019, 61. Del medesimo autore, si vedano anche, D. M. SANDRU, *Elements regarding the regulation of the consent in the processing of personal data, according to article 6 of Regulation 2016/679*, in *Revista română de dreptul afacerilor*, no. 1, 2018; D. M. SANDRU, *The Impossible Coexistence between Data Protection and Virtual Communities? What's next?*, in *Pandectele române*, no. 1, 2018, 17-25.

[70] M. SEGHESIO, *Blockchain and Privacy*, *cit.*, 144. In questo senso, infatti, il GDPR è stato progettato per essere uno "strumento" indipendente. In particolare, i requisiti principali per la cancellazione e la modifica dei dati sembrano essere in conflitto con il modo in cui funziona la tecnologia *blockchain*. In effetti, «the blockchain is intended to be a permanent and tamper-proof record that lies outside the control of any government authority». *Ibid.*

possibilità di rimuovere i dati che siano stati effettivamente aggiunti[71] e (iii) non esistono limitazioni di alcuna sorta per quanto riguarda i dati che possono essere memorizzati sulla *blockchain*[72].

Pertanto, prima di proseguire oltre nell'analisi, sarebbe necessario capire come la protezione dei dati personali, in generale, possa essere riconciliata con un sistema in cui vengono immagazzinate enormi quantità di dati e, in secondo luogo, come le regole relative al tempo di conservazione dei dati all'interno di un siffatto sistema possano essere valide[73].

Per quel che concerne gli elementi di contrasto, innanzitutto, non va sottovalutato il fatto che, alla luce della considerazione che le informazioni non possano essere modificate o cancellate, qualora la *blockchain* dovesse essere fattivamente utilizzata come una sorta di *database* che tratta i dati personali, in base alla propria struttura, violerebbe il GDPR. In aggiunta, poiché la tecnologia *blockchain* è un sistema decentralizzato, sarebbe impossibile, di diritto, identificare un unico responsabile della protezione dei dati, come espressamente richiesto dal GDPR[74].

Queste, in particolare, così come altre caratteristiche della *blockchain* vanno a scontrarsi con quelli che sono gli elementi che caratterizzano le architetture di gestione centralizzata dei dati, che rappresentano ancora, allo stato attuale, l'unica tipologia di architettura che il regolatore aveva in mente quando è stato redatto il GDPR[75].

Dopotutto, l'intento primario dei legislatori europei, sotto il profilo regolamentare, con il GDPR era quello di fornire un paracadute giuridico per le attività degli attori privati, in particolare le nuove società che operano *online*, i cui modelli di business si basano sulla tecnologia *data-driven*[76].

---

[71] Si veda, per un approfondimento sul punto, M. CONOSCENTI, A. VETRÒ, J. C. DE MARTIN, *Blockchain for the Internet of Things: A Systematic Literature Review*, Nexa Center for Internet & Society DAUIN-Politecnico di Torino, 2016.

[72] K. SWAMINATHAN, *Blockchain Versus GDPR*, *cit.* A tal proposito, va evidenziato che tra i diritti dell'individuo, secondo il regolamento GDPR, ci sono quelli di cancellazione, rettifica e modifica dei dati personali. In un sistema centralizzato l'interessato può esercitare tali diritti rivolgendosi al titolare del trattamento. Ovviamente, tutto ciò è diverso nel caso dei sistemi decentralizzati. La domanda, infatti, è la seguente: come fa il soggetto / utente interessato a esercitare tali diritti in un sistema decentralizzato, in cui idati non sono cancellabili e, inoltre, sono anche pubblici e fruibili da chiunque?M. SEGHESIO, *Blockchain and Privacy*, *cit.*, 145, nota 51.

[73] J. SLABY, *Backups and the GDPR "right to be forgotten": Recommendations*, Acronis, 2018. Disponibile al sito https://www.acronis.com. Consultato il 08 giugno 2022.

[74] S. BRAKEVILLE & B. PEREPA, *Blockchain basics: Introduction to distributed ledgers - Get to know this game-changing technology and how to start using it*, IBM Developer, 2018. Disponibile al sito https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemix-trs/. Consultato il 08 giugno 2022. In particolare, gli autori sottolineano la natura distribuita della *blockchain* affermando che si tratta di un «database that is shared, replicated, and synchronized among the members of a decentralized network. The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network. Participants in the network govern and agree by consensus on the updates to the records in the ledger. No central authority or third-party mediator, such as a financial institution or clearinghouse, is involved. Every record in the distributed ledger has a timestamp and unique cryptographic signature, thus making the ledger an auditable, immutable history of all transactions in the network». *Ibid.*

[75] A. TOWERS, *Blockchain Resolution Passed by EU Parliament but GDPR Could Be Weak Link*, William Fry, 2018. Disponibile al sito https://williamfry.com. Consultato il 08 giugno 2022.

[76] In particolare, l'aspetto della pseudonimizzazione dei dati personali (ossia «data can no longer be attributed to a specific individual without the use of additional information» Art. 4, no. 5, GDPR) è specificamente regolato dal GDPR ed è soggetto alla condizione che le informazioni aggiuntive siano «conservate separatamente» e soggette a misure tecniche e organizzative atte a garantire la non attribuzione a persona identificata o identificabile.

Con riferimento, per converso, ai potenziali punti di convergenza tra il GDPR e la tecnologia *blockchain*, va evidenziato come quest'ultima possa anche essere utilizzata in un modo tale da facilitare la protezione dei dati personali[77].

In particolare, ciò è vero perché questa tecnologia garantisce la scissione dei dati dall'identità individuale e la minimizzazione dei dati (ovvero la condivisione dei soli dati inevitabili).

Lo stesso Regolamento prevede che, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, vi è la possibilità che i dati personali possono essere conservati per periodi più lunghi rispetto a quanto acconsentito dal diretto interessato. Rimane, comunque, chiaro che la definizione stessa di pubblico interesse è quanto mai generica.

Più concretamente, i problemi legati alla *privacy* derivanti dalle caratteristiche proprie della *blockchain* possono essere mitigati dalla crittografia *end-to-end*, richiedendo chiavi private e pubbliche e, contestualmente, trovando alternative valide alla cancellazione dei dati[78].

[77] J. SLABY, *Backups and the GDPR*, *cit.*

[78] Anziché utilizzare un'unica chiave per la crittografia e la decrittografia, quindi, vengono utilizzate chiavi separate (una chiave pubblica e una privata, appunto), in modo tale da consentire agli utenti di inviare la propria chiave pubblica a chiunque, senza preoccuparsi che qualcun altro possa accedere alla propria chiave privata. Con riferimento all'aspetto dell'anonimato, si veda G. RESTA, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in *Dir. Infor.*, 2014, 171.

Iorio C, 'Legal issues concerning the circulation and processing of data in the digital age' (2022) 2 EJPLT, 153-168.
DOI: https://doi.org/10.57230/ejplt222CI

EJPLT
ISSN 2704-8012



Legal issues concerning the circulation and processing of data in the digital age.

CHIARA IORIO
Postdoctoral Research Fellow
Università degli Studi di Macerata

Abstract

This paper focuses on some of the most controversial issues concerning the circulation of personal data. The legal nature of personal data will be framed. Then, the liability regime pursuant to Article 82 GDPR will be examined, with particular reference to data breach committed by an Internet service provider and in the context of a Blockchain.

Il presente contributo si propone di esaminare alcune delle questioni più controverse e attuali in materia di circolazione dei dati personali. Prendendo le mosse dall'inquadramento della natura e delle modalità di circolazione dei dati, sarà indagato il regime di responsabilità di cui all'art. 82 GDPR, con particolare riguardo all'illecito commesso dall'internet service provider, o nell'ambito di una Blockchain.

© The author(s) 2022, 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 processing; liability; internet service provider; blockchain; digital services act; digital market act.

Summary: Introduction. – 1. The nature of personal data between fundamental rights and economic asset. – 2. Data processing liability. – 3. The internet service provider's liability for data processing. – 4. Data processing and Blockchain. – 5. Principles of minimization and data protection by design. – 6. The identification of data controller and data processor. – Conclusions.

Introduction[1].

In the digital age, the centrality of personal data is indisputable. Data have acquired a multifunctional dimension, where the boundary between the public and the private sphere is blurred.[2] Data are not only a personal attribute, but also a means for the State to control their respective owners thanks to the use of technology and, therefore, a tool for exercising power. Consequently, many authors are discussing the rise of a "datacracy",[3] as well as a "datification".[4]

This is the reason why a detailed regulation of the use and circulation of data at a European level has been considered necessary in the recent "Digital Services" package, for protecting online users and stimulating innovation.

This paper aims to examine some of the most controversial legal issues in this area with specific regard to the Italian system. The regime of liability as referred to in Art. 82 GDPR will be analyzed starting from the classification of the nature and the circulation of data with particular focus on the damage caused by an internet service provider, or within a Blockchain.

1. The nature of personal data between fundamental rights and economic asset.

The plurality of regulations which have recently been affecting personal data confirms the centrality that data have assumed in the current technological society and highlights multiple legal issues.

The need for a differentiated disciplinary approach to this matter derives from the ambivalent nature of the personal data, which can be considered an

[1] This article has been written within the "TRUST - digital TuRn in EUrope: Strengthening relational reliance through Technology" Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 101007820. This article reflects only the author's view and the REA is not responsible for any use that may be made of the information it contains.

[2] Some authors have long sustained the opportunity to overcome the dichotomy between public and private: see P Perlingieri, 'L'incidenza dell'interesse pubblico sulla negoziazione privata' [1986] Rass dir civ, 57.

[3] See D De Kerckove, 'Mobile Culture in Singapore: from Democrature to Datacracy', in A Serrano (ed.), Between the Public and the Private in Mobile Communication (Taylor & Francis, 2017) 25; S Ranchordas, 'Citizens as Consumers in the Data Economy' (2018) 14 EuCML, 154.

[4] See S Calzolaio, 'Protezione dei dati personali', Dig. disc. pubbl. (Utet giuridica, 2017) 594.

"asset" and as a "fundamental right" at the same time, depending on the chosen approach.

According to the first point of view (the "mercantilist" one), data can be considered an "asset" with an economic value capable of being exchanged contractually. This theory is based on the observation of the economic reality, in which digital content or digital services are often supplied in a way that the consumer does not pay a price but provides personal data to the trader.[5]

The second approach (the "personalistic" one) refuses to compare data to money, noting that the protection of personal data is included among the fundamental rights by Art. 8 of the EU Charter[6]. According to this perspective, data cannot circulate as wealth, but can be seen as an attribute of the person and the foundation of a new conception of the right to "privacy".[7] Privacy indeed can no longer be considered in the "negative" meaning of the "confidentiality" claimed by the individual concerning invasions of the private sphere (especially towards the press)[8] but is to be seen in the (positive) sense of the right of each person to exercise effective control over the data entered in the network.[9]

The tension between the two opposing views about the nature of the data emerges in the legislative process of Directive (EU) 770/2019 concerning contracts for the supply of digital content and digital services.[10] Indeed, in the text of the proposal[11], the conferral of access to personal data by the consumer was expressly qualified as "counter-performance other than money".

---

[5] V Ricciuto, 'Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali (2020) 3 Riv dir civ, 642; see also A De Franceschi, *La circolazione dei dati personali tra privacy e contratto* (Esi, 2017) 10. With specific reference to access to social network by means of consent to data processing, see C Perlingieri, *Profili civilistici dei social networks* (Esi, 2014) 80. See also K E Davis & F Marotta-Wurgler, 'Contracting for Personal Data' (2019) 94 N.Y U. Law Rev, 662.S Spiekermann and others, 'The Challengesof Personal Data Markets and Privacy' (2015) 25 Electron Markets, 25.

[6] See G Gonzlez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 55; J Dai, 'On the Right to the Protection of Personal Data as a Constitutional Right' (2021) 20 J. HUM. Rts., 851.

[7] On the evolution of the concept of privacy see V Cuffaro, 'Il diritto europeo sul trattamento dei dati personali', (2018) 3 Contr impr,1098; G Visintini, 'Dal diritto alla riservatezza alla protezione dei dati personali' [2019] Dir inf e informatica, 1.

[8] G Giampiccolo, 'La tutela giuridica della persona umana e il c.d. diritto alla riservatezza' [1958] Riv trim dir e proc civ, 458; G Pugliese, 'Il diritto alla riservatezza nel quadro dei diritti della personalità' [1963] Riv dir civ, 605; P Rescigno, 'Il diritto all'intimità della vita privata', in *Studi in onore di F. Santoro-Passarelli* (Jovene, 1972) 121.

[9] S Rodotà, 'Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali' [1997] Riv crit dir priv, 583; G Finocchiaro, 'Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali', in G Finocchiaro (ed), *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, (Zanichelli, 2019) 5.

[10] For a detailed analysis of the Directive, see C Camardi, 'Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali' [2019] Giust civ, 499; J M Carvalho, 'Sale of Goods and Supply of Digital Content and Digital Services - Overview of Directives 2019/770 and 2019/771' (2019) 5 EuCML, 194; K Sein, G Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services - Scope of Application and Trader's Obligation to Supply' (2019) 15 ERCL, 257; B Gsell, R Araldi, 'Time Limits of Remedies for Hidden Defects under under Directive (EU) 2019/770 on Contracts for the Supply of Digital Content and Digital Services and Directive (EU) 2019/771 on Contracts for the Sale of Goods' (2020) 12 Cuadernos de Derecho Transnacional, 475; C Cauffman, 'New EU Rules on Business-to-Consumer and Platform-to-Business Relationships' (2019) 26 Maastricht J Eur & Comp L, 469.

[11] See G Spindler, 'Contracts For the Supply of Digital Content - Scope of Application and Basic Approach - Proposal of the Commission for a Directive on Contracts for the Supply of Digital Content', (2016) 12 ERCL, 183; F Zoll, 'The remedies in the Proposals of the Only Sales Directive and the Directive on the Supply of Digital Content' (2016) 5 J Eur Consumer & Mkt L, 250.

The final version of the Directive rejects the equivalence between personal data and goods. In compliance with the comments given by the European Data Protection Supervisor[12], the Directive formally excludes that access to digital content through the transfer of personal data can be qualified as a bilateral contract.[13] Art. 3 distinguishes between case (a) where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price; and case (b) where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader.

Although the Directive shall apply to both cases, hypothesis (a) is expressly qualified as a "contract", while hypothesis (b) is generally referred to as a case "where" the supply takes place.

And yet, despite the wording of the provision, the two hypotheses are not differently regulated, from a substantial point of view. The directive extends, indeed, the application of remedies for non-conformity also to case (b).

In the same sense, should be seen also Directive (EU) 2161/2019[14], whose recital No. 31 highlights the "similarities" and the "interchangeability" of paid digital services and digital services provided in exchange for personal data, and therefore states that they should be subject to the same rules under that Directive.

In this regard, it is also worth mentioning the Art. 3-bis, Dir. (EU) 2011/83[15], which provides for the application of the Directive also to cases where the trader supplies digital services and the consumer gives access to its data.

These regulatory solutions comply with the legal theory and are consistent with the effective dynamics of the traffics in the net.

It is certainly undeniable that the protection of personal data is a component of the rights of the individual. However, it cannot be excluded that the consent to their processing as a condition for the use of digital services gives rise to a negotiation involving consideration.

More specifically, as observed by some authors, in such cases the processing of data becomes an element of a complex contractual situation, in which there is a dual expression of consent: consent to the use of the digital service in the absence of payment of a price in money, on the one hand, and consent to access to data, on the other.

---

[12] EDPS, Opinion 4/2017, in www. edps.europa.eu stated that '[F]undamental rights, such as the right to the protection of personal data, cannot be reduced to mere consumer interests and personal data cannot be considered a mere commodity'.

[13] According to recital n. 24 '[T]he protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity'.

[14] European Parliament and Council Directive 2019/2161/EU of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328/7.

[15] European Parliament and Council Directive 2011/83/EU of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJL 304/64.

The two acts of "consent" [16] cannot be studied independently, being functionally connected. In other words, the consumer's consent to processing is justified precisely in relation to the supply of the service by the trader. In this way, consent to data processing can be seen as the consideration of the negotiation. [17] Therefore, a bilateral contract is configured in the case examined.[18] It should be clarified that this contract cannot be qualified as a "purchase" agreement.[19] Given the peculiarity of personal data (which pertains to a fundamental right), they cannot be definitively ceded to other parties. In this direction, we should remind that Art. 7, par. 3, GDPR states that the data subject has at "any time" the right to withdraw his consent.

We could conclude that the consumer cannot cede the data, but he can transfer the right of economic exploitation of the data, through a negotiation scheme that, according to some authors, could be qualified in terms of a "license".[20]

Moreover, it should be noted that the recognition of the commercial nature of data entails more effective protection for the data subject.

Let us think of the applicable remedies.

The personalist approach should lead to the application of the sole remedies provided for the rights of the personality and in the GDPR, while the discipline regarding patrimonial phenomena (such as the remedies provided for in the matter of unfair commercial practices) could not be applicable.

---

[16] Legal nature of 'consent' is highly debated by the scholars: some authors consider it as a negotial consenus: V Cuffaro, 'A proposito del ruolo del consenso', in V Cuffaro and others (eds), *Trattamento dei dati e tutela della persona* (Giuffré, 1999) 121; G Oppo, '«Trattamento» dei dati personali e consenso dell'interessato", in G Oppo, *Scritti giuridici*, VI, *Principi e problemi del diritto privato* (CEDAM, 2000)113. Other scholars consider it as a legal act in the strict sense: S Patti, 'Il consenso dell'interessato al trattamento dei dati personali' [1999] Riv Dir Civ, 455 qualifies ita as a form of "justification". F Bravo, 'Lo «scambio di dati personali» nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto' [2019] Contr impr, 34 qualifies it as merely authorizing act; R Messinetti, 'Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali' [1998] Riv crit Dir priv, 35, has the same opinion. See also C. Solinas, 'Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette' [2021] Giur it, 320.

[17] See V Ricciuto, 'Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali', (2020), 652: "[T]he economic function, in short, is to realize, concretely and beyond the schemes used, an exchange, even where the contractual scheme is apparently free". Differently, for C Camardi, 'Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali' [2019], 550, the contractual operation can be seen as a supply of digital goods/services with a 'free structure', which is linked to an act of transfer of personal data by the consumer for non-commercial purposes that cannot be considered as consideration.
In case law, see the decision of the Italian Consiglio di Stato of 29 March 2021, n. 2631, GiustizaCivile.com, with comment by V Ricciuto and C Solinas, 'Supply of digital services and provision of personal data: firm points and ambiguities on the equivalence of the contract'. The decision rules that the services of the social network Facebook are '[P]romised as free, but, evidently, are not free, ending up representing the «consideration» of the provision of personal data of the individual user for commercial purposes'.

[18] See also C Perlingieri, *Profili civilistici dei social networks* (Esi, 2014), 88. The author states that "[T]he disposition of privacy and personal data is in function of the use of the platform, so that by virtue of the synallagma, the user has both the right to use the platform - and the social is obliged to allow its use - as the social can collect and exploit personal data. Also A De Franceschi, *La circolazione dei dati personali tra privacy e contratto* (Esi, 2017), 75 affirms the nature of a contract for consideration.

[19] But Tar Lazio of 10 January 2020, n. 260, Giur it, 2021, 320, qualified it as a purchase agreement.

[20] V Zeno-Zencovich, 'Do "Data Markets" Exist?' [2019], 26. See also on this matter V Ricciuto, 'Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali' (2020), 656: '[T]he rights which are transmitted or acquired by the data controller may be of different types, non-exclusive enjoyment, economic exploitation, transformation in order to create additional data through, for example, profiling, etc'.

Otherwise, the full application of the consumer discipline cannot be excluded when we assume that personal data can circulate for commercial purposes.

Thus, in the (very frequent) cases where the trader does not inform the consumer of the profiling of his data for commercial purposes, an unfair commercial practice (according to Articles 20, 21, and 22 of the Italian Consumer Code) or an aggressive practice (according to Article 20, 24 and 25 of the Italian Consumer Code) could be configured.

In this way, there is the overcoming of the logic of the "watertight compartments" of protection. At the same time, a new conception of "multi-level protection"[21] is embraced, which is able to ensure effective protection of the rights of an individual, in the event that a very personal right is exploited for commercial purposes, even independently of the will of the interested party.

2. Data processing liability.

Another controversial issue concerns the reconstruction of the liability regime deriving from the processing of data, currently regulated by Art. 82 GDPR.

As well known, this subject was previously regulated in Italy by Art. 15 of the Legislative Decree 196/2003 (the so-called "Privacy Code"), which stated that "Any person causing harm to others as a result of treatment of personal data is liable to compensation under Article 2050 of the Civil Code".

The reference to Art. 2050 has been variously interpreted by scholars.

According to most authors, it was a classic hypothesis of non-contractual liability, according to the general regime as provided for in Article 2043 of the Civil Code.[22] Other lawyers qualified it as a special form of tortious liability.[23] According to the minority of the scholars, Article 15 provided for a hypothesis of contractual liability, since the reference to Art. 2050 had to be interpreted as referring only to the probative rule established therein.[24]

---

[21] Consiglio di Stato of 29 March 2021, n. 2631 speaks about a "multi-level protection" and rejects the argument that the only GDPR legislation should be considered applicable - because of its alleged specialty - with the effect of excluding the applicability of any other legal framework. Without prejudice to the centrality of the GDPR, the Consiglio di Stato excludes the possibility that, in this matter, "protective watertight compartments" may be identified. It follows that '[W]hen the processing involves conduct and situations governed by other legal sources to protect other values and interests (as important as the protection of data relating to the natural person), the legal system cannot allow any disapplication of other sector disciplines (...) to reduce the safeguards granted to natural person'.

[22] According to this interpretation, in particular, the source of liability would still be unfair damage (where the meritorious subjective situation of the injured person would have to be assessed on a case-by-case basis) caused by intentional or negligent conduct. See F Caringella, 'La tutela aquiliana della privacy nel codice per la protezione dei dati personali (d. lgs. n. 196/2003)' in *Studi di diritto civile. III. Obbligazioni e responsabilità* (Giuffré, 2005) 715.

[23] V Roppo, 'La responsabilità civile per trattamento di dati personali' [1997] Danno resp, 663.

[24] F D Busnelli, 'Itinerari europei nella «terra di nessuno tra contratto e fatto illecito»: la responsabilità da informazioni inesatte' [1991] Contr impr, 539; C Castronovo, 'Situazioni soggettive e tutela nella legge sul trattamento dei dati personali' [1998] Eur dir priv, 656; C Scognamiglio, 'Buona fede e responsabilità civile' [2001] Eur dir priv, 357; E Pellecchia, 'La responsabilità civile per trattamento dei dati personali' [2006] Resp civ prev, 221.

The question arises again in light of the text of the GDPR, which is the result of the mediation between the different legal cultures of the Member States.[25] Article 82 of GDPR establishes that "any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered"[26].

Although the wording of the provision may call to mind Art. 2043 of our Civil Code, a more careful analysis reveals the inadequacy of a unitary reconstruction of the provided liability.[27]

First of all, we can distinguish between the regime of liability of the controller and that of the processor. According to the second paragraph of Art. 82, indeed, any controller involved in processing shall be liable "for the damage caused by processing which infringes this Regulation". The processor shall be liable for the damage caused by processing (a) where "it has not complied with obligations of this Regulation specifically directed to processors" or (b) where "it has acted outside or contrary to lawful instructions of the controller".

We can assume that the liability of the data controller can be qualified as having a contractual nature, while the liability of the data processor has a contractual nature only in case (a).

In order to understand this assumption, it is essential to clarify the radical change of structure of the GDPR, if compared to the "old" Directive (CE) 95/46.[28]

The most recent regulation, indeed, provides for a series of detailed obligations in respect of data controller and data processor[29], aimed at ensuring the lawfulness of the processing and, therefore, at protecting the rights of the data subject (according to art. 5 GDPR). In this way, the principle of "accountability" is implemented, which pursues an "ex-ante" approach, in order to prevent the risk of damage to the data subject.[30]

---

[25] F Bravo, 'Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali', in N Zorzi Galgano (ed) *Persona e mercato dei dati. Riflessioni sul GDPR* (Wolters Kluver, 2019) 393, stresses that, in the force of existing regulations, domestic legal categories must give way to European ones, in the dynamics of 'droit pluriel'.

[26] On the nature of the liability provided for in Art. 82 GDPR see: A B Menezes Cordeiro, 'Civil liability for processing of personal data in GDPR' [2019] Eur. Data prot. Law Review, 492. About liability for data breach, see also J P Kesan & C M Hayes, 'Liability for Data Injuries' (2019) 1 U Ill L Rev, 295; K Nekit, D Kolodin & V Fedorov, 'Personal Data Protection and Liability for Damage in the Field of the Internet of Things' (2020) 10 Juridical Trib, 80.

[27] Among the first interpretations of art. 82 GDPR, it is widespread, however, the qualification of liability arising from data processing as non-contractual. *Ex multis*, see M Gambini, *Principio di responsabilità e tutela aquiliana dei dati personali* (Esi, 2018) 124; E Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale* (Giuffré, 2019) 49.

[28] On the directive, see C M Bianca and F D Busnelli (eds) *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, (Cedam, 2009); V Cuffaro and others (eds), *Il Codice del trattamento dei dati personali* (Giappichelli, 2007); See also S Sica and P Stanzione (eds), *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196* (Zanichelli, 2005).

[29] Consider, *ex multis*, the obligations relating to the adoption of security measures, referred to in art. 24, 25 and 32; to the obligations deriving from the application of the rights of the interested party, referred to in art. 12-22; the provisions relating to informed consent, referred to in art. 6, par. 1 lett. a) and 9, par. 1, lett. b).

[30] See M Renna, 'Sicurezza e gestione del rischio nel trattamento dei dati personali' [2020] Resp civ prev, 1343.

Since the data controller and processor are burdened with heavy obligations to fulfill, we can conclude that a contractual relationship between them and the data subject arises.[31]

It follows that, where, as a result of the infringement of the Regulation (Art. 82), the data subject suffers damage, a contractual liability according to Art. 1218 C.C. will be configured.

Such a solution seems easy to be argued if the subjects are already part of a contractual relationship where the treatment is necessary "for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (Art. 6, paragraph 1, lett. b).

We could reach the same conclusion in cases where the data subject gives specific consent to the processing of data, or in other cases where Art. 6 acknowledges the existence of a "legitimate legal basis" for processing. In fact, the set of information (Art. 12, 13, 14) and security (Art. 32) obligations that are imposed on the data controller (and, in some cases, also on the data processor) exclude that the data controller could be considered just as a "passer-by"[32], i.e. a "quivis de populo" which is only burdened with a generic duty of "neminem laedere".

The applicability of Art. 2043 c.c., indeed, requires that the relationship between the damaging party and the damaged one is created when the damage occurs. Differently, in the case of data processing, we can notice the existence of obligations for the data controller, which are pre-existing with respect to the damage.

We can conclude that GDPR codifies "ex lege" obligations to be included in the "variae causarum figurae" referred to in Art. 1173 c.c.. It means that, in case of their infringement, a classic hypothesis of liability deriving from a breach of an existing obligation is configured.

Therefore, a non-contractual liability could be configured just in two residual cases: a) where the processor "has acted outside or contrary to lawful instructions of the controller", as , in such a case, there is no legal relationship between the data processor and the data subject;[33] b) where the processing is carried out by a person who cannot be qualified as data controller or processor,[34] or outside the existence of a legitimate basis, according to Art. 6 GDPR.

On a disciplinary level, Art. 82 exempts the controller and the processor from liability if it proves "that it is not in any way responsible for the event giving rise to the damage".

---

[31] Cfr. F Piraino, 'Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato' [2017] Nuove leggi civ comm, 369; Similar is the opinion of F Zecchin, ' Molteplicità delle fonti e tutela dei diritti. Il danno non patrimoniale nella lesione della proprietà e dei dati personali' [2022] Eur dir priv, 517.

[32] The theorizing of non-contractual liability as the liability of the "passerby" is due to Carlo Castronovo. See C Castronovo, *Responsabilità civile* (Giuffré, 2018), 551.

[33] The data processor indeed, is subject to liability (pursuant to the second paragraph of art. 82 GDPR) in the event that "it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. See R Bravo, 'Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali' (Wolters Kluver, 2019), 383.

[34] This qualification, in fact, triggers the set of obligations of conduct that leads to the affirmation of the existence of a mandatory relationship.

This provision recalls the wording of Art. 1218 Civil Code and implies a presumption of the existence of the causal link. Once the existence of the damage has been demonstrated and the breach has been alleged, a reversal of the burden of proof is triggered.

Finally, it should be pointed out that the abovementioned obligations of conduct laid down in the Regulation are purely procedural in nature[35] and do not, therefore, confer immediate utility on the data subject. It follows that the award of damages presupposes, in any event, the proof of a "material or non-material" damage suffered by the damaged party.

In the case, however, in which a non-contractual liability is configurable, compensation is subject to proof of the injustice of the damage, given that, under the general theory of tortious liability, we have to exclude the hypothesis of "in re ipsa" injustice.[36]

3. The internet service provider's liability for data processing.

When unlawful processing of data takes place in the context of the supply of an information society service even more issues arise.

The GDPR (Art. 2, paragraph 4) expressly does not affect the application of Directive 2000/31/EC, with particular regard to the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. Therefore, there is a need for coordination between the two disciplines.

As well known, the so-called "e-commerce" Directive set a special regime of liability for internet providers, intending to encourage the expansion of the digital market.[37]

As a result, a set of exemptions of liability has been laid down, depending on the activity carried out by the provider.[38] Moreover, there are not obligations of active conduct for the provider.[39]

---

[35] See F Piraino, 'Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato' [2017] 390.

[36] Under the old Privacy Code, the case law frequently sated the '[T]he non-pecuniary damage [...] does not escape verification of the 'severity of the injury' and the 'seriousness of the damage'. Cass. 8th February 2017 n. 3311, in *DeJure*; Cass. 5th September 2014 n. 18812; Cass. 15th July 2014 n. 16133.

[37] It should be clarified that the very recent Digital Services Act [European Parliament and Council Regulation 2022/2065/EU of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC [2022] OJL 277/1], which will apply from 17 February 2024, regulates the liability of providers in a way which is substantially similar to the old e-commerce Directive. DSA maintains the prevision of the causes of exemption of liability, distinguishing between service providers of 'mere conduit' (art. 4), 'caching' (art. 5) and 'hosting' (art. 6). Substantial innovations consist in the introduction (Art 6) of a cause of exclusion of the benefit of the exemption of responsibility; in the forecast (Art 7) of the 'good samaritan' clause; in the introduction of specific obligations of action for the provider in the case of illicit content (Art 9 and 10).

[38] Intermediaries who are limited to an activity of 'mere conduit' (Art. 12 dir; Art. 14 D. Lgs. 70/2003) and 'caching' are exempt from liability, provided that they do not modify the information transmitted and, if informed of an irregularity on the platform, act promptly to remove the stored information, or to disable access (Art 13; Art 15 D. lgs 70/2003). Even permanent storage ('hosting') does not entail the liability of the operator, provided that the latter is not actually aware that the activity or information is illegal and that, as soon as he is aware of such facts, act immediately to remove the information or to disable access (art. 14 Directive; art. 16 D. Lgs. 70/2003).

[39] Subjection of providers to obligations of monitoring the information transmitted is also excluded; also active search of facts or circumstances indicative of illegal conduct is excluded (Art. 15 Directive; Art. 17 D.lgs. 70/03513). Only where the provider becomes aware of alleged unlawful activities an obligation to inform without delay the judicial or administrative authority acting as a vigilance (Art. 17, paragraph 2, lett

However, this regime turned out to be inadequate in the face of the massive development of digital relations.[40]

This is why the Italian Court of Cassation has tended to bring the provider's liability into line with the ordinary system. A distinction between "passive" and "active" providers has been drafted by the case law.[41]

"Passive" provider benefits from the integral application of the exemption clauses, while the "active" is liable according to the general regime according to Art. 2043 Civil Code.[42]

This distinction corresponds to that of illegal conduct which, as is well known, "may consist of an action or an omission, in the latter case by tort or omission in the proper sense, in the absence of the event, or, where an event results, in an improper sense; where the event is the unlawful act of another person, the offense of commission is constituted by omission in competition with the principal author".[43]

The figure of the active provider must, then, generally be traced back to the case of the illegal active conduct of the competition.

---

a) arises. The third paragraph of that Article states that 'The provider shall be legally responsible for the content of such services if, at the request of the supervisory judicial or administrative authority, he has not acted promptly to prevent access to that content, or if, having become aware of the unlawful or harmful character of a third of the content of a service to which it provides access, it has not informed the competent authority'.

[40] F Bocchini, 'Responsabilità dell'hosting provider, la responsabilità di Facebook per la mancata rimozione di contenuti illeciti' [2017] Giur it, 629 defines Dir. 2000/31/EC as '[T]he directive of irresponsibility'.

[41] Judgment of 23 March 2017, Google vs Louis Vuitton, C-236/08, ECLI:EU:C:2010:159 ruled that the special regime pursuant to Art. 14 dir. Is only applicable where the role played by the operator is 'neutral'. To this end, it is required that the conduct is purely technical, automatic and passive, which implies lack of knowledge or control of the stored content. See also Judgment of 12nd July 2011, L'Oreal c. e-Bay, C-324/09, EU:C:2010:159

The distinction between 'passive' and 'active' hosting providers has been immediately transposed by Italian jurisprudence, which applies just to the 'passive provider the exemption regime referred to in Art. 16, while submitting to the ordinary judgment of Art. 2043 the 'active' provider who 'carries out an activity that is outside a service of purely technical, automatic and passive order, and instead puts in place an active conduct, competing with others in the commission of the offence'. See Cass of 19March 2019, n. 7708, in *Foro it.*, 2019, I, c. 2045.

See F Di Ciommo, 'Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei provider di Internet nell'incerta giurisprudenza europea' (2019) I Foro it., 2078; G Cassano, 'La Cassazione civile si pronuncia sulla responsabilità dell'internet service provider' [2019] Dir ind, 35; F Bocchini, 'La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP' [2019] Giur it, 2604; M L Gambini, 'La responsabilità dell'internet service provider approda in Cassazione' [2020] Corr giur, 177.

The case-law has identified a number of symptomatic factors which may indicate the 'active' nature of the service provider. Consider, by way of example, activities of 'filter, selection, indexing, organization, cataloguing, aggregation, evaluation, use, modification, extraction or promotion of content, carried out through an entrepreneurial management of the service, as well as the adoption of a technique of behavioural evaluation of users to increase their loyalty: conduct that have, in essence, the effect of completing and enriching in a non-passive way the enjoyment of the contents by indeterminate users'. In such cases, therefore, the affirmation of the liability of the intermediary is subject to the assessment of the constitutive elements of the non-contractual liability referred to in Art. 2043 c.c. See Trib. Roma of 2 October 2019, DeJure.

[42] The system of immunity therefore ceases to apply in cases where the provider plays an active role, giving it knowledge or control of the said contents. It is therefore essential that the 'unlawful nature of the activity or information should result from an actual knowledge or be manifest, that is to say that it must be concretely demonstrated or easily identifiable' (Judgment of 22 June 2021, *Cyando*, C-682/18 Press and Information YouTube, C-683/18 Youtube and Cyando, C-682/18 - C-683/18, EU:C:2021:50.

[43] Cass., 19th March 2019, n. 77008.

When the damage derives from the processing of data, the internet provider could be generally considered as the data controller, or as the data processor.[44] As far as the liability regime is concerned, we must make a distinction. The "passive" provider can go exempt from liability (according to Article 14 et seq.), while the "active" provider will be subject to the application of the common rules according to Art. 1218 or Art. 2043 c.c. (depending on the relevant liability regime, as already noted in the previous paragraph).

Once the liability of the service provider has been established, special attention should be paid to the quantification of damages.

The identification of the parameters for the liquidation requires the interpreter to take note of the now acclaimed "polyfunctionality" of civil liability, which, in order to guarantee effective protection to the injured party, pursues not only a compensatory function but also a sanctioning and deterrent purpose.

To this end, it is essential to consider the specificity of the offense committed via the Internet.

The absence of spatial boundaries of the net,[45] on the one hand, and the speed of propagation of the offense, on the other, determine the opportunity to set effective remedies, able to ensure full protection for the damaged interests, and, at the same time, to act as a deterrent in a general-preventive perspective.

On this point, it should be remembered that, under the "old" Privacy Code, the case law tended to award compensation for the unlawful processing of data based on a presumptive mechanism which reconnected the existence of damage to the particular wrongfulness of the conduct, or to the type of interest affected.

We can consider the (widely known) case[46] where the violation of the privacy of a famous footballer was compensated with a large number of damages (two million by the Tribunal, reduced to 70,000 Euros by the Court of Appeal).[47] This case is relevant because, even though there was no proof of actual damage, the compensation was assessed by the Court on the basis that the conduct was "particularly reprehensible for their sneaky and unfair character" and aimed "at the distorted use of the telephone for the achievement of illicit purposes".

---

[44] The investigation about the qualification of the provider must necessarily be carried out on a case-by-case basis. For example, the provider of the 'web hosting' service is 'responsible for processing' on behalf of the website operator, which is 'data controller'. The 'cloud provider' - according to a recent opinion of the Slovenian Data Protection Authority (IP - 0612-23/2019/19) - qualifies as joint data controller together with the customer, and not as a mere processor. As for social networks, the EDPB has issued guidelines (n. 8/2020), in which it is noted that the advertiser and the social media provider operate jointly in the case of targeted display advertising and must, consequently, qualify as joint processors. With regard to the relationship between social networks and the operator of a page administered by a different entity, the Court of Justice (Judgment of 5 June 2018, C-210/16, EU:C:2018:388) ruled that the administrators of 'Fanpage' on Facebook should be considered 'joint controllers' together with Facebook itself, in relation to the processing carried out through the use of such social pages.

[45] See N Irti, *Norma e luoghi. Problemi di geo-diritto* (Ed. Laterza, 2006) 5; N Irti, *L'ordine giuridico del mercato* (Ed. Laterza, 2009) 150.

[46] Trib Milano of 3 September 2012, n. 9749, Danno resp (2013), 51.

[47] App Milano of 22 July 2015, *Danno resp* (2015), 1047 states that "there is no doubt that the conduct of which the companies are responsible for appears to be particularly reprehensible because of their sneaky and unfair nature'.

Similarly, the Italian Court of Cassation considered awarding non-pecuniary damage as a result of the mere "violation of the rules of correctness and lawfulness, which are aimed at balancing the freedom of those who process data with the preservation of the sphere of the damaged party".[48]

As a result, damages are aimed to sanction the damaging party. In fact, the constitutional status of the interests damaged in the case of the processing of personal data justifies the assessment of damages even "in the absence of any evidence of a concrete alteration of the domestic customs" of the injured party, in order "to ensure the punitive value which is also proper to the compensation of the non-pecuniary damage from injury to fundamental rights".[49]

Moreover, in certain rulings on the liability of active providers, case law has assessed damages based on the degree of the wrongfulness of the operator's conduct. We can consider a case concerning the infringement of copyright on the internet. The Court of Rome decided to quantify the amount of compensation based on the "conduct held by the counterfeiter, the more or less sudden reaction in the removal of the materials illicitly transmitted and therefore the gravity and duration of the omissive conduct perpetrated to the detriment of the damaged party".[50]

The degree of the wrongfulness of the conduct and the peculiarity of the injured interest (eligible to be compensated "in re ipsa") are, hence, the parameters of the liquidation.

Therefore we can conclude that this field constitutes a further emergence point of the "polyfunctionality"[51] of non-contractual liability, which can provide adequate protection for the personality rights of network users and can act as an impulse for the accountability of internet providers.

4. Data processing and Blockchain.

Even denser are the questions that arise when unlawful data processing takes place within a Blockchain.

---

[48] Cass of 4 June 2016, Giur it (2019), 41, with reference to an unlawful data processing carried out by the Customs Agency, responsible for having communicated sensitive data relating to the judicial affairs of an employee through an ordinary protocol open to all. It ruled that Art 15 raised the presumption that the non-pecuniary damage is to be considered 'in re ipsa' unless the person causing damage proves that no loss have been suffered.

[49] Trib. Catania of 31 January 2018, n. 466 about the infringement of the constitutionally guaranteed right to the protection of one's domicile.

[50] Trib. Roma of 10 January 2019, *Dir internet* (2019), 140.

[51] C Salvi, 'La responsabilità civile', in G Iudica and P Zatti (eds) *Tratt. dir. privato* Iudica-Zatti (Giuffré, 2019) 11; G Alpa, *La responsabilità civile. Parte generale* (Utet giuridica, 2010) 159; P Trimarchi, *La responsabilità civile: atti illeciti, rischio, danno* (Giuffré, 2019) 283; A Di Majo, 'Principio di legalità e di proporzionalità nel risarcimento con funzione punitiva' [2017] Corr giur, 1042; P G Monateri, 'Le Sezioni Unite e le funzioni della responsabilità civile' [2017] Danno resp, 419; G Ponzanelli, 'Polifunzionalità della responsabilità civile tra diritto internazionale privato e diritto privato' [2017] Danno resp, 435; C Scognamiglio, 'Le Sezioni Unite ed i danni punitivi tra legge e giudizio' [2017] Resp civ prev, 1109; P Perlingieri, 'Le funzioni della responsabilità civile' [2004] Rass dir civ, 115; P Perlingieri, 'La responsabilità civile tra indennizzo e risarcimento' [2004] Rass dir civ, 1063; P Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, IV, *Attività e responsabilità* (Esi, 2020) 406.

In this case, indeed, the issues concern the compliance between the discipline referred to in Reg. 679/2016 and the architecture of the distributed Ledger.[52]

It should be noted that, despite the intent of its creators, the Blockchain does not constitute a system independent of the application of the rules established by the legal system.[53]

Therefore, the Blockchain needs to be framed and regulated according to the traditional legal categories.

In this context, the GDPR is abstractly applicable concerning the processing of data recorded in the ledger. Despite being encrypted, the information on the blockchain is not technically anonymous,[54] but it is pseudonym.[55]

However, it is hard to reconcile the decentralized system of the Distributed Ledger with the centralized structure of GDPR.

5. Principles of minimization and data processing by design.

The structure of the Blockchain seems hardly consistent with some of the cornerstones on which the implementation of the principle of accountability in Reg. 679/2016 is based, and which are essential for ensuring the safety of data processing.

First of all, we can consider the principle of "minimisation", according to Art. 5, paragraph 1, lett. c), which requires data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

This requirement contrasts with the distributed nature of the Blockchain, where data are replicated on each server. The same issue can be found concerning the right to restriction of processing (Art. 18).

We can think, again, about some of the fundamental rights of the data subject, such as the right to rectification (Art. 16) and to the erasure of data (Art. 17), which appear difficult to be exercised in the context of the Blockchain, where the recorded information is characterized by immutability.

Therefore, the existence of technical solutions for ensuring the implementation of the GDPR provisions must be checked.

---

[52] *Ex multis*, M Berberich-Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?' [2016] European Data Protection Law Review, 422; A Palladino, 'L'equilibrio perduto della blockchain tra platform revolution e GDPR compliance' [2019] MediaLaws, 150; G Frezza, 'Blockchain, autenticazione e arte contemporanea' [2020] Dir fam pers, 489; F Rampone, 'I dati personali in ambiente blockchain tra anonimato e pseudonimato' [2018] Ciberspazio e dir, 459; A Mirchandani, 'The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR' (2019) 29 Fordham Intell Prop Media & Ent LJ, 1201.

[53] C Iorio, 'Blockchain e diritto dei contratti: criticità e prospettive' [2021] Actualidad juridica iberoamericana, 656.

[54] The GDPR is not applicable in the case of anonymous data, namely 'information that does not relate to an identified or identifiable natural person or to personal data rendered sufficiently anonymous to prevent or no longer allow the identification of the data subject' (recital 26 GDPR).

[55] There is always, in fact, the possibility, through special techniques, of re-identification. See F Faini, 'Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection' [2020] Resp civ prev, 297; A Gambino and C Bomprezzi, 'Blockchain e protezione dei dati personali' [2019] 619.

Concerning the principles of minimization and limitation of processing, some authors have suggested solutions which may prove useful for this purpose. They go from the addition of "noise" to the data, to making it more difficult to associate a private key and the data entered.[56] Also, the use of c.d. "disposable addresses"[57] that allow for the creation of a new address and a new one-time password for each transaction could grant compliance with GDPR.

More complex is the attempt to reconcile the Blockchain with the exercise of the right to erasure and rectification of data.[58] In fact, there is the technical possibility of acting on the blocks and modifying the recorded information. However, such an intervention undermines the users' trust in the Blockchain, whose use is justified precisely because the ledger guarantees the certainty and unchangeability of the information recorded on the chain.

Therefore, we can agree with the authors who propose to interpret the right to "erasure" in the generic meaning of making data "inaccessible" for the users. In case the "right to be forgotten" is exercised by the data subject, the information could be made unreachable by means of the destruction of the private key.[59] Another solution is the storing of personal data on an "off-chain" database, which would be linked to the Blockchain (and, therefore, not recorded on the blocks) through a hash.

Thus, the personal data could be deleted, or corrected, without altering the algorithmic function, which would remain unchanged in the digital ledger.[60]

6. The identification of data controller and data processor.

Therefore, there are technical solutions capable of ensuring compliance between the Blockchain and the principles of privacy by design and by default.

Critical issues remain concerning the difficult identification of data processors and data controller within a Blockchain, given the absence of a central authority with supervisory powers in the Ledger.

Several solutions have been suggested by scholars concerning the permissionless Blockchain.

---

[56] The proposed solutions, in detail, include the use of: a) 'Zero-knowledge proofs', a technique that allows a given subject to acquire evidence of a given statement, without guaranteeing access to the underlying data; b) adding 'noise' to data, consisting in grouping a given number of transactions together, so that it is impossible to discern the identity of part of the same; c) 'ring signature', that is, a special type of digital signature that, given a group of users equipped with public and private keys, allows to associate the transaction to the group in a generic way, without detecting the identity of the signing user. M Finck, 'Blockchains and Data Protection in the European Union' [2018] *European Data Protection Law Review*, 15. This opinion is followed by A Gambino and C Bomprezzi, 'Blockchain e protezione dei dati personali' [2019] 622.

[57] M Finck, 'Blockchains and Data Protection in the European Union' [2018] *European Data Protection Law Review*, 15.

[58] There are several technical solutions that can make recorded data editable: ranging from the function of 'chamelon hashes', to the technique of 'pruning' (which allows to delete a data, when the same is no longer necessary), or that of 'fork', leading to the redefinition of chain rules, with the creation of a new Ledger. See M Finck, 'Blockchains and Data Protection in the European Union' [2018] 15.

[59] This solution was suggested by the French CNIL: Solutions for a responsible use of the blockchain in the context of personal data", in https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

[60] This solution could be achieved by using the IPFS protocol ('interplanetary file system'), which includes 'on chain' only the link to the data, in addition to a time stamp and a hash of the outsourced data. M Finck, 'Blockchains and Data Protection in the European Union' [2018] 15.

As for the data controller, there is a tendency to exclude that this role can be played by the software developers, since they do not have the power to decide the purposes or means of processing, or by miners, who only participate in the process of validation of transactions and, therefore, of formation of the chain, without affecting the determination of the purposes of the processing.[61]

Some authors state that data controllers are all the nodes involved in the transaction, provided that the user's choice to make use of that specific Blockchain to carry out a very precise economic operation integrates the determination - respectively - of the means and purposes of data processing.[62]

At the same time, all the nodes that do not participate in the transaction and maintain a copy of the data qualify as data processor.

The identification of the data processor seems less problematic. This role can be easily attributed to the developers of smart contracts or to the "miners": the former are called to process data on behalf of users, while the latter validate the transactions containing personal data, so both of them clearly "process data on behalf of the data controller".[63]

And yet, although we can abstractly proceed to the attribution of the relevant qualifications for the purposes of the GDPR, it is a fact that the features of the permissionless Blockchain make it extremely difficult to fulfill the penetrating obligations provided by the GDPR.

On the one hand, the nature of the register makes it difficult for the data controller to monitor the totality of transactions added to the blocks; but, above all, the pseudonym of the identities prevents users from identifying the controllers, and the latter from identifying the recipient of specific obligations of conduct.

At present, therefore, it would seem that the only technology fully compatible with the legal framework is that of private permissioned Blockchain.

In this case, indeed, since there is an entity that determines the rules of access to the system, roles under the GDPR are easily identifiable: the title of data controller should be assumed by the central authority responsible for determining the criteria for selecting nodes, the system updates, and the rules of transparency.

Conclusions.

The purpose of this paper is to examine some of the critical issues related to the circulation and data processing in the digital age.

As outlined, the disciplinary framework is far from being considered defined.

---

[61] V Bellomia, 'Il contratto intelligente: questioni di diritto civile', in www.judicium.it

[62] M Finck, 'Blockchains and Data Protection in the European Union' [2018] 17; see also French CNIL, 'Solutions for a responsible use of the blockchain in the contex of personal data'; *contra* V Bellomia, 'Il contratto intelligente: questioni di diritto civile', www.judicium.it, 12, who states that this thesis - resulting in a 'widespread responsibility', would involve for any intervention on the treatment (such as the correction of a data) the necessary consent of the majority of nodes, as all co-controllers of each treatment, with the effect of paralyzing the system.

[63] This is the opinion of CNIL, 'Solutions for a responsible use of the blockchain in the context of personal data'.

There are still uncertainties about the legal nature of personal data, as well as about the identification of contractual schemes for their circulations, and the available remedy in case of infringement.

In order to guarantee more extended protection to interested parties, we must welcome the innovations introduced by the two recent EU Regulations of the "Digital Services Act"[64] and the "Digital Market Act".[65]

In order to face the opacity of the algorithmic choices also in relation to the use of data, the first Act provides specific obligations for platforms in terms of information and transparency. In particular, it requires that users are made aware of the rules on the operation of moderation and content recommendation systems, as well as on online advertising. Significantly, there are bans on the use of deceptive practices to manipulate users' choices, and targeted advertising aimed at minors or based on sensitive user data. Also, an obligation for the platforms to enable users to block "recommendations" based on profiling is introduced.

The Digital Market Act completes the set of protections for the consumer, looking at the possible use of data, by the "gatekeeper", for purposes that distort competition in the market.[66] For this reason, the Act establishes new prohibitions on restricting or refusing data portability or data reuse, in order to discourage or prevent the user from leaving the platform; it also provides for the prohibition of combining personal data of the user, derived from the platform services, with other personal data obtained from other services, including third parties, without the user's express permission. In addition, it states the obligation to provide commercial users with effective, continuous, and real-time access to aggregated and non-aggregated data provided or generated in the context of the use of the relevant basic platform services (always with the user's consent).

These Regulations, read in conjunction with the GDPR, are a further piece of the design of that "multi-level protection" of the digital user that, as we have pointed out, is essential to fully implement the effectiveness of the protection of fundamental rights in the technological society.

[64] European Parliament and Council Regulation 2022/2065/EU of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC [2022] OJ L 277/1.

[65] European Parliament and Council Regulation 2022/1925/EU 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 [2022] OJL265/1.

[66] "Gatekeepers" are the subjective categories of platforms subject to the application of the Digital Market Act. The designation as gatekeeper takes place on the basis of qualitative and subjective criteria, as well as in reference to the types of services offered (the so-called "Core Platform Services"), according to the thresholds established by Art. 3.

Dicorato S F, de Pamphilis M, 'Stretching the rules': how racing design may drive the evolution of the technological and legal environment' (2022) 2 EJPLT, 169-186.
DOI: https://doi.org/10.57230/EJPLT222SFDMDP

EJPLT
ISSN 2704-8012



'Stretching the rules': how racing design may drive the evolution of the technological and legal environment.

SIMONE FABIO DICORATO
MEng in Advanced Motorcycle Engineering
Motorvehicle University of Emilia Romagna

MATTEO DE PAMPHILIS
Contract Professor of Product Safety,
Product Liability and Automotive
Alma Mater Studiorum Università di Bologna

Abstract

Andrea Dovizioso's victory in the opening race of the 2019 Moto GP season at Qatar has been subjected to appeal. Dovizioso raced in Qatar using the new aerodynamic components and he won a thrilling close race by a margin of only 0,023 seconds from Marc Màrquez; the top five finished within six tenths of a second. The new aero parts prompted four factories (Aprilia, Honda, KTM, and Suzuki) to lodge a protest with the FIM Stewards, claiming that the aerodynamic device attached to the swingarm was illegal. 'The Spoon' developed by Ducati Moto GP team led to significant technical improvement of the Ducati GP19 motorcycle and its legal debate, involving the FIM, had a huge media impact. According to Ducati the discussed component had a function of cooling the rear tire by directing airflow directly onto its surface. However, exploration into its exact effect had thrown up a number of theories to its main function, one being that it helped the bike in becoming more slippery through the air, improving its aerodynamics and therefore reducing drag. Drag reduction or tyre cooling? On 22nd March 2019, the Moto GP Court of Appeal ruled that Ducati's aero spoiler was legal.

La vittoria di Andrea Dovizioso nella gara inaugurale della stagione 2019 di Moto GP, in Qatar, è stata oggetto di contestazione. Dovizioso ha corso in Qatar utilizzando i nuovi componenti aerodinamici e ha vinto un'emozionante gara ravvicinata con un margine di soli 0,023 secondi da Marc Màrquez; i primi cinque classificati hanno chiuso entro sei decimi di secondo. I nuovi componenti aerodinamici hanno spinto quattro case costruttrici (Aprilia, Honda, KTM e Suzuki) a presentare una protesta ai commissari sportivi della FIM, sostenendo che il dispositivo aerodinamico montato sul forcellone fosse illegale. Il 'cucchiaio' sviluppato dal team Ducati Moto GP ha portato a un significativo miglioramento tecnico della moto Ducati GP19 e la disputa legale, che ha coinvolto la FIM, ha avuto un enorme impatto mediatico. Secondo Ducati, il componente in questione aveva la funzione di raffreddare lo pneumatico posteriore dirigendo il flusso d'aria direttamente sulla sua superficie. Tuttavia, lo studio del suo effetto esatto ha fatto emergere una serie di teorie sulla sua funzione principale, una delle quali è che rende la moto più fluida nell'impatto con l'aria, migliorando la sua aerodinamicità e quindi riducendo la resistenza aerodinamica. Riduzione della resistenza aerodinamica o raffreddamento degli pneumatici? Il 22 marzo 2019, la Corte d'Appello della Moto GP ha stabilito che lo spoiler aerodinamico della Ducati è legale.

© The author(s) 2022, 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: MotoGP; Sports law; Appeal.

Summary: Introduction. – 1. Case background. – 2. A look at Moto GP rules and regulations in 2019. – 3. Case study: Moto GP Ducati GP19 swingarm device in 2019. – 4. Notes on the case final outcome. – Conclusions.

Introduction.

Nowadays, the evolution of law is increasingly guided by technological development.[1] In this perspective, the interdisciplinary collaboration between legal[2] and engineering experts becomes central. This collaboration serves not only to manage the problems that occur to the attention of the legislator, but also to anticipate them. In this sense, the world of automotive and motorcycle sports competitions represents a very interesting study soil. In fact, the technological solutions adopted in the context of these sports competitions have always permeated the market of cars and motorcycles for private use, increasing its safety.[3] The mobility sector, as known, has been and is at the centre of the evolution of modern society and, consequently, of the legal framework.[4] Jurists and engineers are now called to collaborate to define the legal framework of the mobility of the future, studying the best technological and legal solutions to protect the safety of drivers, passengers and in general of users of mobility services, bearing also in mind the need to design economically sustainable solutions.[5] In this context, the case of study proposed in this article can represent a fruitful meeting soil between the legal and

[1] See L B Moses, 'Agents of change: how the law copes with technological change' (2011) 20(4) Griffith L. Rev., 764 ff.; see also A J Cockfield, 'Towards a law and technology theory' (2004) 30(3) in Man. LJ, 383 ff.; In the Italian perspective, see also E Al Mureden, 'Event data recorder e advanced driver assistance system': la 'spinta gentile' verso la mobilità del futuro (2022) 2 in Contr. impr., 390 ff; see also E Al Mureden, G Calabresi, 'Driverless car' e responsabilità civile (2020) suppl. Riv. dir. banc., 7 ff.; see also E Al Mureden, U Ruffolo, 'Autonomous vehicles e responsabilità nel nostro sistema ed in quello statunitense' (2019) 7 Giur. it., 1704 ff.; see also E Al Mureden, 'Autonomous cars e responsabilità civile tra disciplina vigente e prospettive de iure condendo' (2019) 3 Contr. impr., 895 ff..

[2] An overview on the legal perspective can be found in L Gatt, 'Legal anthropocentrism between nature ad technology: the new vulnerability of human beings' (2022) 1 EJPLT, 15 ff.; MC Gaeta, Liability rules and self-driving cars: the evolution of tort law in the light of new technologies (ESI, 2019); MC Gaeta, 'Automazione e responsabilità civile automobilistica' (2016) 5 Resp. civ. e prev., 1718 ff.; MC Gaeta, 'La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi' (2018) 1 Dir. inf. e informatica, 147 ff.; MC Gaeta, 'The regulation of certain aspects of autonomous driving in the Italian legal system' (2022) 1 EJPLT, 263 ff.: L Gatt, IA Caggiano, MC Gaeta, 'Italian Tort Law and Self-Driving Cars: State of the Art and Open Issues', in BH Oppermann e L Stender-Vorwachs (a cura di), Autonomes Fahren. Technische Grundlagen, Rechtsprobleme, Rechtsfolgen (C.H.Beck, 2020), 239 ff..

[3] See E Candelo, *Marketing Innovations in the Automotive Industry. Meeting the Challenges of the Digital Age* (Springer, 2019).

[4] See E Al Mureden, G Calabresi, *Driverless cars* (Bologna, 2021).

[5] See E Al Mureden, 'Il futuro del 'law and economics' nel pensiero di Guido Calabresi' (2018) 3 Riv. dir. civ., 778 ff.; see also E Al Mureden, *Costo degli incidenti e responsabilità civile' quarant'anni dopo. Attualità e nuove prospettive dell'analisi economico-giuridica di Guido Calabresi* (ivi, 2015, 1026); see also E Al Mureden, 'Il pensiero di Guido Calabresi e il suo influsso sull'armonizzazione della responsabilità del produttore nell'Unione Europea [2015] in Not. Politeia, 102.

engineering knowledge, in the path that will lead to drawing the future of mobility.[6]

1. Case background.

If a student inquired about a course in sports law at a university or law school 25 years ago, that student may have encountered a blank stare. Fortunately, that is not the case today. The business of sports has become a multimillion-dollar industry with sports law leading the way. The topics of sports law run the gamut of legal and societal issues, dealing with many categories of law, including contracts, torts, intellectual property, labour relations, antitrust and agency law. The rise of interest in sports law mirrors the explosion of the interest in sports in society and the business of sports. Sports law looks at the major legal cases, statutes, and regulations that explore a variety of legal issues in sports law.

For what concerns the Moto GP world, which is the main topic of this paper, it could be said that the Race Direction is the observant nerve centre of the Moto GP.[7]

The Race Direction must manage the event (Moto GP race) and everything that comes with it, both for sports-related and non-sports related things. For example, if the race has a problem with the spectators, the Race Direction should solve the trouble.

A famous historical case is that of Indianapolis, in which the forecast announced that there was going to be a lightning storm on the track and according to American legislation, if necessary, the circuit had to be evacuated within certain times. All these decisions are made by the Race Direction.

Moreover, when the Spanish Grand Prix is hold, there is always a member of the Guardia Civil, the National Police, present, or a member of the Mosso D'esquadra, regional police, in Catalonia, in case there are any problems with the spectators.

In Misano, the Race Direction decide when to let people onto the track. It's not a decision taken at that time, but completely the opposite: it is something that is decided on beforehand between the police chief and Race Direction.

On the international side, the Race Direction is made up of three people. For example, there are three of them that make decisions to raise the red flag.

In the past, there was a Race Director who would make all the decisions. This led to several problems because there were decisions made that people did not understand. So, it was decided to create a system in which there is a representative from each member group of the Championship.

IRTA has a representative, FIM has another one and Dorna has another representative. Together they make joint decisions. When a decision must be made, the IRTA representative will support teams more, the FIM representative

[6] See M Wegener, 'The future of mobility in cities: Challenges for urban modelling' [2013] *Transport Policy*; see also J Zmud, L Ecola, P Phleps, J Feige, *The future of mobility: Scenarios for the United States in 2030* (RAND, 2013); see also S Shaheen, H Totte, A Stocker, *Future of mobility white paper* (in eScholarship, 2018).

[7] Box Repsol, *Race Direction: the observant nerve centre of the MotoGP* [2016] in https://www.boxrepsol.com/en/motogp-en/race-direction-the-observant-nerve-centre-of-the-motogp/.

will support safety, and the Dorna representative opt for decisions that affect the show. The truth is that Dorna holds races. At Dorna there is the motto: '*Hold races, show them on TV, and then sell time for adverts but... You have to hold races*'.

During a GP, fans often read the TV news ticker that shows that an incident is being investigated. What is the protocol in these cases and what stages do these investigations go through?

Race Direction has always investigated what has needed to be investigated, but not that long ago, Race Direction spoke with press representatives and decided that it was better to announce it. A pre-analysis of the situation is done and if it seen that a more in-depth analysis must be performed, that is when Race Direction makes it public. The situation is managed in this way so that everyone understands that Race Direction has seen the fact and is analysing what people saw on TV and what commentators continue to mention.

People must understand that sometimes it's difficult when a race is going on to work on analysing a specific moment of it. That's why sometimes the accident is analysed after the fact. On other occasions, if Race Direction feels that what has happened could affect the result of the race, it tries to do it during the race.

In a tense situation when Dorna members are deliberating what penalty the rider will receive, do they have a time limit to decide? If so, how long is it?

Of course, it depends on the penalty. If a rider gets a head start, Dorna has four laps to notify him. If two riders touch one another, which sometimes Dorna can't see and in the afternoon one of the riders calls the Race Direction and tells it that this has happened, Dorna looks into it. There have been cases when a rider was penalised a week after.

Dorna has always tried to have an ongoing dialogue with teams and riders. A decision is usually made because Dorna believes that it is the right one. However, Dorna tries to involve everyone affected by this decision. The process may be a little long, but it is a way to ensure that everyone is involved and that they agree with what Dorna is doing.

There are meetings every two or three GPs for the new technical or sport regulations. Every Friday, meetings are held with the riders and with the teams, almost one out of every two races. Anyway, later, Dorna keeps in touch constantly with teams: even if there is no definite structure, Dorna tries to talk about everything with everyone.

FIM President Vito Ippolito, in 2018, has given an interview in which he explains what has changed in terms of the disciplinary procedures since 2016.[8]

Following a process that began in 2016, the FIM Stewards are now responsible for disciplinary sanctions, while the Race Direction takes care of the management of the race. What is the reason for this decision? Vito Ippolito, FIM President, said: *'In the last years we were thinking how to improve the management of Moto GP during the races. In the past, race direction had all the responsibility; not only to manage the races, but also to penalise the riders. We were thinking it would be much better to separate these two functions because*

[8] Moto GP official website (2018), *Race Direction and FIM Stewards: Vito Ippolito explains*, https://www.motogp.com/en/news/2018/04/17/race-direction-and-fim-stewards-vito-ippolito-explains/255236.

the race direction is very busy, there is a big responsibility, but the management of the race have to decide how to place the grid to show a red a flag to intervene in many delicate parts of the races, take decisions about whether the race is wet or dry and the judges are the FIM stewards. Now we separate these two functions because of the way you approach the race, the event is different because now you are a judge – a judge is different from a race director, for example (…) FIM Stewards are expert people. Their job is only to penalise. They have a lot of experience, of course, and I can add that after each race there is an analysis; a study of what happened during the race, about the behaviour of the riders or about any other kind of problem around the penalties. Then we have many stewards; more than twenty but for each championship, in this case Moto GP, we choose a small part of these stewards, one of them is permanent for each race and the others rotate but, in any case, there is a short choice of stewards for the Moto GP (…) The advantage of this new structure is that, because the Moto GP Race Direction is too busy, they haven't got enough time to manage the race at the same time and penalise, we were thinking that if we separate these two structures, we will have better results because at the end the justice that the stewards do and they can impose penalties during the event, which is extremely important. We must not only be fair but show that we're fair and for this reason we decided that we would separate this function. Then, since 2017, it is the FIM stewards that are responsible for all penalties during Moto GP'.

Several analyses on the present case of study have been carried-out by journalists and published as articles on magazines. However, nobody has performed a conjoint study between technical and law aspects, which is the purpose of this paper.

This paper has been structured coherently with its purpose: at first all the law elements that should be known to deeply understand the legal case are provided and then, the case study is analysed from a technical engineering point of view.

As a matter of fact, the paper deals with Moto GP rules and regulations and all the legal system laying behind it. A wider picture of the hierarchical structure for Moto GP legal cases is depicted and legal debates between two or more teams are discussed. In addition, providing an insight of the FIM Moto GP regulation, possible consequences for non-compliant teams are presented. Then the article provides a technical description of the case study of this report. To be a fluent reading also for a non-expert public, a description of the main engineering features of a general motorcycle swingarm is initially given. After, a deeper analysis of the Moto GP Ducati GP19 swingarm device is carried out and the legal debate about it is described. Eventually, the final judgement of the Court and the consequences for Ducati Moto GP team are discussed. Moving toward its conclusion, the paper provides general conclusions regarding the Ducati aero appeal. Afterwards, a new hypothetical scenario for future rules and regulations applied to counter similar cases is figured with the aim of assessing who will be liable for them in case of new class actions and which could be the legal consequences.

2. A look at Moto GP rules and regulations in 2019.

What follows is based on the *'Disciplinary and Arbitration Code'* of the FIM World Championship Grand Prix Regulations (amended as from 01/01/2021).[9]

The obligations incumbent upon the participants, officials and organisers are set out in the Regulations published by the FIM.

Proven violation or non-observance of these obligations will be subject to the penalties laid down in this chapter.

The bodies of the FIM, qualified to deal with race decisions, disciplinary and arbitration matters, are the Race Directio;[10] the FIM Moto GP Stewards Panel;[11]

[9] FIM official website (2022), *FIM World Championship Grand Prix Regulations 2022*, in https://www.fim-moto.com/en/documents.

[10] The Constitution of the Race Direction is in accordance with the requirements laid down by the Regulation. The Race Direction will comprise the following people: the FIM Representative; the DORNA Representative; the IRTA Representative (who is the Race Director). These persons can perform other functions during the event. The quorum for a meeting of the Race Direction is two persons. Each member has one vote. Decisions are based on a simple majority. The Race Direction will meet at any time required during the event. The duties of the Race Direction are: to take decisions as provided in the Regulations; to oversee operational matters to ensure the safe, efficient, and timely running of the event according to the FIM World Championship Grand Prix Regulations; to make changes in the conduct and/or format of a race and/or a practice session based on safety considerations, provided that such decision is absolutely necessary to resolve a situation not foreseen in the FIM World Championship Grand Prix Regulations. In such exceptional cases, such decision may prevail over specific provisions of the FIM World Championship Grand Prix Regulations. Provided that it is necessary to resolve a situation not foreseen in the Regulations, the Race Direction may issue pre-race instructions or clarifications and in specific cases even create pre-race regulations. However, such actions may only be taken within the limits set out by the FIM World Championship Grand Prix Regulations. The Race Direction has the authority to refer any case involving riders, teams' personnel, Officials and Promoters/Organisers, and all persons involved in any capacity whatsoever in the event or in the Championship, to the FIM MotoGP Stewards Panel for possible disciplinary for: any voluntary or involuntary action or deed accomplished by a rider or team member or any other person as mentioned above, contrary to the current Regulations or instructions given by an official of the meeting; any voluntary or involuntary action of Officials and Promoters/Organisers for having been unable to ensure the smooth and efficient running of the event or for serious breaches of the Regulations and Protocols covering the event organisation.

[11] The Constitution of the FIM Moto GP Stewards Panel is in accordance with the requirements laid down by the same Regulation. There will be a panel comprised of three persons holders of an FIM GP Super- licence; Two FIM Stewards will be nominated by the FIM, the third one will be nominated by IRTA, who will be a permanent member and the Chairman. Each FIM Steward may be a permanent appointment, or appointed by rota, and approved by the Permanent Bureau. These people can perform other functions during the event. The quorum for a meeting of the FIM Moto GP Stewards Panel is two people. Each member has one vote. Decisions are based on a simple majority. In the case of a tie, the Chairman will exercise a casting vote. The FIM Stewards have no executive role in the running of the events, except for the imposition of penalties and the adjudication of protests as per Art. The FIM Moto GP Stewards Panel will meet at any time required during the event. The FIM Moto GP Stewards Panel is responsible for: taking decisions as provided in the Regulations; imposing penalties for any infringements of the Regulations; adjudicating on any protest relating to infringements of the Regulations. All decisions of the FIM Moto GP Stewards Panel must be communicated in writing to the Race Direction and all affected parties. The FIM Moto GP Stewards Panel has the authority to penalize riders, teams' personnel, officials, promoters/organizers and all the persons involved in any capacity whatsoever in an event or in the Championship for: infringements of the Regulations; any voluntary or involuntary action or deed accomplished by a person or a group of persons during a meeting, contrary to the current Regulations or instructions given by an official of the meeting; any corrupt or fraudulent act, or any action prejudicial to the interests of the meetings or of the sport, carried out by a person or a group of persons occurring during an event. The FIM Moto GP Stewards Panel is competent to adjudicate upon a protest relating to infringements of the Regulations. Penalties that may be pronounced by the FIM Moto GP Stewards Panel: a warning; a fine; a change of position; long lap penalty(ies); a ride through; a time penalty; a grid penalty; a disqualification; a withdrawal of Championship points; a suspension. Furthermore, the FIM Moto GP Stewards Panel can refer the case to the Moto GP Court of Appeal in order to impose a higher penalty than the FIM Moto GP Stewards Panel is empowered to do.

the FIM Appeal Stewards;[12] the International Judicial Panel;[13] the Moto GP Court of Appeal.[14]

For all the appeals to the Moto GP Court of Appeal, the FIM is entitled to assert its interests or to explain its position by means of a prosecution address. The Executive Board shall appoint in each case, the person who will represent the FIM. The intervention of the FIM is optional and is left to the appreciation of the Executive Board. As a party, the FIM enjoys the same rights and obligations as the other parties. The FIM may be present in person at a hearing or may present its claims in writing.

In case of a behaviour of an exceptional gravity, the President of the FIM, the FIM Executive Board may refer the case to the FIM CDI which will hear such a case according to the procedures and time limits laid down by the General FIM Disciplinary and Arbitration Code.

A protest is an action taken by any legal entity or any individual, rider, team, manufacturer, official etc. against another legal entity or any individual, rider, team, manufacturer, official etc.

After an immediate hearing, the FIM Moto GP Stewards Panel must make a decision on any protest presented. The protest has to be judged according to the provisions of the Regulations.

The decision of the FIM Moto GP Stewards Panel of determination of penalty is immediate.

An appeal is an action taken by any legal entity or any individual, rider, team, manufacturer, official etc. affected by a penalty or decision issued by the FIM disciplinary authorities (whether arising from a protest or otherwise).

It is interesting also to note that in the procedure before all the Disciplinary and Arbitration Bodies there shall be the unquestionable right of any person or body charged with any offence under the Regulations to defend themselves,

---

[12] The FIM Appeal Stewards will consist of one FIM Steward with FIM Sporting Steward Superlicense, who will be the chairman of the FIM Appeal Stewards and exercise a casting vote if necessary. This Steward will be nominated by the FIM and approved by the Permanent Bureau; one FMNR Steward with FIM Sporting Steward License, nominated by the FMNR and approved by the FIM. The FIM Appeal Stewards will hear any appeals against decisions taken by the FIM Moto GP Stewards Panel. The FIM Appeal Stewards may confirm or overturn a decision of the FIM Moto GP Stewards panel or impose a different penalty. The FIM Appeal Stewards may refer the case to the Moto GP Court of Appeal if it appears impossible to deal with the case for any valid reason. Such a decision will be justified in writing by the FIM Appeal Stewards.

[13] The International Judicial Panel (CJI) is composed of qualified persons from which the member of the Moto GP Court of Appeal is nominated. The International Judicial Panel shall consist of members nominated by FMNs. Each FMN may nominate one or several members having the nationality of that FMN. The appointments shall be confirmed by the General Assembly for 4-year periods. In order to qualify for appointment to the International Judicial Panel, a candidate must be in possession of a diploma in Law studies of university level. He must be able to express himself in at least one of the official languages of the FIM. He cannot however be an officer or a license holder of the FIM.

[14] The FIM Legal Director in collaboration with the Director of the CJI will ap- point, each time, the judge(s) who will constitute the Moto GP Court of Appeal. The name of the judge(s) appointed must be communicated to all interested parties in the case, who have the right to make a duly documented objection to the composition of the Court, the day after having received the information. If the Permanent Bureau considers that a reasonable objection is made, they must appoint the necessary replacements. Otherwise, they reject the objection and fix the date for the hearing. The court may request the opinion of an expert or summon a witness who it considers useful. The Moto GP Court of Appeal will hear any appeals against decisions taken by the FIM Appeal Stewards. The Moto GP Court of Appeal adjudicates upon request of the Race Direction, the FIM Moto GP Stewards Panel, or the FIM Appeal Stewards. The President of the FIM, the Executive Board or the Management Council may, within 4 days after an Event, refer to the Moto GP Court of Appeal matters of violation or infringement of the FIM regulations not concerning sporting or technical regulations.

either in person or by proxy. Any party convened before a disciplinary or arbitration body has the right to be represented by one defence counsel of its own choice and at its own expense. Adequate notice of this intention must be given in order that this may also be notified to all other parties in the case. Failure to do so may result in the disciplinary or arbitration body upholding an objection to such representation. If any of the parties duly convened do not appear, judgment can be rendered by default.

The disciplinary or arbitration bodies may decide that the hearing take place by means of a telephone conference call or through any other means of communication using a telephone or electronic device. Such a method of conducting a hearing shall only take place with the consent of all parties involved.

The hearing shall be public unless the disciplinary or arbitration body itself decides otherwise in exceptional circumstances. The hearing shall be conducted in one of the official languages of the FIM. Should one of the parties wish to use another language, it shall provide the necessary interpreters at its own costs. The appellant must be present or duly represented, failing which, the protest will not be admissible, and the costs shall be borne by the appellant.

Once the Judge(s) has opened the proceedings, he will invite the parties involved to state their respective cases without the witnesses being present. After statements of the parties concerned, the disciplinary or arbitration body shall hear the various witnesses and experts to complete the evidence. The parties involved in the case shall have the right to question all witnesses and experts on their evidence. Any member of the disciplinary or arbitration body may, at any time during the hearing and with the Judge's approval, question any of the parties involved, the witnesses and experts.

Each party is responsible for the convening and appearance of its own witnesses, as well as their expenses unless decided otherwise by the Court. The disciplinary or arbitration body has no authority to oblige the witnesses to swear on oath; therefore, testimony shall be given freely. The witnesses may only testify to the facts they know and shall not be allowed to express an opinion, unless the disciplinary or arbitration body should regard them as experts on a particular subject and should ask them to do so.

After having made their statements, the witnesses may not leave the Courtroom and shall not be allowed to speak to any other witness who has still to give evidence. The Court may summon experts.

Decisions of all disciplinary or arbitration bodies will be reached in camera by a simple majority of votes. All members will have equal voting rights which must be exercised when a decision is required. Abstention is not permitted. Each member of the disciplinary or arbitration body binds himself to keep all deliberations secret. The disciplinary or arbitration body imposing a penalty or adjudicating a protest or an appeal must have its findings published and quote the names of all parties concerned. The persons or bodies quoted in these statements have no right of action against the FIM nor against any person having published the statement.

Furthermore, final decisions will be published in the Media Centre and in the FIM Magazine unless the Court itself decides otherwise.

As a consequence of the agreement of reciprocity concluded on April 30th,

1949 between the 4 organisations controlling motorised sports internationally (i.e. in addition to the FIM, the Fédération Internationale de l'Automobile, FIA, the Fédération Aéronautique Internationale, FAI, and the Union Internationale Motonautique, UIM), penalties of suspension or exclusion may also be applied to one or another of the sports represented by the above organisations, upon request of the FIM.

3. Case study: Moto GP Ducati GP19 swingarm device in 2019.

A swingarm (*fig. 1*), or swinging arm (UK), originally known as a swing fork or pivoted fork, is a single- or double-sided mechanical device which attaches the rear wheel of a motorcycle to its frame, allowing it to pivot vertically. It's the main component of the rear suspension of most modern motorbikes, it holds the rear axle firmly, while pivoting to absorb bumps and suspension loads induced by the rider, acceleration, and braking.[15]



Figure 1: Traditional motorbike swingarm
(Picture courtesy of: https://www.cycleworld.com/sport-rider/2003-yamaha-yzf-r6/)

The main goal to achieve when finding the optimal design of a Moto GP swingarm is to obtain a final lightweight component, but which can withstand all the external fluctuating loads without showing a plastic deformation.

Luigi Dall'Igna (Technical Crew Chief of Ducati Moto GP) got a genial idea, which costed him the appellative of 'the wizard': why not exploiting the ground effect also in Moto GP?

He developed his technical concept and, for the first time, some aerodynamic appendages have been seen on a motorcycle swingarm. These appendages, visibly made with 3D technology, leave many doubts about their real function: do they serve to promote downforce and give more grip to the rear tire, or simply to cool the tread? Or both effects? For sure, a fin positioned

[15] Giacomo Guidotti (Crew Chief of Hector Barbera in 2013) said: '*The swingarm is a part of the chassis and it works everywhen during the action of a motorbike. It's really important in launch starts because it needs to be enough rigid to support the load of the engine, which in first gear is very huge. It comes into play also in braking manoeuvre because it should be enough stiff and stable to support all the stresses concentrated in this so short deceleration time. In addition, it's very important also in mid-corner areas because it should be able to absorb and damp all the vibrations coming from asphalt disturbances and bumps*'.

on the swingarm can generate an effect tending to keep the bike attached to the asphalt, particularly useful during acceleration.[16]



Figure 2: Ducati GP19 Swingarm Attachment device
(Picture courtesy of: https://www.corsedimoto.com/motomondiale/motogp/motogp-la-tecnica-lo-spoiler-ducati-quante-polemiche/)



Figure 3: Ducati GP19 Swingarm Attachment device, zoomed view
(Picture courtesy of: https://www.motogp.com/en/news/2019/07/30/technology-trends-through-2019/301476)

The philosophy of Ducati Racing Team was to make a larger use of the aerodynamic downforce to improve the performance of the motorcycle controlling the centre of gravity of the bike and the lack of wheelbase. Ducati's controversial will born due to wing elements mounted on the swingarm of Ducati Moto GP racing motorbike GP19. As it can be seen from *fig. 2* and *fig. 3*, there are three elements that look like to be designed by a road racing car designer to produce downforce.

Taking a deeper look to the whole design of the swingarm and of these wing elements (*fig. 4*), it can be easily seen that these three elements split and the gaps between the elements have the function of flow air.

[16] Corse di moto la nostra passione (2019), *Spy MotoGP: La Ducati ad 'effetto suolo'?*, in https://www.corsedimoto.com/motomondiale/spy-motogp-la-ducati-e-ad-effetto-suolo/.



Figure 3: Ducati GP19 Swingarm Attachment device, 3 split elements

The lowest element, which is the shallowest one, would feed the central element and the central element would feed the steepest element, in order to prevent the wing stall or the aerodynamic package stall.

Ducati claimed that this device was designed cool the rear tyre, but they could easily reach this goal by using scoops or by mounting NACA ducts at the side of the swingarm, just to push air to the tyre and to the top of the wheel. Apparently, it doesn't quite make sense for them to cool the rear tyre in this way, because if this system was designed only on purpose to do that, the tyre in the lowest point (just behind the 3 elements) immediately reaches the ground and it will have no time to cool.

However, the new component hadn't to introduce any kind of instability in the motorcycle in all the dynamic manoeuvres.



Figure 4: Ducati GP19 braking manoeuvre, right-side lateral view
(Picture courtesy of: https://www.infomotori.com/motorsport/motogp-2019-gp-di-gran-bretagna-acuto-di-marquez-nelle-libere-di-silverstone-poi-vinales-dovizioso-quarto-rossi-17esimo_301599/foto-11/)

Starting with the braking phase, when the motorcycle is breaking into a corner (*fig. 5*), the swingarm drops and it exposes much the wing elements.

In addition, Ducati had mounted on the bike also front brake discs spats to improve the air flow towards these 3 wing elements (*fig. 6*). Actually, on Danilo Petrucci's Ducati GP19, another deflector has been added on the front wheel which probably has the purpose of channelling the air flow that goes to the radiator and back, and therefore to the fin of the movable arm. Obviously, during braking manoeuvre, also this component is producing downforce. A

further analysis of the front brake discs spats will be carried out while studying the acceleration phase.



Figure 5: Ducati GP19 braking manoeuvre, left-side lateral view
(Picture courtesy of: https://it.motorsport.com/motogp/news/la-corte-dappello-da-ragione-a-ducati-vittoria-confermata-e-spoiler-legale/4358989/#gal-4358989-m0-andrea-dovizioso-ducati-team-43241470)

During mid corner phase (*fig. 7*), the downforce would push the bike to slide more, against the centripetal force. Ducati engineers cleverly designed this 'spoon' so that during cornering it sort of tuck in, not producing too much downforce when the bike is leaning.



Figure 6: Ducati GP19 mid corner
(Picture courtesy of: https://www.cnnindonesia.com/olahraga/20190811190857-156-420333/hasil-motogp-austria-dovizioso-menang-dramatis-atas-marquez)

During acceleration phase (*fig. 8*), the wing elements are slightly tucked inside and not sticking out to scoop more air, since the rear suspension is compressed. Effectively, it can be said that this wing element, the front brake discs spats (*fig. 9*) that complement it and the achieved air flow are designed for manoeuvres such as high speed breaking and entering into a corner so that the structural swingarm would have some downforce on it. It will drop and it will keep the rear wheel on the ground, reducing the possibility to have a 'stoppie' of the motorbike, maintaining lateral grip and making the bike swing. Under heavy breaking, the bike would be swinging side by side and become unstable. Having this innovative rear wing element, the bike would neutralize the negativity of the front wings: the motorcycle brakes and this system makes

the rear suspension drop down intaking an air flow which provides downforce for the rear.



Figure 7: Ducati GP19 acceleration manoeuvre
(Picture courtesy of: https://www.gpone.com/it/2019/05/30/motogp/dovizioso-stoner-lorenzo-ducati-cerca-il-poker-al-mugello.html)



Figure 8: Ducati GP19 front brake discs spats: on the left the optimized air flow could be seen
(Picture courtesy of: Sky Sport)



Figure 9: Ducati GP19 ground effect
(Picture courtesy of: Sky Sport)

Summing up, the global effect generated by the air flows is clearly displayed in *fig. 10*.

In a press conference, Luigi Dall'Igna said: '*Of course, we are still a long way far from the ground effect of a Formula 1*'.

In the past, in the motorcycles, some 'splits' had been seen fixed on the lower part of the fairings of some Aprilia GP125s. Who was the technical director in Aprilia at that time? The same Luigi Dall'Igna who is now the wizard of Ducati secrets.[17]

This is the first time in which a manufacturer was really working on the flow of air that passes under a motorcycle: the imagination of the Italian engineer has no limits.

Andrea Dovizioso's victory in the opening race of the 2019 Moto GP season in Qatar had been subject to appeal. Dovizioso raced in Qatar using the aerodynamic components previously debuted by factory Ducati teammate Danilo Petrucci at the Qatar test and used by Petrucci and Pramac Ducati's Jack Miller during practice at the Qatar Moto GP round. After Dovizioso won a thrilling, close race by a margin of 0,023 seconds from Marc Màrquez the top five finishing with six tenths of a second, but the race was the first time Dovizioso had used the new aero parts.

Following the Moto GP Race of the Qatar Grand Prix, four factories – Aprilia, Honda, KTM, and Suzuki – filed a protest with the FIM Moto GP Stewards Panel, meaningfully the body of first instance competent to adjudicate upon a protest related to infringements of the FIM World Championship Grand Prix Regulations.

The protest concerned the aerodynamic device in mention, mounted on the rear swingarm of Ducati motorcycles driven by Andrea Dovizioso (using this device for the first time in this race), Danilo Petrucci and Jack Miller.

The FIM Moto GP Stewards Panel rejected the claim, considering that the aerodynamic device used did not contravene the regulations.

So, after conferring with the Technical Director Danny Aldridge, the FIM Stewards rejected the protest by the four factories, on the grounds that the aerodynamic devices used did not contravene the regulations.

Anyway, the four factories then immediately lodged a protest, which they had prepared previously. According to Manuel Pecino, writing in the Spanish daily Mundo Deportivo, the parties involved had signaled in advance that they would be protesting Ducati's use of the devices, if they were used in the race.

Therefore, the protestants, within the time limit of 30 minutes set forth in the Regulations, lodged an appeal with the FIM Appeal Stewards, the body of second instance competent to hear any appeal against decisions taken by the FIM Moto GP Stewards Panel.

FIM Appeal Stewards, considering impossible to deal with the case (absent any further detail), referred the case to the Moto GP Court of Appeal.

The appeal went forward to the Moto GP Court of Appeals, which met in Geneva, where they considered the case. A judgment is expected to take a couple of weeks and may not be ready before the next round of Moto GP at Termas de Rio Hondo in Argentina.

The results of the Qatar round of MotoGP staid unless they were overturned by the Court of Appeal, although if they were overturned, and Ducati's aero

[17] Corse di moto la nostra passione, *Spy MotoGP: La Ducati ad 'effetto suolo'?* [2019] https://www.corsedimoto.com/motomondiale/ spy-motogp-la-ducati-e-ad-effetto-suolo/

devices ruled illegal, Ducati was certain to appeal to the Court of Arbitration for Sport (CAS). If the Court of Appeal upholds the ruling of the FIM Stewards, then that would settle the matter once and for all. No right of further appeal exists in that case.

Speaking on Sunday night, Ducati Corse Sporting Director Paolo Ciabatti explained why Ducati believed the aero devices are legal: '*It should be clear to everyone, because all manufacturers received a document from Danny Aldridge on the 2nd of March, which was guidelines for aerodynamics in general, mainly due to the bodywork. But it had a specific article related to that, saying that you can use such parts under certain limits: it has to be attached to the swingarm, it has to move with the swingarm, it has to be used for cooling, protecting from water, protecting the rear wheel from debris. We use it for cooling'*

This directly contradicted Danilo Petrucci, who told on Friday, '*We saw on television that it was for cooling down the rear tire, but it is not like this. But I can't tell you what it is for, because Gigi will get angry'*. Ciabatti said that Ducati had not wanted anyone to know that the purpose of the aero device was cooling, for the same reason they don't tell anyone about what any of the rest of the bike does. '*We didn't like to say this, because we don't like to tell people what we are doing'*, Ducati's Sporting Director said. '*But that's the main purpose. Its purpose is not to create an aerodynamic force to the ground, which is what they say. And ours is not for that'*. The biggest question, of course, is whether it is legal or not. Speaking to Danny Aldridge on Friday, he said that the parts did not contravene the regulations.

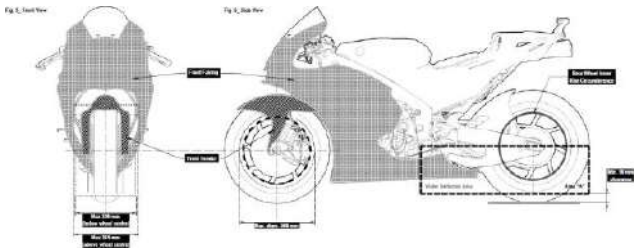


Figure 10: Aero Body of a Moto GP motorcycle, FIM World Championship Grand Prix Regulation (page 258)

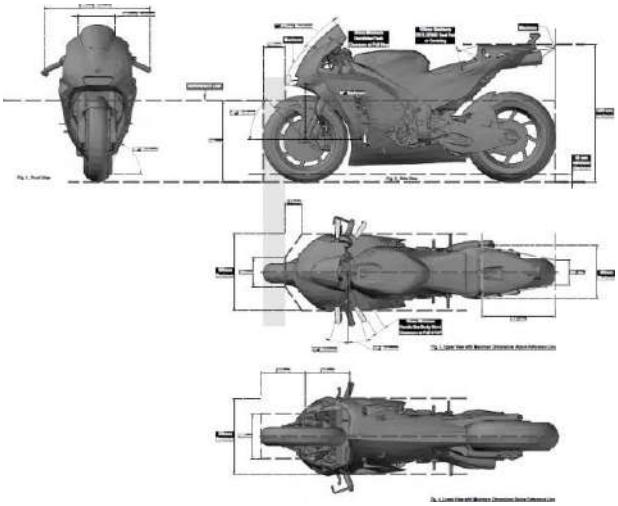


Figure 11: Fairings of a Moto GP motorcycle, FIM World Championship Grand Prix Regulation (page 259)

The Moto GP regulation on aerodynamics does not cover devices attached to the swingarm, or to the bottom of the front wheel, where the carbon covers are located.

Here is what the relevant part of the rules said: '*The Moto GP Aero Body is defined as the portion of the motorcycle bodywork that is directly impacted by the airflow while the motorcycle is moving forward, and is not in the wake (i.e. aerodynamic 'shadow') of the rider's body or any other motorcycle body parts. Therefore, the Aero Body consists of the two separate components Front Fairing and Front Fender (Mudguard)'.*

To make the rules clear, the rule book also has pictures (*fig. 11* and *fig. 12*).

If someone compared these pictures with the Ducati aero-device photos, they could clearly see that Ducati have looked at the diagram and seen where the loophole was. They applied the covers to the bottom of the front wheel and attached a spoiler to the bottom of the swingarm.

The Court of Appeal sat in Mies, Switzerland, the offices of the FIM, and heard submissions from Ducati, and from the other four factories. Ducati had Fabiano Sterlacchini present alongside Gigi Dall'Igna, while Suzuki and Aprilia had brought Filippo Petrucci, a Ferrari engineer who had worked with Michael Schumacher in F1 previously, to help present their objections. The case revolved around the function of the spoiler fitted to the bottom of the Ducati's swingarm. Ducati claim that it helps to cool the rear tire. The other four factories, Aprilia foremost among them, point to the fact that the spoiler has three horizontal vanes, which must, they claim, create some kind of downforce. However, as these parts were not attached to what the rules called the Aero Body (the fairing and front fender), Ducati were free to attach and remove them as they see fit. This was why they do not fall under the ban on detachable aerodynamic parts, as set out in the rules. Actually, the MotoGP Court of Appeal[18] had ruled that Ducati's aero spoiler, attached to the bottom of the swing arm of the three Desmosedici GP19s and used in the opening Moto GP race at Qatar, was legal. The decision of the Court means that the race result stands, and that Ducati can continue to use the spoiler going forward.

[18] The Moto GP Court of Appeal consists of three FIM judges, chosen from the governing body's international commission of judges; it must pronounce a decision within 4 weeks after the brief of appeal is received. Both the appellant/s and the respondent/s are by right parties of the proceeding, they must be represented by one defense counsel of their own choice and at their own expense. The appellant/s must be present, or duly represented, otherwise the protest will not be admissible, and the costs of the proceeding shall be borne by the appellant/s. The intervention of the FIM is, instead, optional and the decision left to the appreciation of its executive board. The hearing is public unless the Court decides otherwise in exceptional circumstances (it could be indeed the case of the proceeding in mention) and is conducted in one of the official languages of the FIM. The hearing is basically divided into two parts. Firstly, the parties involved are invited to state their respective cases, the witnesses being absent. Following, the Court hears the various witnesses and experts to complete the evidence. The parties as well as the Court have the right to question all witnesses and experts on their evidence. Once completed the evidence and after the hearing, in any case within the mentioned 4-weeks term after the brief of appeal is received, the Court decides in camera by a simple majority of votes of its three members; all members have equal voting rights and abstention is not permitted. The judgement has to be notified in writing, by registered letter with acknowledgement of receipt or by electronic mail, to all the parties concerned. From this time and date of receipt of the decision, the time limit of 5 days runs to lodge the appeal before the Court of Arbitration for Sports ('CAS') which is the body of third instance entitled to judge any appeal, according to the Regulations, against the decisions of the Moto GP Court of Appeal.

The MotoGP Court of Appeal's complete decision consisted in ruling that: the appeals filed by Team Aprilia, Team Suzuki, Team Honda and Team KTM are admissible; the provisional race results are confirmed and are declared as final; the request to declare the Device illegal and ban its use in future races is rejected. No appeal against this decision had been lodged before the Court of Arbitration of Sport (CAS) in Lausanne Switzerland.

4. Notes on the case final outcome.

The Moto GP Court of Appel had basically to decide whether the Ducati swingarm device was a tyre cooler, for which the use was approved by the FIM, or an aerodynamic device; in this second case, the device would not be permitted by the guidelines (and not the Regulations) which were provided to all the teams on 2nd of March by Technical Director Danny Aldridge.[19]

In the second scenario, the three riders subject to the proceeding could be disqualified and lose the points scored in the Qatar GP. Perhaps, the Moto GP Court of Appel could even decide in a 'Solomonic' way stating, for instance, that the devices would be banned from the next races. However, it wasn't so! In this contest, what it is noteworthy that the three appointed members of the Moto GP Court of Appel are not technicians; therefore, presumably, they could have little knowledge about the aerodynamic principles and devices. In order to avoid similar cases in the future, where the race final standing is decided in the following weeks in a courtroom rather than at the track, the FIM should find a way to deal with the anodyne situations inevitably inherent to technical regulations, given the highly competitive environment the FIM World Championship is. In this regard a good example could be provided by Formula 1 system currently in place, by means of which the borderline technological innovations – adopted by the teams and not expressly banned and/or contrary to the letter of the regulations in force – are allowed to be used for the remainder of the ongoing season; being it understood that, at the end of the season, where required, these borderline technological innovations will be double checked by the competent subjects in order to decide whether to allow their use in the next season or to ban them by mean of specific integration to the regulations.

Conclusions.

The case of study that we examined has as its object (although within a sports regulation) the assessment of compliance of an innovative component,

[19] See Asphalt Rubber, *Analyzing the Ducati Aero Appeal: The Process, The Future, Where the MSMA Goes from Here* [2019] in https://www.asphaltandrubber.com/motogp/ducati-aero-appeal-analysis-motomatters/; see also Motomatters.com (2019), *MotoGP Court Of Appeal Rules Ducati's Swing Arm Aero Spoiler Legal, Confirms Dovizioso As Qatar Race Winner*, in https://motomatters.com/news/2019/03/26/motogp_court_of_appeal_rules_ducati_s.html; see also Bike sport news, *MotoGP Argentina: Ducati swingarm device is 'Yamaha copy'* [2015] in https://www.bikesportnews.com/news/news-detail/motogp-argentina-ducati-swingarm-device-is-yamaha-copy.

the result of the most advanced technological development. It is a theme that is acquiring increasing interest also in the field of law. The paradigmatic example is perhaps the evolution of the product liability regulation.[20] In this context, we have witnessed a significant evolution of the criteria based on which the judge makes his own judgment on the product's compliance-safety. Originally, in fact, this judgment was made to the light of general criteria, the result of daily experience: the judge verified if the product was conceived and created in accordance with the 'state of art', 'to perfection', or 'in a workmanlike manner', according to a criterion of judgment widely marked by the impressions of the average man. Technological evolution has upset these settings. The modern discipline on the manufacturer's liability and product safety is flourishing widely on technical standards, that is, on technical disciplines that integrate the content of the law and assist the judge in the assessment of compliance-defectiveness.[21] In this context, the need for ever greater collaborations between lawyers and engineers is evident. In fact, technological development is achieved in increasingly accelerated times and now involves (in decisive terms) the new technologies of the digital world, generating new legal problems for which legal experts are called to give new answers. [22] In this perspective, analyzing cases of study such as the one proposed in this article is of extreme utility, because it allows us to verify the method of evaluating the technical-regulatory problems that the vertiginous innovation of the technology also proposes to the highest levels of the sports competition, with obvious reflections on the future of our mobility system.

[20] See P Machnikowski, *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies* (Intersentia, 2016); B Cappiello, *AI-systems and non-contractual liability. A European private international law analysis* (Giuffrè, 2022).
[21] See J L Contreras, *The Cambridge Handbook of Technical Standardization Law. Further Intersections of Public and Private Law* (Cambridge, 2019).
[22] See *The Europen Law Institute Draft of a Revised Product Liability Directive*, in https://www.europeanlawinstitute.eu.

Izzo L, 'Il difficile rapporto tra diritto alla privacy e dovere di contribuzione alla spesa pubblica' (2022) 2 EJPLT, 187-214.
DOI: https://doi.org/10.57230/EJPLT222LI

EJPLT
ISSN 2704-8012



Il difficile rapporto tra il diritto alla privacy e il dovere di contribuzione alla spesa pubblica.

The difficult relationship between the right to privacy and the duty to contribute to public expenditure.

LUIGI IZZO
PhD (c) in Humanities and Technologies: an integrated research path
Università Suor Orsola Benincasa

Abstract

Da tempo oramai nel nostro Paese si trascina una situazione incresciosa in tema di contrasto all'evasione e di riscossione dei carichi affidati alle Agenzie Fiscali. Da un lato è una patologia (ormai endemica) della società italiana, ma al contempo il fenomeno dell'evasione ha conosciuto una recrudescenza a causa dell'applicazione strettissima del diritto della privacy nei confronti dell'esercizio del potere di accertamento dell'imponibile da parte delle Agenzie Fiscali. Da qui la necessità di riscoprire la dicotomia tra diritti e doveri nel nostro ordinamento da cui potrebbe derivare un bilanciamento dei principi costituzionali più adeguato alle necessità reali del Sistema Paese.

For some time now, an unfortunate situation has been dragging on in our country with regard to the fight against tax evasion and the collection of debts entrusted to the Tax Agencies. On the one hand, it is a (now endemic) pathology of Italian society, but at the same time, the phenomenon of evasion has experienced a resurgence due to the very strict application of the right to privacy against the exercise of the tax assessment power by the Tax Agencies. Hence the need to rediscover the dichotomy between rights and duties in our legal system, from which a balance of constitutional principles more suited to the real needs of the Country System could be derived.

© The author(s) 2022, 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: privacy; riscossione fiscale; diritti e doveri; IA; big data; principi costituzionali; PNRR.

Summary: Introduzione: l'attuale situazione fotografata dalle Istituzioni. – 1. Il finanziamento della spesa pubblica tra aumento della pressione fiscale e contrasto all'evasione. – 2. L'evoluzione del sistema di accertamento fiscale alla luce del PNRR. – 2.1. Banche dati e *compliance*. – 2.2. La posizione del Garante della Privacy. – 2.3. I nuovi poteri di indagine. – 3. Uno spunto dalla Giurisprudenza della Corte Costituzionale. – 3.1. La Sent. N. 51/1992 e la riservatezza dei dati bancari. – 3.2. La Consulta e i "diritti tiranni". – 4. Gli orientamenti in sede europea e il principio di proporzionalità. – 5. La dicotomia tra diritti e doveri nella nostra Carta Costituzionale: riprendere un discorso lasciato in sospeso. – Conclusioni: "ri-bilanciare" il diritto alla privacy con il dovere di contribuzione e i principi solidaristici.

Introduzione: l'attuale situazione fotografata dalle Istituzioni.

In seguito all'audizione tenutasi il 7 aprile 2022 davanti alla Commissione parlamentare per l'attuazione del federalismo fiscale[1] è emerso un quadro desolante con riferimento all'attività di riscossione fiscale.

Pur sembrando, agli occhi di molti, rientrante nell'attività di routine, questa specifica audizione ha avuto una grande rilevanza.

Infatti, è bene riportare le esatte parole del Presidente della Commissione, l'On. Invernizzi:

"*L'ordine del giorno reca l'audizione, ai sensi dell'articolo 143, comma 2 del Regolamento della Camera, nonché ai sensi dell'articolo 5, comma 5 del regolamento della Commissione parlamentare per l'attuazione del federalismo fiscale, del direttore dell'Agenzia delle entrate, avvocato Ernesto Maria Ruffini, sull'assetto della finanza territoriale e sulle linee di sviluppo del federalismo fiscale. Faccio presente che l'avvocato Ruffini è accompagnato dal dottor Sergio Cristallo, direttore centrale coordinamento normativo dell'Agenzia delle entrate, e dal dottor Luigi Favè, direttore dell'Area riscossione dell'Agenzia delle entrate-riscossione. Per introdurre l'audizione odierna, sottolineo che la presenza dell'avvocato Ruffini permetterà alla Commissione di acquisire un importante bagaglio di informazioni e di elementi valutativi circa il ruolo svolto dall'Agenzia delle entrate nell'ambito del processo finalizzato alla piena attuazione del federalismo fiscale e dai principi di autonomia finanziaria delle regioni e degli enti locali. Potranno, pertanto, essere affrontati in questa sede molti dei delicati profili concernenti il complesso ambito di funzioni che afferiscono all'amministrazione dei tributi, a partire dalle competenze in materia di accertamento e riscossione, di controllo e verifica, di contrasto agli inadempimenti all'evasione, di contenzioso,*

[1] Al link https://webtv.camera.it/evento/20411 è disponibile la registrazione video (con sottotitoli in italiano) dell'audizione, mentre il relativo resoconto stenografico è raggiungibile al link https://www.camera.it/leg18/1058?idLegislatura=18&tipologia=audiz2&sottotipologia=audizione&anno=2022&mese=04&giorno=07&idCommissione=62&numero=0052&file=indice_stenografico

di assistenza ai contribuenti, di gestione del catasto e del patrimonio immobiliare, fino alle attività di consulenza e supporto tecnico, nonché di collaborazione e scambio di dati con il sistema delle autonomie per i servizi connessi al prelievo fiscale.".

Ebbene, già da ciò si evince come si intendesse affrontare, con una prospettiva a trecentosessanta gradi, la questione delle attività dell'Agenzia delle Entrate, tant'è che, dopo una lunga relazione dell'Avv. Ruffini sul complesso di operazioni finora portate avanti, durante il *question time* si sono seguite, l'una all'altra, domande molto rilevanti.

In particolare, l'On. Perosino ha chiesto di conoscere del "*[…] famoso magazzino fiscale, di cui abbiamo parlato in altre Commissioni, è una cosa delicata da vedere, è stato poi realizzato quel provvedimento di sistemazione contabile del magazzino fiscale che era a miliardi e che poi è stato, con un provvedimento, riportato alle vere posizioni? Non mi ricordo più. È un po' dove volevo arrivare, perché è stato interessante anche per noi commissari, di capire meglio come funziona ma, tutto sommato, credo che sia uno dei reparti dell'Amministrazione pubblica che ha fatto dei passi notevoli, soprattutto in termini di trasparenza, di chiarificazione e anche semplificazione.*".

A tale domanda la risposta del Direttore dell'Agenzia delle Entrate è stata la seguente:

"*Per quanto riguarda la questione del magazzino, io mi rifarei e mi fermerei alla relazione che il Ministro dell'economia delle finanze ha fatto al Parlamento nell'estate del 2021 dove ha sostanzialmente ripercorso tutta quanta la storia della motivazione, del formarsi del magazzino e del non riscosso, magazzino con non riscosso che continua ad aumentare evidentemente […]. In più, il magazzino di Agenzia entrate-riscossione si è arricchito […] e, quindi, diciamo possiamo poi, se ritenete, possiamo dare dati più specifici ma sicuramente abbiamo sfondato il tetto dei 1.100 miliardi non riscossi.*".

Quindi, non solo il complesso dei carichi non riscossi è in costante aumento, ma è stata superata la soglia dei 1.100 miliardi a livello nazionale.

Eppure, tale risultato non è certamente una sorpresa, dal momento che già la Corte dei Conti, evidenzia: "*Come si evince dai dati riportatati nella tavola che segue, a distanza di un ventennio dall'iscrizione a ruolo la percentuale delle riscossioni è inferiore al 30 per cento del carico netto. Dopo dieci anni dall'iscrizione le riscossioni non raggiungono il 15 per cento.*"[2]. La tabella in questione è la seguente, da cui si evince un andamento non certo lusinghiero dell'attività di riscossione finora svolta.

[2] CORTE DEI CONTI, SEZIONI RIUNITE IN SEDE DI CONTROLLO, *Rapporto sul coordinamento della finanza pubblica 2021*, pag. 139, disponibile al link https://www.corteconti.it/Download?id=867011ba-87e4-4e6b-8338-dd4874ff0b39

TAVOLA 1

CARICO AFFIDATO E CARICO RISCOSSO AL 2020

Anno affidamento del carico	Carico netto (affidato al netto di sgravi e sospensioni)	Totale riscosso dal 2000 al 2020	% riscosso su carico netto
2000	32.340,1	9.043,9	28,0%
2001	18.957,6	5.025,0	26,5%
2002	17.720,0	4.042,3	22,8%
2003	19.187,0	4.829,4	25,2%
2004	24.500,4	5.169,0	21,1%
2005	34.927,9	5.864,5	16,8%
2006	47.513,7	9.923,2	20,9%
2007	45.750,5	7.982,7	17,4%
2008	44.349,2	8.555,4	19,3%
2009	54.517,6	8.401,6	15,4%
2010	61.540,9	9.265,6	15,1%
2011	68.342,5	8.317,5	12,2%
2012	71.350,1	7.866,3	11,0%
2013	69.467,2	7.688,3	11,1%
2014	72.718,2	8.929,6	12,3%
2015	70.584,8	8.248,7	11,7%
2016	63.236,6	6.871,0	10,9%
2017	63.960,2	5.715,1	8,9%
2018	69.925,6	4.637,5	6,6%
2019	68.888,9	2.983,0	4,3%
2020	49.023,8	177,4	0,4%
Totale	**1.068.802,8**	**139.537,1**	**13,1%**

Fonte: Agenzia delle entrate-Riscossione

A ciò si aggiunga l'effetto derivante dalla presenza di un *tax gap* medio, inteso come il divario tra gettito teorico e gettito effettivo, che nell'ultimo Rapporto presentato dal MEF è pari, per il triennio 2016-2018 a circa 105,9 miliardi di euro, ripartiti in 94,3 miliardi di mancate entrate tributarie e 11,6 miliardi di mancate entrate contributive[3]. Vale a dire che, in media, per tre anni si sono avute mancate entrate per quasi 106 miliardi di euro, per complessivi 318 miliardi di euro.

Verissimo è, come risulta dai dati diffusi dal MEF[4], che nel periodo compreso tra il 2014 e il 2018 il *tax gap* si è ridotto in termini assoluti di circa 6,7 miliardi di euro ma è pur vero che tale riduzione rappresenta una goccia nel *mare magnum* delle mancate entrate considerate nel loro insieme. In più, risulta che se il *gap* di alcune imposte (IRES, IRAP e IVA) viene gradualmente a diminuire, d'altra parte sta crescendo il *gap* relativo all'IRPEF per specifici soggetti, in tal

[3] MINISTERO DELL'ECONOMIA E DELLE FINANZE, *Rapporto sui risultati conseguiti in materia di misure di contrasto all'evasione fiscale e contributiva anno 2021*, pag. 10, disponibile su https://www.finanze.gov.it/export/sites/finanze/.galleries/Documenti/Varie/Rapporto_evasione_2021_25-Settembre_2020.pdf

[4] MINISTERO DELL'ECONOMIA E DELLE FINANZE, *Relazione sull'economia non osservata e sull'evasione fiscale e contributiva anno 2021*, pagg. 16 ss., disponibile su https://www.finanze.gov.it/export/sites/finanze/.galleries/Documenti/Varie/Relazione-evasione-fiscale-e-contributiva_25_09_finale.pdf

modo frenando la riduzione del *tax gap* complessivo (che considera l'apporto derivante da tutte le imposte e tasse e contributi attualmente presenti nell'ordinamento).

Solo per operare una comparazione, si rapportino i 318 miliardi di euro di mancato gettito sia al costo dei provvedimenti urgenti varati dal Governo Draghi per fronteggiare la crisi economica derivante dalla guerra in Ucraina sia all'insieme della spesa pubblica delineata nel DEF, che viene annualmente presentato.

Pertanto, considerando l'effetto combinato dei carichi accertati e non riscossi e dei tributi non riscossi nella misura predeterminata per legge (vuoi per elusione, vuoi per evasione), emerge un panorama desolante per le finanze pubbliche ma anche per i singoli cittadini.

1. Il finanziamento della spesa pubblica tra aumento della pressione fiscale e contrasto all'evasione.

Però, prima di procedere oltre nella trattazione, va compreso come la spesa pubblica venga finanziata, al fine di erogare i servizi alla cittadinanza, così da chiarire il ruolo della tassazione in tal senso e il rapporto di questa con la spesa pubblica in sé.

Per meglio affrontare questo aspetto, è necessario capire *cosa sia* la spesa pubblica, ossia quale funzione abbia.

Ora, da un lato si è per lungo tempo considerata la spesa pubblica quale erogazione di risorse volte a finanziare le funzioni essenziali dello Stato, riducendo al minimo l'impatto sul mercato[5]. D'altra parte, però, la cd. "Grande Depressione" del biennio 1929-1930, unitamente alla sempre più vasta diffusione delle ideologie socialiste e marxiste, ha condotto a un intervento sempre più vasto dello Stato sul mercato, al fine di correggerne le storture, secondo una concezione keynesiana[6].

Ragion per cui, in verità, non sarebbe errato affermare che la spesa pubblica sia volta tanto a correggere l'andamento del mercato[7] quanto a espletare le funzioni tipiche di uno Stato.

Le due componenti funzionali della spesa pubblica sarebbero, invero, complementari.

Tuttavia, a prescindere dalla concezione adottata, è necessario che la spesa pubblica raccolga preliminarmente le risorse economiche necessarie.

E, al contempo, va considerato che tale spesa non può definirsi senza limiti, almeno non per lo Stato Italiano, dovendosi rispettare il principio del pareggio di bilancio cristallizzato nella nostra Carta Costituzionale[8], dove – giusto per ricordarlo – si pongono "paletti" non indifferenti alla possibilità di reperire

[5] Vedasi, per esempio, A. SMITH, *The Wealth of Nations*, 1937

[6] V. TANZI, L. SCHUKNECHT, *La spesa pubblica nel XX secolo - Una prospettiva globale*, Firenze University Press, 2007, pp. 7 ss., disponibile su https://media.fupress.com/files/pdf/24/650/650_19120

[7] Si ricordi il *whatever it takes* di Mario Draghi, che par quasi simboleggiare un superamento del *laissez-faire* che ha permeato a lungo il sistema economico in chiave neoliberale, un momento talmente iconico da indurre la Treccani a dedicarvi una voce nel Vocabolario online al link https://www.treccani.it/vocabolario/whatever-it-takes_%28Neologismi%29/

[8] Art. 81 Cost.

risorse mediante indebitamento[9].

Ciò ha comportato il venir meno di una delle modalità "tradizionali" per l'ottenimento dei fondi necessari al funzionamento della "macchina amministrativa"

Parimenti è impossibile sfruttare una qualsivoglia leva monetaria in perfetta autonomia, atteso che, in seguito all'adozione della Moneta Unica, la politica monetaria è stata accentrata a livello europeo, ponendola nelle mani della Banca Centrale Europea[10].

Quindi, venute meno sia la leva monetaria che la possibilità di indebitarsi, in un contesto europeo l'unica reale soluzione a disposizione dello Stato per poter finanziare la propria spesa (ovvero per rientrare da un debito pubblico eccessivo) è aumentare il livello di tassazione, andando a gravare direttamente sulla popolazione.

Ma nessuna di queste alternative è senza conseguenza!

Infatti, se la leva monetaria e il ricorso all'indebitamento comportano – ove usate eccessivamente – una forte esposizione alle fibrillazioni dei mercati finanziari, pure l'aumento della tassazione – se effettuato "indiscriminatamente" – conduce a una "esposizione" dello Stato.

Un'esposizione, però, nei confronti dei propri cittadini.

Ciò in quanto va ricordato che i tributi sono il corrispettivo che i cittadini versano per la prestazione di servizi pubblici. Ragion per cui, laddove questi servizi risultino inadeguati, si giunge facilmente a indurre all'evasione il contribuente stesso, il quale sarà più propenso a nascondere una parte – se non la totalità – del proprio reddito. Tale omessa dichiarazione, però, comporta a sua volta una diminuzione delle entrate fiscali e, quindi, delle risorse che possono essere destinate all'erogazione dei servizi.

Da ciò, a meno di non condurre a una *spending review* particolarmente drastica (si ricordino i tagli attuati dal Governo Monti ovvero quelli teorizzati da Cottarelli[11]), tale da far perdere fiducia nei confronti dello Stato, si arriva ad alzare ulteriormente la pressione fiscale, a un livello tale da incentivare l'evasione, che a sua volta conduce a un aumento della tassazione e così via.

Un meccanismo particolarmente distorto, quello del rialzo delle tasse (laddove effettuato senza combinarlo con altri strumenti), da condurre a una "evasione drogata", in cui si possono ricondurre sia quei contribuenti che – con gran danno per gli altri – hanno deciso di non pagare le tasse già quando erano più basse, sia quei contribuenti che, pur non volendo, non sono in grado di sostenere un simile livello di tassazione per ovvi limiti di reddito.

---

[9] Art. 81, co. 2 Cost.: *Il ricorso all'indebitamento è consentito solo al fine di considerare gli effetti del ciclo economico e, previa autorizzazione delle Camere adottata a maggioranza assoluta dei rispettivi componenti, al verificarsi di eventi eccezionali.* Sul punto, vedasi anche Corte Cost., Sent. n. 10/2015, che qualifica ormai l'equilibrio di bilancio quale principio fondamentale.

[10] Non solo: si consideri che già con i criteri sulla finanza pubblica fissati dal Trattato di Maastricht sono stati posti ulteriori limiti finalizzati a tenere sotto controllo:
1) il disavanzo pubblico (cioè la differenza tra le entrate e le uscite pubbliche) che non deve superare il 3% del PIL (rapporto indebitamento netto/PIL);
2) il debito pubblico che non deve superare il 60% del PIL (rapporto debito/PIL).

[11] Si rimanda all'intervento di Cottarelli all'evento "*La lista della spesa*", organizzato dalla Adam Smith Society a Milano, il 26 giugno 2015, disponibile al link https://www.adamsmith.it/wp-content/uploads/documenti/post0000428.pdf. Per quanto su alcuni punti una *spending review* possa essere più che sensata, laddove attuata senza utilizzare nessuna delle suddette "tre leve" di bilancio può risultare molto dannosa

Quindi, la soluzione per migliorare la situazione economica di uno Stato fortemente indebitato e caratterizzato da una elevata evasione sembrerebbe essere una combinazione di *spending review* e, soprattutto, di abbassamento delle tasse. Ciò, però, non farebbe altro che ridurre il numero assoluto di cittadini che possono permettersi un dato servizio (emblematico è il caso del sistema sanitario statunitense se rapportato a quello di molti Paesi europei), creando disparità e ulteriore sfiducia.

Ragion per cui, si pensa più a una riduzione delle tasse, senza accompagnarla con altre scelte di politica fiscale.

L'idea di ridurre le tasse per favorire la *compliance* dei cittadini troverebbe fondamento nella teorica della cd. "curva di Laffer", sulla base della quale sarebbe "*possibile individuare un livello soglia per l'aliquota fiscale t* tale da massimizzare il gettito derivante Tmax. Ulteriori incrementi dell'aliquota, oltre la soglia, risulterebbero dunque controproducenti […].*"[12].

Eppure, la mera diminuzione delle tasse, laddove non accompagnata da interventi "di fiancheggiamento" non pare affatto funzionare.

Non solo mancano prove a sostegno dell'equazione secondo cui "tasse basse=maggior gettito fiscale" e non pochi economisti sarebbero contro tale assunto[13], ma il Governo Trump, negli Stati Uniti, ha adottato una riforma del genere nel 2017 che, circa due anni dopo, ha portato a una diminuzione delle entrate fiscali[14], così trasformando il taglio della tassazione in una "riforma a perdere" se si considera il fabbisogno in termini di spesa pubblica.

Quindi, la prova è stata ottenuta, ma in senso contrario!

Ragion per cui, sul piano fiscale è necessario intervenire sulla condotta dei contribuenti, meglio se avviando un efficace sistema di accertamento ai fini della riscossione.

Ciò in quanto il comportamento del cittadino è influenzato da una serie di fattori. In particolare, si rilevi quanto segue:

"*The tax declaration decision is a decision under uncertainty. The reason for this is that failure to report one's full income to the tax authorities does not automatically provoke a reaction in the form of a penalty. The taxpayer has the choice between two main strategies: (1) He may declare his actual income. (2) He may declare less than his actual income. If he chooses the latter strategy his payoff will depend on whether or not he is investigated by the tax authorities. If he is not, he is clearly better off than under strategy (1). If he is, he is worse off. The choice*

---

[12] Voce *Laffer, curva di*, *Dizionario di Economia e Finanza*, Treccani, 2012, su https://www.treccani.it/enciclopedia/curva-di-laffer_%28Dizionario-di-Economia-e-Finanza%29/

[13] Nel 2012 la Booth School of Business di Chicago ha raccolto l'opinione di 40 economisti di fama internazionale – link https://www.igmchicago.org/surveys/laffer-curve/ - ponendo loro i seguenti quesiti: "*1) A cut in federal income tax rates in the US right now would lead to higher GDP within five years than without the tax cut.?*". Ovviamente, a questa domanda quasi tutti hanno risposto affermativamente. In fondo, con un taglio della tassazione non fa che aumentare la ricchezza dei singoli, che può essere investita secondo le inclinazioni e le scelte di questi. Quando, però, gli è stato chiesto "*A cut in federal income tax rates in the US right now would raise taxable income enough so that the annual total tax revenue would be higher within five years than without the tax cut?*", la totalità dei soggetti intervistati si è mostrata fortemente incerta oppure in disaccordo con una simile asserzione.

[14] J. TANKERSLEY, *It's Official: The Trump Tax Cuts Didn't Pay for Themselves in Year One*, 11/10/2019 disponibile su https://www.nytimes.com/2019/01/11/business/trump-tax-cuts-revenue.html

of a strategy is therefore a non-trivial one."[15]

Parimenti, va considerato che "*A final aspect is that individuals are motivated by a wide range of factors, including selfinterest (narrowly defined) but also by notions that arise more from group considerations, such as fairness, altruism, reciprocity, empathy, sympathy, trust, guilt, shame, morality, alienation, patriotism, social norms, social customs, social capital, tax morale, intrinsic motivation, and many other objectives.*"[16], con ciò ponendo fine all'assioma secondo cui una diminuzione dei tributi sia corrisposta necessariamente da un aumento delle entrate fiscali.

Per cui, da un lato è ben chiaro che un soggetto razionale – in assenza di controlli – deciderebbe di pagare il meno possibile. Ciò potrebbe essere vero in special modo laddove il soggetto abbia un reddito particolarmente alto, dal momento che si riterrebbe in grado di affrontare l'esborso per eventuali sanzioni e, quindi, penserebbe che sia conveniente affrontare il rischio in luogo del versare il dovuto.

D'altra parte, proprio la condotta dei propri consociati, eventuali "stimoli" esterni, ecc. sono tutti elementi in grado di influenzare l'agire di un individuo in senso negativo, inducendolo a tenere un comportamento *contra legem* anche nel caso in cui, magari, vi siano buone probabilità di essere scoperti dai funzionari preposti.

A questo punto, per forza di cose, si rende ineluttabile il ricorso a un sistema di accertamento fiscale più efficace, giacché scoraggerebbe il ricorso a "scommesse" (aumenterebbero le probabilità di venir perseguiti, piuttosto) e renderebbe meno diffusi e percepiti come meno "normali" fenomeni quali l'evasione e l'elusione fiscale, diminuendo la propensione del singolo ad "accodarsi" a una condotta negativa specifica.

Giustamente, con riferimento al caso specifico dello Stato Italiano, è indubitabile che sia necessaria una rimodulazione della tassazione se non una diminuzione delle aliquote.

Tuttavia, tralasciando per un momento il fatto che questo specifico punto non è oggetto del presente contributo, l'esperienza statunitense insegna come non sia possibile *solo* la riduzione delle tasse, senza accompagnarla con interventi volti a potenziare le capacità di indagine e di riscossione in capo alle Agenzie Fiscali e alla Guardia di Finanza[17].

Ciò riporta il discorso, inevitabilmente, all'attività di accertamento fiscale svolta in Italia.

---

[15] M. G. ALLINGHAM E A. SANDMO, *INCOME TAX EVASION: A THEORETICAL ANALYSIS*, in *Journal of Public Economics*, 1 (1972) 323-338, p. 324, disponibile al link http://www3.nccu.edu.tw/~klueng/tax%20paper/1.pdf

[16] J. ALM, *What Motivates Tax Compliance?*, in *Tulane Economic Working Paper Series*, Working Paper 1903 – aprile 2019, p. 16, disponibile al link http://repec.tulane.edu/RePEc/pdf/tul1903.pdf#page=17

[17] "*In questa prospettiva va studiata una revisione profonda dell'Irpef con il duplice obiettivo di semplificare e razionalizzare la struttura del prelievo, riducendo gradualmente il carico fiscale e preservando la progressività. Funzionale al perseguimento di questi ambiziosi obiettivi sarà anche un rinnovato e rafforzato impegno nell'azione di contrasto all'evasione fiscale.*". GOVERNO, *Le dichiarazioni programmatiche del Presidente Draghi*, 17 febbraio 2021, su https://www.governo.it/it/articolo/le-comunicazioni-del-presidente-draghi-al-senato/16225

2. L'evoluzione del sistema di accertamento fiscale alla luce del PNRR.

Ebbene, proprio in ragione del quadro desolante derivante da tali *report* e dell'impossibilità di agire solo con la riduzione della pressione fiscale in conseguenza degli aspetti sopra evidenziati, il contrasto all'evasione fiscale e la riduzione del *tax gap* sono stati considerati obiettivi prioritari nell'ambito del Piano Nazionale di Ripresa e Resilienza (d'ora in avanti PNRR), tant'è vero che la relativa riforma è considerata tra le cd. "Riforme abilitanti", ossia "*gli interventi funzionali a garantire l'attuazione del Piano e in generale a rimuovere gli ostacoli amministrativi, regolatori e procedurali che condizionano le attività economiche e la qualità dei servizi erogati;*"[18].

Ciò in quanto l'evasione fiscale è oramai riconosciuta come un elemento atto a:

- Danneggiare i contribuenti onesti, dal momento che si traduce in una minor qualità dei servizi erogati dalla P.A., dovuta a tagli alla capacità di spesa per finanziarli, nonché in un aumento del livello di tassazione, poiché in presenza di evasione fiscale e di aumento del fabbisogno di spesa pubblica si tende più ad aumentare la pressione fiscale anziché ridurla;
- Danneggiare il sistema di concorrenza all'interno dei mercati, atteso che le imprese oneste si ritrovano concorrenzialmente meno competitive rispetto a quelle che eludono o evadono la tassazione, in quanto queste ultime dispongono di maggiori capitali;
- Danneggiare le prospettive di crescita economica, poiché la minor qualità dei servizi erogati alle imprese non consente di sfruttare appieno il potenziale delle stesse.

Proprio la considerazione degli effetti – negativi – dell'evasione ha condotto a ripensare l'approccio complessivo, con un maggior ricorso alle nuove tecnologie, scelta peraltro premiata dall'Unione Europea[19] e dai risultati in tema di accertamento e riscossione ottenuti nei primi sette mesi del 2022[20].

2.1. Banche dati, *compliance* e poteri.

Uno dei punti su cui maggiormente si è concentrata l'attività delle agenzie fiscali in seguito alla svolta impressa sotto il Governo Renzi con la Legge di Stabilità 2015[21] è senza dubbio quello di favorire l'adempimento spontaneo dei contribuenti e porre le basi per una effettiva *compliance* (ossia collaborazione) tra questi e le agenzie fiscali.

In quell'occasione si è messa in evidenza l'opportunità di utilizzare i dati presenti nella cd. "super anagrafe" dei conti correnti attivata con il Decreto

---

[18] GOVERNO ITALIANO, *Piano Nazionale di Ripresa e Resilienza*, pag. 35, disponibile su https://www.governo.it/sites/governo.it/files/PNRR.pdf

[19] AGENZIA DELLE ENTRATE, *Via libera della UE al finanziamento del progetto dell'Agenzia delle Entrate. In campo Intelligenza Artificiale, network science e data visualization. Oltre tre miliardi di dati per intercettare la rete delle frodi e favorire l'adempimento spontaneo*, Comunicato stampa del 4 marzo 2021, su https://www.agenziaentrate.gov.it/portale/web/guest/-/comunicato-del-4-marzo-2021-audizione

[20] MINISTERO DELL'ECONOMIA E DELLE FINANZE, *Entrate tributarie: nei primi sette mesi dell'anno gettito pari a 288 miliardi*, Comunicato Stampa N° 156 del 05/09/2022, su https://www.mef.gov.it/ufficio-stampa/comunicati/2022/Entrate-tributarie-nei-primi-sette-mesi-dellanno-gettito-pari-a-288-miliardi/.

[21] Art. 1, co. 634-637, l. n. 190/2014

Legge n. 201/2011. Infatti, ai sensi dell'art. 11, co. 2 ss., gli operatori finanziari sono obbligati a comunicare periodicamente all'anagrafe tributaria le movimentazioni sui conti correnti e l'Istituto Nazionale della previdenza sociale deve fornire all'Agenzia delle entrate ed alla Guardia di finanza i dati relativi alle posizioni di soggetti destinatari di prestazioni socio-assistenziali. Ciò al fine di far emergere l'imponibile e di consentire una più efficace valutazione del rischio di evasione.

In questo stesso senso si è mossa la Legge di Bilancio 2020, presentata in una ottica di potenziamento dell'accertamento, dal momento che, nelle intenzioni del Legislatore, l'Agenzia delle Entrate e la Guardia di Finanza avrebbero potuto interconnettere i dati presenti nell'archivio dei rapporti finanziari con quelli di altre banche dati a loro disposizione al fine di far emergere criteri ulteriori e idonei allo svolgimento di una analisi di rischio[22], a mezzo della quale individuare eventuali posizioni a rischio da sottoporre poi ad accertamento.

Ciò al fine di "invogliare" alla *compliance*.

Dati che, in verità, vengono costantemente alimentati anche dal sistema di *fatture elettroniche* [23] , i cui files sono memorizzati fino al 31 dicembre dell'ottavo anno successivo a quello di presentazione della dichiarazione di riferimento ovvero fino alla definizione di eventuali giudizi, al fine di essere utilizzati:

a) dalla Guardia di finanza nell'assolvimento delle funzioni di polizia economica e finanziaria di cui all'articolo 2, comma 2, del decreto legislativo 19 marzo 2001, n. 68;

b) dall'Agenzia delle entrate e dalla Guardia di Finanza per le attività di analisi del rischio e di controllo a fini fiscali.

Attività da svolgere, invero, sentito il Garante per la protezione dei dati personali e adottando idonee misure di garanzia a tutela dei diritti e delle libertà degli interessati[24].

Proprio questa necessità di sentire il Garante in plurime occasioni ha condotto, più recentemente, a una novella legislativa volta a non "intralciare" l'esecuzione delle riforme del PNRR.

Infatti, con il D.L. n. 139/2021, si è prevista l'abrogazione del terzo comma dell'art. 22, d.lgs. n. 101/2018 [25] , il quale, a sua volta, ha comportato l'abrogazione dell'intero art. 2 *quinquiesdecies* del D.L. n.196/2003[26].

---

[22] Per il testo originale del DDL n. 1586, vedasi al link https://www.senato.it/japp/bgt/showdoc/18/DDLPRES/0/1125303/index.html?part=ddlpres_ddlpres1-altro_altro2

[23] D.lgs. n.127/2015

[24] Vedasi comunicato stampa dell'Agenzia delle Entrate del 30 giugno 2021 al link https://www.agenziaentrate.gov.it/portale/web/guest/-/cs-30-giugno-2021-memorizzazione-fatture

[25] Si riporta il testo ante abrogazione: "*3. Sino all'adozione dei corrispondenti provvedimenti generali di cui all'articolo 2-quinquiesdecies del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, i trattamenti di cui al medesimo articolo, già in corso alla data di entrata in vigore del presente decreto, possono proseguire qualora avvengano in base a espresse disposizioni di legge o regolamento o atti amministrativi generali, ovvero nel caso in cui siano stati sottoposti a verifica preliminare o autorizzazione del Garante per la protezione dei dati personali, che abbiano individuato misure e accorgimenti adeguati a garanzia dell'interessato.*"

[26] Si riporta il testo ante abrogazione: "*Trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico. 1. Con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'articolo 35 del Regolamento, il Garante può, sulla base di quanto disposto dall'articolo 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale*

Queste, invero, erano proprio le norme che fondavano maggiormente il potere di intervento del Garante della Privacy nei confronti delle Pubbliche Amministrazioni.

A tale novella si è aggiunta la previsione, sempre nel D.L. n. 139/2021, di cui all'art. 9, co. 3, in base alla quale il Garante ha un termine di 30 giorni per trasmettere i pareri richiesti con riferimento alle riforme previste nell'ambito del PNRR, trascorsi i quali le P.A. sono autorizzate ad agire autonomamente, anche in assenza di tali pareri.

2.2. La posizione del Garante della Privacy.

In tema di contrasto all'evasione e di utilizzo delle banche dati, invero, la posizione del Garante è ben nota e in linea con il suo "mandato"[27].

In primo luogo, si consideri la questione della cd. "super anagrafe". Sul punto, l'Agenzia delle Entrate aveva richiesto un parere in data 12 marzo 2012, relativo allo schema di provvedimento del Direttore dell'Agenzia in materia di *"Disposizioni di attuazione dell'articolo 11, commi 2 e 3, del decreto legge 6 dicembre 2011 n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011 n. 214. Comunicazione integrativa annuale all'archivio dei rapporti finanziari"*.

In un primo momento il Garante ha risposto con provvedimento n. 145/2012 [28], evidenziando preliminarmente che "*L'accesso all'archivio dei rapporti finanziari è, allo stato, previsto per le indagini finanziarie da parte dell'Agenzia delle entrate e della Guardia di finanza (art. 32, comma 1, n. 7, del d.P.R. 29 settembre 1973, n. 600 e art. 51, comma 2, n. 7 del d.P.R. 26 ottobre 1972, n. 633), oltre che per le ulteriori finalità di cui all´art. 7, comma 11, del d.P.R. n. 605 del 1973. Una volta acquisite tali informazioni sui rapporti finanziari, i soggetti legittimati possono richiedere attraverso un'apposita procedura telematica tutti i dati di dettaglio direttamente agli operatori finanziari presso i quali i contribuenti sono stati censiti.*".

Poi, ha evidenziato le criticità insite, sul piano soprattutto organizzativo e della concentrazione dei dati, dall'attuazione del piano di "accesso automatizzato" all'anagrafe dei rapporti finanziari, specialmente in considerazione del fatto che già allora risultavano "*circa 600.000.000 (seicento milioni) di rapporti attivi e che annualmente gli operatori finanziari effettua*(va)*no circa 155.000.000 (centocinquantacinque milioni) di comunicazioni relative alle sole variazioni dei rapporti in essere e alle c.d. operazioni extraconto.*".

Tuttavia, pur comprendendo le preoccupazioni del Garante, va evidenziato che l'accesso all'archivio per i fini delle indagini finanziarie di cui sopra è previsto nei confronti di soggetti o gruppi di soggetti già sottoposti ad accertamenti e, quindi, individuati.

Ragion per cui, il richiamo a tale disciplina potrebbe essere poco adeguato,

---

adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare."

[27] C. LAUDANNA, *Norme privacy in rapporto alla lotta all'evasione fiscale*, in *Data Protection Law*, n. 1/2021, p. 34 ss., su https://www.dataprotectionlaw.it/wp-content/uploads/2021/01/RIVISTA-1_2021.pdf

[28] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Comunicazione dei dati contabili all'anagrafe tributaria da parte di banche e operatori finanziari: parere all'Agenzia delle entrate sulle modalità di trasmissione e di conservazione dei dati*, provv. N. 145/2012, disponibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1886775

se si tiene in conto l'obiettivo sotteso all'evoluzione della disciplina in materia di contrasto all'evasione, volta a individuare più rapidamente i soggetti a rischio (soprattutto evitando di allertarli).

Proprio in considerazione di tale necessità – sempre più stringente se si considera anche l'ammontare del non riscosso – si è giunti all'approvazione del provvedimento dell'Agenzia delle Entrate, sia pur richiedendo una grande prudenza nell'adozione delle misure tecniche e organizzative per la gestione dei dati, nonché in relazione alla definizione dei criteri di valutazione di detti dati, di modo da evitare un processo decisionale fondato unicamente su un trattamento automatizzato dei database.

Quindi, si può dire che effettivamente il Garante abbia dato un "sì a denti stretti"[29], espresso anche nei confronti del Provvedimento dell'Agenzia delle Entrate relativo alla "*Partecipazione all'accertamento fiscale e contributivo da parte dei Comuni*" [30], il quale aveva sollevato – di fatto – le medesime perplessità.

Tuttavia, non può esser trascurato che il contrasto all'evasione deve oramai essere "multilivello" e attuato in tempi rapidi, con la conseguenza che è inevitabile il coinvolgimento di numerosi soggetti in relazione alle attività di accertamento fiscale. Ciò anche a costo di accettare rischi molto grandi dovuti alla diffusione di dati personali, cui si può porre rimedio solamente con una previa sperimentazione delle procedure di analisi e trattamento[31].

Con riferimento, poi, all'interconnessione tra le banche dati introdotta con la legge di bilancio 2020, ha affrontato una analisi dell'art. 86 del DDL[32], poi rivisto in relazione proprio alle osservazioni presentate dal Garante.

I punti critici erano, sostanzialmente, due:

1) La Guardia di Finanza sarebbe stata sostanzialmente parificata all'Agenzia delle Entrate, duplicando i ruoli e, quindi, il trattamento dei dati;
2) La pseudonimizzazione non sarebbe stata sufficiente a fornire adeguata tutela ai dati personali, i quali rivestono tale caratteristica non solo quando consentano una diretta identificazione di un soggetto, ma anche

---

[29] A. CHERCHI, *Super-Anagrafe troppo invasiva*, disponibile su https://st.ilsole24ore.com/art/norme-e-tributi/2012-04-19/superanagrafe-troppo-invasiva-064149_PRN.shtml

[30] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Partecipazione all'accertamento fiscale e contributivo da parte dei Comuni: parere del Garante sul nuovo provvedimento dell'Agenzia delle entrate - 17 aprile 2012*, provv. N. 144/2012, disponibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1886825

[31] Infatti, per ben due volte l'Agenzia delle Entrate si è interfacciata con il Garante per sperimentare sistemi di analisi volti a un più efficace e corretto utilizzo dei dati ottenuti. Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sperimentazione di una procedura basata sull'utilizzo di informazioni fornite dall'Archivio dei rapporti finanziari e degli elementi presenti nell'Anagrafe tributaria per l'individuazione di profili di evasione rilevanti - 20 luglio 2017*, provv. N. 321/2017, disponibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/6843736 nonché GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul provvedimento del Direttore dell'Agenzia delle entrate recante "Disposizioni di attuazione dell'articolo 11, comma 4, del DL 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214, e successive modificazioni. Analisi del rischio di evasione. Estensione all'anno 2014-2015 della sperimentazione della procedura di selezione basata sull'utilizzo delle informazioni comunicate all'Archivio dei rapporti finanziari - 14 marzo 2019*, provv. N. 58/2019, disponibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9106329

[32] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Memoria del Presidente dell'Autorità garante per la protezione dei dati personali sul disegno di legge di bilancio 2020*, 12/11/2019, disponibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9184376#:~:text=86

nel caso in cui permettano di identificarlo indirettamente.

Oltre a ciò, è stato stigmatizzata anche la previsione del secondo comma dell'art. 86 del DDL, che "*ricomprende gli interessi tutelati in base alla disciplina in materia di prevenzione e contrasto dell'evasione fiscale tra i presupposti che, ai sensi dell'art. 2-undecies del d.lgs. n. 196 del 2003 e successive modificazioni, recante il Codice in materia di protezione dei dati personali (di seguito: Codice), consentono di limitare o escludere l'esercizio dei diritti dell'interessato, riconosciuti dalla normativa in materia di protezione dati personali e, in particolare, dal Regolamento.*", scelta effettivamente in contrasto con il principio di proporzionalità, con lo Statuto dei diritti del contribuente e con gli orientamenti della giurisprudenza amministrativa in materia di trasparenza e accesso ai documenti detenuti dalla P.A., tendenti ad allargare quanto più possibile il diritto di accesso ex l. 241/90 e atti connessi[33].

Tuttavia, il fatto che questa scelta possa pregiudicare l'azione amministrativa e di riscossione – non ha avuto torto il Garante a temere che l'accertamento potesse essere effettuato sulla base di dati eventualmente errati – non vale ad escludere che sia necessario porre a sistema le banche dati, anche accettando il rischio di trattamenti non conformi, pena l'inutilità pratica di quegli stessi dati[34].

Può essere poi ben noto il rischio di *data breach*[35] come pure l'esistenza di una tendenziale inadeguatezza del sistema di accertamento in termini di

---

[33] Si pensi, per esempio, alle decisioni del Consiglio di Stato, che ha più volte aperto alle varie forme di accesso, declinandole nel senso più ampio possibile, specialmente laddove tale accesso sia strumentale ad esigenze difensive. Ancora, in tema di accesso agli atti dell'anagrafe tributaria, vedasi Cons. Stato, Ad. Plen., Sent. n. 19/2020, i cui insegnamenti impongono di considerare il diritto all'accesso come vero e proprio principio dell'ordinamento. Più recentemente, vedasi anche Cons. Stato, Sent. n. 6964/2021 per una espansione ulteriore del diritto di accesso agli atti tributari rispetto alle esigenze di tutela della riservatezza. A tal punto una questione, però, sorge spontanea: ma se viene consentito l'accesso agli atti fiscali altrui per esigenze, ad esempio, di difesa – che, attenzione, è tra i diritti da garantire in via prioritaria – per quale ragione non si dovrebbe consentire ampiamente un diritto – questa volta allo Stato – a trattare nel miglior modo possibile tali dati, così da consentire un effettivo contrasto all'evasione? Forse che questo "diritto" dello Stato è di "serie B" rispetto a quello del singolo contribuente? Partendo da questa giurisprudenza, però, il Garante della Privacy, nel corso di una audizione davanti alla Commissione parlamentare di Vigilanza sull'Anagrafe Tributaria, ha affermato che "*In ogni caso, prima di ipotizzare qualsiasi ampliamento del patrimonio informativo dell'amministrazione finanziaria, il legislatore dovrebbe tenere in considerazione anche il fatto che, in base alla costante giurisprudenza del Consiglio di Stato, le dichiarazioni, le comunicazioni e gli atti acquisiti dall'Agenzia delle entrate, contenenti dati reddituali, patrimoniali e finanziari, ed inseriti nelle banche dati dell'anagrafe tributaria, ivi compreso l'archivio dei rapporti finanziari, costituiscono documenti amministrativi e sono, quindi, soggetti all'accesso di cui agli artt. 22 e ss. della legge n. 241/1990 da parte di chiunque ne abbia interesse. Ne deriva una potenziale, significativa esposizione della sfera privata laddove i dati nella disponibilità dell'amministrazione finanziaria non risultino necessari al perseguimento, in concreto, dell'interesse pubblico sotteso al trattamento.*" (il testo completo dell'audizione è disponibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9678216)

[34] In tema di accesso agli atti tributari vedasi anche F. SERGIO, *Riflessioni sul diritto d'accesso agli atti tributari: la dialettica fra la tutela della privacy del contribuente ed il perseguimento dell'interesse fiscale dell'amministrazione finanziaria*, in *European Journal of Privacy Law and Technologies*, n. 1/2022, su https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1557/1099

[35] CENTRO STAMPA DEL GARANTE, *Evasione fiscale, la privacy non frena il contrasto - Intervista ad Antonello Soro*, 18 novembre 2019, tratto da *Il Sole 24 Ore*, disponibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9188282. Vedasi anche il caso di una ventina di funzionari infedeli dell'Agenzia delle Entrate belga (SPF Finances), indagati per aver trafugato dati personali dei contribuenti al fine di rivenderli ad un'agenzia di investigazioni private e ad un'altra società a questa collegata – cfr. B. SAMYN, *Procès à Liège: des fonctionnaires des Finances volaient et revendaient des informations sur des contribuables*, 04/09/2020, disponibile al link https://www.rtl.be/info/belgique/faits-divers/proces-a-liege-des-fonctionnaires-des-finances-volaient-et-revendaient-des-informations-sur-des-contribuables-1242037.aspx?dt=19:20 .

risorse umane, tecniche ed economiche. Può anche darsi che la raccolta di tutti i dati presenti nelle fatture elettroniche [36] possa presentare di per sé un indubbio rischio per la privacy dei contribuenti, atteso che viene memorizzata anche la descrizione dell'operazione oggetto di fatturazione.

Eppure, tutti questi elementi non necessariamente possono essere invocati a paralizzare l'azione di accertamento, quasi come a fare applicazione di un principio di "precauzione totale" quasi allo stesso livello di quello che ha governato la gestione della pandemia nel corso del 2020.

Anzi, per converso, proprio la descrizione delle operazioni fatturate, combinata con la limitazione dell'uso del contante, può aiutare ad affinare gli algoritmi di ricerca delle Agenzie Fiscali e portare alla luce il sommerso.

Infatti, si ipotizzi che il contribuente Tizio, con un reddito mensile netto *dichiarato* di 1.800,00 euro, sostenga spese voluttuarie per una percentuale pari al – si ipotizza – 75% del totale. Al contempo dai dati fiscali risulta una famiglia a suo carico, ecc. Se un reddito simile viene al 75% consumato in spese non afferenti alla famiglia e non risultano altre fonti di reddito per la stessa, sarà difficile immaginare che quel contribuente abbia effettivamente dichiarato appieno il suo reddito.

Sembra, quindi, che nell'ottica di una precauzione "paralizzante", il Garante sia più propenso ad evidenziare i rischi di una data condotta anziché i benefici della stessa. Tuttavia, così facendo, non solo si limita il potenziale delle Autorità fiscali ma si introduce anche una forte disparità di trattamento tra i contribuenti che siano pubblici dipendenti – funzionari, dirigenti, impiegati, docenti, militari, ecc. – e i contribuenti privati e le persone giuridiche, che hanno modo di "non dichiarare" il dovuto.

E proprio per tale ragione, in un ideale eterno ritorno dell'infinito, si ripropone l'impossibilità di ridurre il carico fiscale, di cui non pochi beneficerebbero.

Non sorprende, quindi, che in vista dell'attuazione del PNRR, si sia deciso di limitare fortemente l'ambito di operatività del Garante[37]. Anzi, non sarebbe errato affermare che proprio il Garante, assieme ai TAR, sia uno di quegli attori che più condizionano – spesso in senso limitante – l'azione della P.A.[38].

2.3. I nuovi poteri di indagine a seguito degli ultimi sviluppi.

Quindi, l'AdE e la GdF, in forza delle ultime novelle normative, hanno la possibilità tanto di accedere – pressoché senza limiti – ai dati contenuti nella superanagrafe dei conti correnti ma anche, in caso di necessità e tramite apposita procedura, ai dati di dettaglio depositati presso i soggetti da cui provengono i documenti che alimentano le banche dati.

---

[36] F. ME., *E-fattura, botta e risposta Soro-Gualtieri sulla privacy dei contribuenti*, 07/11/2019, disponibile al link https://www.corrierecomunicazioni.it/pa-digitale/e-fattura-monito-del-garante-troppi-dati-raccolti-gualtieri-privacy-tutelata/

[37] D. AQUARO, A. CHERCHI, *Meno poteri al Garante se la privacy si allinea al regolamento europeo*, in *Norme&Tributi Plus Enti Locali & Edilizia*, 29/11/2021, sulla banca dati Plusplus24

[38] Vale ricordare, in questa sede e con limitato riferimento al ruolo dei TAR in ambiti strategici, la recentissima sentenza del TAR Puglia, n. 1576/2022, relativa a un progetto PNRR, la cui progettazione tecnica è tuttavia ben risalente e di cui non si è considerata una differente variante presumibilmente proprio per evitare di dover riprogettare tutto, ponendo a rischio i fondi a causa delle lentezze che caratterizzano le consultazioni con il territorio.

Ancora, tra la superanagrafe e le altre banche dati si avrà una interoperabilità sempre più estesa e capillare[39], che consentirebbe di mettere "a sistema" una mole impressionante di dati.

In più, nel d.l. 26 ottobre 2019, n. 124, si consente all'Agenzia delle Entrate e alla Guardia di Finanza di utilizzare i dati contenuti nelle fatture elettroniche (art. 14) e si incentiva l'uso dei pagamenti elettronici (artt. 18-22).

Tutto ciò, invero, sarà ulteriormente alimentato dalle comunicazioni periodiche effettuate dagli intermediari nei confronti dell'Agenzia delle Entrate.

Questi *big data*, poi, saranno successivamente utilizzati per le analisi di rischio, da cui partire al fine di individuare eventuali incoerenze fra le movimentazioni e le giacenze finanziarie e i ricavi, volumi d'affari e redditi dichiarati.

In tal modo, sarà possibile stilare delle specifiche liste selettive di contribuenti, classificati secondo ben definiti indici di rischiosità fiscale, così da sottoporli a controllo ovvero invitarli all'adempimento spontaneo[40].

3. Uno spunto dalla Giurisprudenza della Corte Costituzionale.

Ebbene, delineato il quadro complessivo dei rapporti tra fisco e privacy sul piano normativo e in conseguenza degli "incontri" tra Governo, Agenzia delle Entrate e Garante Privacy, è doveroso affrontare la questione dal punto di vista della Carta Fondamentale dello Stato italiano.

Ciò in quanto entrambi gli aspetti fin qui affrontati – la tutela della privacy e la riscossione fiscale – trovano un ancoraggio a livello costituzionale, sia pure secondo opposte prospettive.

Da un lato si ha "*un diritto che trova riferimenti nella Costituzione italiana (artt. 2, 14, 15 Cost.), già riconosciuto, in relazione a molteplici ambiti di disciplina, nella giurisprudenza di questa Corte (sentenze n. 173 del 2009, n. 372 del 2006, n. 135 del 2002, n. 81 del 1993 e n. 366 del 1991)*" [41]. Diritto, quindi, non espressamente previsto – essendosi diffuso a livello sociale solo *dopo* la stesura della Carta Costituzionale – ma ricavabile in via interpretativa dalle disposizioni indicate dal Giudice delle Leggi.

A tale diritto, fa da contraltare il ben più che esplicito dovere generale di contribuzione previsto dall'art. 53 Cost., il quale dispone che "*Tutti sono tenuti a concorrere alle spese pubbliche in ragione della loro capacità contributiva. Il*

---

[39] Sul punto non sarebbe errato valersi della competenza dell'ISTAT, da *aggiungere* a quella della Guardia di Finanza e delle Agenzie Fiscali, atteso che "*Ad oggi, l'Istat utilizza oltre 30 archivi di dati fiscali provenienti dall'Agenzia delle Entrate, acquisiti tramite protocolli sicuri di trasmissione sulla base di una pianificazione annuale, che trova nel Piano Statistico Nazionale (PSN) e nei regolamenti statistici comunitari la principale fonte di liceità per il loro utilizzo a fini di produzione statistica ufficiale. Questi archivi vengono impiegati in modo intensivo ed integrato, e in particolare forniscono un input per la produzione statistica di ben 222 progetti statistici definiti nel PSN a titolarità Istat.*" – ISTAT, *Indagine conoscitiva sulla digitalizzazione ed interoperabilità delle banche dati fiscali - Audizione dell'Istituto nazionale di statistica, Dott. Massimo Fedeli*, 20/01/2021, pp. 17-18, disponibile al link https://www.istat.it/it/files//2021/10/Istat-Audizione-Commissione-anagrafe-tributaria_Camera-Deputati_20-ottobre-2021.pdf

[40] A. BONGI, *Archivio rapporti finanziari al centro delle attività di intelligence fiscale*, 27/12/2019, su https://www.ipsoa.it/documents/quotidiano/2019/12/27/archivio-rapporti-finanziari-centro-attivita-intelligence-fiscale

[41] Corte Cost., Sent. n. 20/2019

sistema tributario è informato a criteri di progressività.".

Ora, fermo restando che anche la Consulta valuta attentamente, caso per caso, le ipotesi in cui si deve decidere in merito al corretto esercizio della discrezionalità da parte del Legislatore[42], è utile accendere un faro su una giurisprudenza ben precisa della Corte, anche risalendo indietro nel tempo.

3.1. La Sent. N. 51/1992 e la riservatezza dei dati bancari.

Innanzitutto, laddove si intenda parlare di evasione e riservatezza, una pietra miliare da considerare è certamente la Sent. n. 51/1992, che ha condotto a una forte limitazione al segreto bancario[43] e che è stata posta a fondamento della giurisprudenza degli Ermellini[44].

Questa sentenza – che pare essere un *unicum* nel panorama costituzionale – prende le mosse da un accertamento della Guardia di Finanza. Per meglio comprendere la vicenda concreta che ha condotto al giudizio costituzionale, si riporta uno stralcio dal testo della decisione:

"*Il giudice a quo, in punto di rilevanza, precisa che, nell'ambito di un'ispezione, autorizzata dall'autorità giudiziaria, svolta ai fini dell'accertamento delle imposte sui redditi e sul valore aggiunto, la Guardia di finanza ha reperito documenti bancari, sulla cui base si è attivata un'indagine di polizia giudiziaria, anch'essa autorizzata dal giudice, nel corso della quale sono state acquisite notizie bancarie di rilievo pure per il predetto accertamento fiscale. Dopo che l'autorità giudiziaria titolare dell'indagine penale aveva autorizzato l'utilizzazione a fini fiscali delle notizie così acquisite, si è proceduto alla notifica dei relativi accertamenti, dalla cui opposizione ha avuto origine il giudizio a quo.*

A seguito di una specifica eccezione preliminare proposta dal ricorrente nel processo a quo, la Commissione tributaria di Pordenone ha sollevato questione di legittimità costituzionale dei citati artt.63 e 33, sospettando un vizio di questi ultimi per eccesso di delega rispetto all'art. 10, n. 12, della legge n. 825 del 1971, il quale contiene la direttiva rivolta al legislatore delegato di stabilire "l'introduzione, limitata a ipotesi di particolare gravità, di deroghe al segreto bancario nei rapporti con l'amministrazione finanziaria, tassativamente determinate nel contenuto e nei presupposti". Secondo il giudice a quo, con tale

---

[42] Si pensi, per esempio, alle diverse decisioni in tema di PMA – che hanno progressivamente demolito l'impianto originario della l. n. 40/2004 – o quelle in tema di rilancio dell'ILVA di Taranto. Con riferimento al sistema tributario, si segnala Corte Cost., Sent. n. 144/2005, laddove si censura l'irragionevolezza di una presunzione assoluta operante nell'ambito del sistema sanzionatorio volto al contrasto del lavoro irregolare. Ancora, vedasi Corte Cost. Sent. n. 111/1997 in tema di assoggettamento a ICI di cespiti solo immobiliari.

[43] Corte Cost. Sent. n. 51/1992, su https://www.giurcost.org/decisioni/1992/0051s-92.html?titolo=Sentenza%20n.%2051, menzionata molto brevemente in A. FANTOZZI, *La giurisprudenza della Corte Costituzionale in materia tributaria*, disponibile su https://www.giustizia-tributaria.it/allegati/AF-Corte_Costituzionale_definitivo.pdf

[44] Cass., Sez. Tributaria, Sent. n. 10573/2011 – "*Nei casi ivi in esame, sono state ritenuti legittimi gli accertamenti anche nel caso di conti correnti bancari o libretti di deposito intestati a familiari del contribuente, non potendosi ragionevolmente disconoscere la sussistenza di un identico interesse all'accertamento, in presenza di gravi, precisi e concordanti indizi circa la fittizia intestazione di tali conti, utilizzati al medesimo scopo di evasione fiscale (Cass. nn. 6232/2003, 8683/2002, 8826/2001). Ciò in conformità all'insegnamento (Corte. Cost. sent. n. 51/1992) che la tutela del segreto bancario non può spingersi fino a costituire ostacolo o intralcio all'attuazione di esigenze costituzionali primarie, come l'accertamento degl'illeciti tributari, costituenti ipotesi di particolare gravità in quanto rappresentano violazione di un dovere inderogabile di solidarietà.*"

disposizione il legislatore ha inteso sottolineare che il segreto bancario ha trovato, nell'ambito della riforma tributaria, uno specifico riconoscimento, nel senso che ha assunto valore di norma avente una precisa connotazione positiva e sistematica rispetto ad ogni attività ispettiva e di verifica posta in essere dall'amministrazione finanziaria.".

Secondo il giudice rimettente, sussisteva un eccesso di delega per le norme impugnate, in quanto "*dopo aver previsto che la Guardia di finanza coopera con gli uffici delle imposte per l'acquisizione degli elementi utili all'accertamento e alla repressione delle violazioni connesse con gli obblighi tributari, stabilisce che la stessa Guardia di finanza, "previa autorizzazione dell'autorità giudiziaria in relazione alle norme che disciplinano il segreto istruttorio, utilizza e trasmette agli uffici documenti, dati e notizie acquisiti nei confronti dell'imputato nell'esercizio dei poteri e facoltà di polizia giudiziaria e valutaria*".

Da ciò si riscontrerebbe un eccesso di delega, poiché, "*a fronte di una direttiva che esige deroghe al segreto bancario limitate a ipotesi di particolare gravità e tassativamente determinate nel contenuto e nei presupposti, essa sarebbe, invece, priva di ogni limite. Le deroghe ivi previste, infatti, sarebbero soggette al solo vincolo della previa autorizzazione dell'autorità giudiziaria, autorizzazione che, peraltro, non ha nulla a che vedere con considerazioni di indole tributaria, ma ha riguardo, piuttosto, all'event di mantenere integro il segreto istruttorio.*".

Posizione, quella avanzata dal giudice di merito, non condivisa dalla Corte Costituzionale, la quale, anzi, ribalta la prospettiva e – indirettamente – qualifica come incostituzionale l'ipotesi interpretativa fornita dal rimettente, dal momento che avrebbe condotto al paradossale risultato di ritenere la norma impugnata (laddove così interpretata) realmente in contrasto con la Costituzione e, precisamente, con gli artt. 2 e 53 Cost[45].

[45] Si riporta il passo dove viene effettuato il ragionamento dei giudici della Consulta, particolarmente rilevante: "*Interpretata nel contesto dei principi costituzionali ora menzionati, la disposizione della legge delega invocata come norma interposta nel presente giudizio di costituzionalità non può avere il significato ad essa attribuito dal giudice a quo. In altri termini, la norma direttiva contenuta nell'art. 10, n. 12, della legge n. 825 del 1971 - per la quale il legislatore delegato è tenuto a provvedere alla "introduzione, limitata a ipotesi di particolare gravità, di deroghe al segreto bancario nei rapporti con l'amministrazione finanziaria, tassativamente determinate nel contenuto e nei presupposti" - non può avere il significato di riconoscere il segreto bancario come principio anche nei confronti dell'autorità finanziaria procedente all'accertamento degli illeciti tributari, principio che può essere derogato soltanto nei casi, tassativamente determinati, di illeciti di particolare gravità. Se questo dovesse esserne il significato, si dovrebbe seriamente dubitare della legittimità costituzionale dell'art. 10, n. 12, della legge delega in riferimento ai principi costituzionali affermati negli artt. 2 e 53 della Costituzione e questa Corte non esiterebbe ad accogliere il suggerimento dell'Avvocatura dello Stato a sollevare di fronte a se stessa la questione di costituzionalità.*
In realtà, se la norma di delega dev'esser interpretata in armonia con la Costituzione e, più in particolare, con il principio che il dovere di riservatezza connesso con il segreto bancario non può coprire illeciti tributari e non può essere di ostacolo all'accertamento dei medesimi illeciti, l'art. 10, n. 12, non può essere visto come diretto a riconoscere il principio del "segreto bancario", di fronte al quale gli interventi dell'autorità pubblica volti all'accertamento degli illeciti tributari siano configurati come "deroghe eccezionali" e, persino, "sospette", tanto da esigere determinazioni tassative e limitate ai casi di maggior gravità.
In altri termini, alla riservatezza cui le banche sono tenute nei confronti delle operazioni dei propri clienti non si può applicare il paradigma di garanzia proprio dei diritti di libertà personale, poiché alla base del segreto bancario non ci sono valori della persona umana da tutelare: ci sono, più semplicemente, istituzioni economiche e interessi patrimoniali, ai quali, secondo la giurisprudenza costante di questa Corte, quel paradigma non è applicabile (v. sentt. nn.55 del 1968 e 22 del 1971).
Ciò significa che la stessa norma di delega non può essere interpretata come una norma restrittiva dei poteri di accertamento dell'amministrazione tributaria di fronte al segreto bancario, tanto più che, quando l'art. 10, n. 12,

Ciò conduce a violare sia uno dei principi più sacri della Costituzione – quello di solidarietà – sia uno dei doveri più caratteristici dell'essere un cittadino, ossia quello di contribuire alla spesa pubblica[46].

Non solo, tra le due violazioni – solidarietà e dovere di contribuzione – la Corte mostra di dare maggior peso alla prima:

"*Alla luce dei principi costituzionali, infatti, l'evasione fiscale costituisce in ogni caso una "ipotesi di particolare gravità", per il semplice fatto che rappresenta, in ciascuna delle sue manifestazioni, la rottura del vincolo di lealtà minimale che lega fra loro i cittadini e comporta, quindi, la violazione di uno dei "doveri inderogabili di solidarietà", sui quali, ai sensi dell'art. 2 della Costituzione, si fonda una convivenza civile ordinata ai valori di libertà individuale e di giustizia sociale.*".

Ne consegue che il contrasto finora delineato tra diritto alla privacy e dovere di contribuzione va rimeditato e considerato un contrasto tra *uno* dei tanti diritti riconosciuti al cittadino – che, come si vedrà, non può essere tenuto in tal considerazione al punto di farlo diventare un "diritto tiranno" – e uno dei *principi supremi dell'ordinamento*.

3.2. La Consulta e i "diritti tiranni".

Si è accennato, in chiusura del precedente paragrafo, al concetto di "diritto tiranno". Trattasi di postulato interessantissimo per la problematica in esame e, soprattutto, non nuovo per il panorama costituzionale nazionale[47], che si intreccia saldamente con i principi di ragionevolezza e proporzionalità[48].

Infatti, già nel 2012[49] la Consulta ricordava – in materia di rapporti con la Corte EDU – che la "*tutela dei diritti fondamentali deve essere sistemica e non frazionata in una serie di norme non coordinate ed in potenziale conflitto tra loro.*".

---

fa riferimento alle "ipotesi di particolare gravità" che legittimerebbero l'accesso degli uffici finanziari ai dati riservati custoditi dalle banche, non può non ricomprendere in quelle ipotesi tutti i possibili casi di illecito tributario per evasione."

[46] Dovere posto in risalto e in correlazione con la solidarietà anche nella successiva Corte Cost., Sent. n. 177/1992

[47] Vedasi l'intervista comparsa sul Corriere della Sera del 28 ottobre 2020 – in piena pandemia – a firma G. BIANCONI, titolata "*E' l'ora della solidarietà anche tra le istituzioni. Possibile ridurre i diritti, nel giusto equilibrio*" e disponibile al link https://www.cortecostituzionale.it/documenti/media_morelli/Morelli_Corriere_28_ottobre_2020.pdf. L'autore, intervistando l'allora presidente della Consulta Mario Morelli, chiedendo se il bilanciamento dei diritti in gioco è una regola che vale sempre, anche in situazioni di piena emergenza, riceve la seguente risposta: *"Certo, e comporta un piccolo sacrificio di tutti i valori in campo, perché non esistono "diritti tiranni". La Corte lo ha scritto, tra l'altro, nella sentenza sull'Ilva di Taranto, quando bisognava trovare un equilibrio tra il diritto alla salute, il diritto al lavoro, il diritto d'impresa: non ce n'è uno da tutelare in maniera integrale a discapito di altri, ma, in una situazione di conflitto, ciascuno può essere sacrificato, sia pure nella misura minima possibile, per consentire la tutela degli altri. Ciò vale anche nella difficilissima stagione che stiamo vivendo*".

[48] Si legga l'intervento di Marta Cartabia, all'epoca giudice della Corte Costituzionale, alla *Conferenza trilaterale delle Corte costituzionali italiana, portoghese e spagnola* del 24-26 ottobre 2013, disponibile al link https://www.cortecostituzionale.it/documenti/convegni_seminari/RI_Cartabia_Roma2013.pdf. L'autrice, prima ricorda che "*parlare di ragionevolezza e di proporzionalità equivale a parlare del lavoro quotidiano della Corte costituzionale. I giudizi di ragionevolezza e proporzionalità, infatti, attraversano – esplicitamente o implicitamente – un grande numero di questioni che giunge all'esame della Corte, nell'esercizio di ogni sua funzione."* (p. 1) e, poi, nel trattare del bilanciamento dei diritti quale ambito privilegiato di applicazione di simili principi, si riporta al concetto di "diritto tiranno", allora di freschissimo conio (p. 9) a seguito del deposito della pronuncia sul caso Ilva.

[49] Corte Cost., Sent. n. 264/2012

Successivamente, proprio con il caso Ilva, la Corte Costituzionale, molto chiaramente, enuncia il seguente postulato:

"*Tutti i diritti fondamentali tutelati dalla Costituzione si trovano in rapporto di integrazione reciproca e non è possibile pertanto individuare uno di essi che abbia la prevalenza assoluta sugli altri. La tutela deve essere sempre «sistemica e non frazionata in una serie di norme non coordinate ed in potenziale conflitto tra loro» (sentenza n. 264 del 2012). Se così non fosse, si verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe "tiranno" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette, che costituiscono, nel loro insieme, espressione della dignità della persona. […] La Costituzione italiana, come le altre Costituzioni democratiche e pluraliste contemporanee, richiede un continuo e vicendevole bilanciamento tra princìpi e diritti fondamentali, senza pretese di assolutezza per nessuno di essi. La qualificazione come "primari" dei valori dell'ambiente e della salute significa pertanto che gli stessi non possono essere sacrificati ad altri interessi, ancorché costituzionalmente tutelati, non già che gli stessi siano posti alla sommità di un ordine gerarchico assoluto. Il punto di equilibrio, proprio perché dinamico e non prefissato in anticipo, deve essere valutato – dal legislatore nella statuizione delle norme e dal giudice delle leggi in sede di controllo – secondo criteri di proporzionalità e di ragionevolezza, tali da non consentire un sacrificio del loro nucleo essenziale.*"[50].

Ora, partendo da tali insegnamenti, è possibile comprendere come una supposta "assolutezza" del diritto alla privacy come enucleato dal combinato disposto degli artt. 2, 13, 14, 15, 21 Cost. si ponga in diretto – e, per la verità, difficilmente accettabile – contrasto con i vari diritti riconosciuti dalla Carta Costituzionale[51], nonché con il principio di solidarietà ex art. 2 Cost. e con il dovere – inderogabile – di concorrere alle spese pubbliche di cui all'art. 53 Cost.

Paradossalmente, il diritto alla privacy, ove applicato senza bilanciarlo in considerazione della situazione storica, economica e sociale attuale, potrebbe essere considerato perfino come il diritto maggiormente "tiranneggiante" possibile, anziché essere quello più "tiranneggiato".

Ciò, ovviamente, nel caso in cui si consideri l'effetto complessivo di un dato diritto sull'intera società ed economia, invece di verificare l'effetto dello stesso per ogni singola partizione dei problemi che caratterizzano l'umana società.

[50] Corte Cost., Sent. n. 85/2013, richiamata in Corte Cost., Sent. n. 58/2018

[51] A titolo esemplificativo, si pensi al diritto alla difesa ex art. 24 Cost.: può funzionare l'amministrazione della giustizia senza che sia presente un apposito finanziamento nel bilancio dello Stato? Ovviamente no. E la mancanza di detti fondi – se rapportata alle esigenze dell'amministrazione giudiziaria – è palese nel caso in cui si pensa alle carenze di organico della Magistratura, con inevitabili impatti sui procedimenti in corso (cfr. L. MILELLA, *Mancano 1600 magistrati e i tribunali sospendono i processi*, su www.repubblica.it del 27 agosto 2022). Ancora, si può, in carenza di fondi, fornire appropriata tutela alla salute (art. 32 Cost.), all'istruzione (art. 34 Cost.), alla proprietà privata (in particolare vedasi artt. 42 e 43 Cost. in combinato disposto) oppure al risparmio (art. 47 Cost.)?

4. Gli orientamenti in sede europea e il principio di proporzionalità.

Nell'ambito della presente trattazione è imprescindibile riportare, sia pur brevemente, la posizione della giurisprudenza europea sul tema del rapporto tra il fisco e la tutela dei dati personali.

Già prima dell'avvento del GDPR la Corte di Giustizia UE si è espressa in merito al rapporto tra la tutela dei dati e il soddisfacimento di esigenze pubblicistiche, sia pure in materie non tributarie.

Essenziali sono le decisioni – che possono fungere quali coordinate interpretative – Digital Right Ireland[52] e Tele2 Sverige AB[53].

Entrambe hanno fatto uso del principio di proporzionalità per valutare la legittimità di una Direttiva europea – nel primo caso – e di un atto interno – nel secondo caso – in rapporto alla tutela dei diritti fondamentali dell'uomo e, in particolare, in relazione alla protezione della sua privacy[54].

In entrambi i casi la CGUE ha ritenuto che, pur essendo rilevanti le esigenze pubblicistiche sottese agli atti normativi contestati, l'ingerenza complessiva fosse sproporzionata rispetto al fine perseguito.

In tal modo, quindi, ha reso il principio di proporzionalità un assioma imprescindibile anche in tema di tutela dei dati in ambito pubblicistico, posizione successivamente confermata nell'ottobre 2020[55].

Tuttavia, ciò non significa certo che le banche dati fiscali non possano assolutamente acquisire e trattare dati personali dei contribuenti.

Anzi, in senso contrario la CGUE si è espressa con una sentenza afferente all'ambito tributario e relativa a un "*elenco di persone considerate dalla Direzione delle Finanze* (della Repubblica Slovacca) *dei prestanome, quale stabilito da quest'ultima ai fini della riscossione delle imposte e aggiornato a cura della Direzione delle Finanze medesima, delle autorità fiscali ad essa subordinate nonché dell'Ufficio Crimini dell'amministrazione finanziaria.*"[56].

---

[52] CGUE, Sent. 8 aprile 2014, Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a. Domande di pronuncia pregiudiziale proposte dalla High Court (Irlanda) e dal Verfassungsgerichtshof. Cause riunite C-293/12 e C-594/12, disponibile al link https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62012CJ0293

[53] CGUE, Sent. 21 dicembre 2016. Tele2 Sverige AB contro Post- och telestyrelsen e Secretary of State for the Home Department contro Tom Watson e a. Domande di pronuncia pregiudiziale proposte dal Kammarrätten i Stockholm e dalla Court of Appeal (England & Wales) (Civil Division). Cause riunite C-203/15 e C-698/15, disponibile al link https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62015CJ0203

[54] G. PALUMBO, *Fisco e Privacy – Il difficile equilibrio tra lotta all'evasione e tutela dei dati personali*, Pacini Giuridica, 2021, pp. 99 ss.

[55] CGUE, Sent. 6 ottobre 2020 (domande di pronuncia pregiudiziale del Conseil d'État e della Cour constitutionnelle – Belgio, Francia) – La Quadrature du Net (C-511/18 e C-512/18), French Data Network (C-511/18 e C-512/18), Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 e C-512/18), Igwan.net (C-511/18) / Premier ministre (C-511/18 e C-512/18), Garde des Sceaux, ministre de la Justice (C-511/18 e C-512/18), Ministre de l'Intérieur (C-511/18), Ministre des Armées (C-511/18), Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX / Conseil des ministres .Cause riunite C-511/18, C-512/18 e C-520/18, disponibile su https://curia.europa.eu/juris/document/document.jsf?text=&docid=235490&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=38742 .

[56] CGUE, Sent. 27 settembre 2017. Peter Puškár contro Finančné riaditeľstvo Slovenskej republiky e Kriminálny úrad finančnej správy. Domanda di pronuncia pregiudiziale proposta da Najvyšší súd Slovenskej republiky. Causa C-73/16, disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62016CJ0073

In tale decisione – si ricordi che non era ancora vigente il GDPR ma i principi ermeneutici sono ancora gli stessi – la CGUE ha ammesso la legittimità del trattamento dei dati ai fini del contrasto all'evasione[57], sia pur rispettando il principio di proporzionalità, in quanto l'inclusione negli elenchi a scopi fiscali potrebbe, per esempio, nuocere alla reputazione del singolo.

Pertanto, "*l'articolo 7, lettera e), della direttiva 95/46 deve essere interpretato nel senso che esso non osta a un trattamento dei dati personali da parte delle autorità di uno Stato membro ai fini della riscossione delle imposte e della lotta alla frode fiscale, come quello a cui si è proceduto con la redazione dell'elenco di cui al procedimento principale, senza il consenso delle persone interessate, a condizione, da un lato, che a tali autorità siano stati affidati compiti di interesse pubblico dalla normativa nazionale ai sensi di detta disposizione, la redazione di tale elenco e l'iscrizione in quest'ultimo del nome delle persone interessate siano effettivamente idonee e necessarie al raggiungimento degli obiettivi perseguiti e sussistano elementi sufficienti per presumere che le persone interessate figurino a ragione in tale elenco e, dall'altro lato, che siano soddisfatte tutte le condizioni di liceità di tale trattamento dei dati personali imposte dalla direttiva 95/46.*".

Nello stesso senso si pone una recentissima pronuncia, sempre della CGUE, ma successiva all'entrata in vigore del GDPR ed emessa nel febbraio 2022[58].

Nel caso di specie, l'amministrazione tributaria lettone aveva rivolto alla SS, una società fornitrice di servizi di annunci online, una "*richiesta di informazioni sulla base dell'articolo 15, paragrafo 6, della legge sulle imposte e sulle tasse, con*

---

[57] Si riportano i punti in cui risponde alla questione posta: "*Occorre esaminare la seconda questione alla luce della direttiva 95/46, nei limiti in cui, come risulta segnatamente dall'obiettivo di quest'ultima, stabilito al suo articolo 1, paragrafo 1, se sono soddisfatte le condizioni del trattamento legale dei dati personali imposte dalla direttiva medesima, detto trattamento è ritenuto conforme altresì ai requisiti di cui agli articoli 7 e 8 della Carta. 103 Come risulta dai punti 33 e 34 della presente sentenza, la redazione di un elenco quale l'elenco controverso, che contiene i nomi di talune persone fisiche e collega queste ultime a una o più persone giuridiche nelle quali tali persone fisiche rivestirebbero in modo fittizio funzioni direttive, costituisce un «trattamento di dati personali» ai sensi dell'articolo 2, lettera b), della direttiva 95/46. 104 Ai sensi del capo II della direttiva 95/46, intitolato «Condizioni generali di liceità dei trattamenti di dati personali», fatte salve le deroghe ammesse dall'articolo 13 di tale direttiva, qualsiasi trattamento di dati personali deve essere conforme, da un lato, ai principi relativi alla qualità dei dati enunciati all'articolo 6 di quest'ultima e, dall'altro, a uno dei principi relativi alla legittimazione del trattamento dei dati elencati all'articolo 7 della stessa direttiva (v. sentenza del 1o ottobre 2015, Bara e a., C-201/14, EU:C:2015:638, punto 30). 105 Occorre altresì ricordare che dall'obiettivo di garantire un livello di protezione equivalente in tutti gli Stati membri, perseguito da tale direttiva, deriva che l'articolo 7 di quest'ultima prevede un elenco esaustivo e tassativo dei casi in cui il trattamento dei dati personali può essere considerato lecito (v. sentenza del 24 novembre 2011, ASNEF e FECEMD, C-468/10 e C-469/10, EU:C:2011:777, punto 30). 106 In particolare, si deve rilevare che la lettera e) di detto articolo 7 stabilisce che il trattamento dei dati personali è lecito se «necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati». 107 Orbene, la redazione dell'elenco controverso può rientrare in suddetta disposizione.*

108 Risulta, infatti, che la riscossione delle imposte e la lotta alla frode fiscale, ai cui fini è stabilito l'elenco controverso, devono essere considerate compiti di interesse pubblico ai sensi della citata disposizione. 109 Incombe nondimeno al giudice del rinvio verificare se le autorità slovacche che hanno redatto tale elenco o quelle alle quali quest'ultimo è stato comunicato siano state investite di detti compiti dalla normativa slovacca. 110 A tal riguardo occorre osservare che l'articolo 6, paragrafo 1, lettera b), della direttiva 95/46 richiede che i dati personali siano rilevati per finalità determinate, esplicite e legittime. Come constatato dall'avvocato generale al paragrafo 106 delle sue conclusioni, l'obiettivo del trattamento dei dati personali è indissolubilmente collegato, nell'ambito di applicazione dell'articolo 7, lettera e), della direttiva 95/46, con i compiti affidati al responsabile del trattamento. L'attribuzione di detti compiti a quest'ultimo deve pertanto ricomprendere chiaramente l'obiettivo del trattamento in questione.".

[58] CGUE, Sent. 24 febbraio 2022. «SS» SIA contro Valsts ieņēmumu dienests. Domanda di pronuncia pregiudiziale proposta dalla Administratīvā apgabaltiesa. Causa C-175/20, disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62020CJ0175&qid=1670689194811

la quale invitava tale società a ripristinare l'accesso, di cui disponeva detta amministrazione tributaria, ai numeri di telaio dei veicoli oggetto degli annunci pubblicati sul portale Internet di tale società e ai numeri di telefono dei venditori, nonché a comunicarle, entro il 3 settembre 2018, informazioni sugli annunci pubblicati nel periodo compreso tra il 14 luglio e il 31 agosto 2018 nella rubrica di detto portale intitolata «Autoveicoli».

In tale richiesta si precisava che dette informazioni, le quali includevano il link all'annuncio, il testo di quest'ultimo, la marca, il modello, il numero di telaio e il prezzo del veicolo, nonché il numero di telefono del venditore, dovevano essere trasmesse per via elettronica, in un formato che consentisse di filtrare o selezionare i dati.

Inoltre, qualora l'accesso alle informazioni contenute negli annunci pubblicati sul portale Internet in questione non potesse essere ripristinato, si invitava la SS a indicarne il motivo e a comunicare, entro il terzo giorno di ciascun mese, le informazioni pertinenti sugli annunci pubblicati nel mese precedente.".

Tale richiesta, a prima vista, pareva porsi in contrasto con i principi di proporzionalità e minimizzazione nel trattamento dei dati personali.

Però, andavano considerati alcuni elementi:

1. la riscossione delle imposte e la lotta all'evasione fiscale devono essere considerate compiti di interesse pubblico ai sensi dell'articolo 6, paragrafo 1, primo comma, lettera e), del GDPR, riprendendo così quanto già affermato nella sentenza Puskar;
2. il fatto che tali dati siano raccolti senza che l'amministrazione tributaria lettone abbia dichiarato, nella richiesta stessa di informazioni, alcun limite temporale per siffatto trattamento non consentiva di ritenere che la durata del trattamento fosse sproporzionata rispetto all'obiettivo perseguito;
3. il titolare del trattamento non può raccogliere dati personali in modo generalizzato e indiscriminato e, in quell'occasione, aveva chiesto di ottenere dati relativi agli annunci di vendita di autoveicoli pubblicati sul suo sito Internet tra il 14 luglio e il 31 agosto 2018.

Ciò posto, per la CGUE le disposizioni del GDPR non ostano a che l'amministrazione tributaria di uno Stato membro imponga a un fornitore di servizi di annunci pubblicati su Internet di comunicarle informazioni relative ai contribuenti che abbiano pubblicato annunci in una delle sezioni del suo portale Internet, "*purché, segnatamente, tali dati siano necessari rispetto alle finalità specifiche per le quali sono raccolti e il periodo oggetto della raccolta di detti dati non oltrepassi la durata strettamente necessaria per raggiungere l'obiettivo di interesse generale perseguito*.".

Ciò considerato, si può comunque immaginare che, in un approccio *data-driven* che sia veramente efficace e pure rispettando i principi posti dalla CGUE nelle ultime statuizioni:

- i dati richiesti non possano essere pochi;
- il tempo necessario al trattamento possa esser limitato, ma sempre avendo riguardo alle tempistiche complessive per la fase dell'accertamento, quella della composizione dell'eventuale contrasto in sede giudiziaria/amministrativa e la fase della riscossione, materialmente parlando, del dovuto.

In caso contrario, applicando il principio di proporzionalità senza considerare le peculiarità delle attività fiscali, si viene a negare valenza stessa al concetto di proporzione, vanificando qualsiasi possibilità di porre rimedio a situazioni di illegalità che, per la società, sono pressochè inaccettabili.

Infatti, parlando in astratto qualsiasi dato è utilizzabile per il contrasto all'evasione e può, quindi, esser definito personale.

Ne consegue che potrebbe rivelarsi irragionevole pretendere che il Legislatore, per venire (forse eccessivamente) incontro ai timori ingenerati per la privacy, restringa la richiesta di dati solo ed esclusivamente ad alcune tipologie.

Per esempio, anche i dati presenti sul portale JuzaPhoto, un *forum* di fotografia, potrebbero essere utilizzati per individuare evasori.

Ciò in quanto è possibile capire, incrociando i metadati delle foto caricate sul *forum* con i dati relativi al valore di mercato delle macchine fotografiche e degli obiettivi e accessori, se un determinato soggetto sia o meno a rischio di evasione, allo stesso modo in cui si opera guardando al mercato automobilistico.

Si ipotizzi, per esempio, che Tizio abbia un reddito annuo dichiarato di 20.000,00 euro, viva da solo, senza altre entrate e abbia un profilo su JuzaPhoto.

Se dai dati di scatto delle foto risulta che questi adopera una Sony A9 II (valore di mercato sui 5.000,00 euro al 10/12/2022) con un obiettivo Zeiss Batis 18mm f/2.8 (valore di mercato sui 1.400,00 euro al 10/12/2022), per un totale di quasi 6.000 euro, già si può ipotizzare la necessità di qualche controllo.

Se poi dovesse risultare che utilizza addirittura un corredo Leica – del valore di migliaia e migliaia di euro – a quel punto il sospetto di trovarsi di fronte a un evasore diventa altissimo.

Allo stesso modo, ottenendo i dati dai social network – cosa che già si fa – è possibile valutare la compatibilità tra lo stile di vita del soggetto attenzionato e il reddito dichiarato. Per cui, se un tale che dichiari 20.000,00 euro annui, in un solo anno, fa un viaggio alle Maldive e uno a Cortina, di nuovo può essere tenuto in debita considerazione per futuri accertamenti.

Ma, senza questi dati, per minimizzare il più possibile l'impatto sulla privacy, è realmente possibile procedere ad attività di accertamento fiscale?

Ne consegue, quindi, la necessità di applicare gli orientamenti ermeneutici della CGUE di modo tale che abbiano un qualche impatto pratico in senso positivo per l'ordinamento giuridico e la società.

5. La dicotomia tra diritti e doveri nella nostra Carta Costituzionale: riprendere un discorso lasciato in sospeso.

In ultimo, tralasciando la questione del contrasto tra il diritto alla privacy e tutti gli altri diritti nonché quella del rapporto tra Stato e singolo cittadino che permea alcune disposizioni del GDPR, si dovrebbe riprendere il filo conduttore della dicotomia tra diritti e doveri a livello costituzionale[59].

[59] In tema di doveri vedasi R. GUASTINI, *Dovere giuridico* e A. CERRI, *Doveri pubblici*, in *Enciclopedia giuridica*, Treccani, 2002

Per quanto negli ultimi lustri si sia parlato – soprattutto a livello politico – dei diritti presenti nella nostra Carta, non si può dimenticare che la stessa disciplina i rapporti fondamentali che caratterizzano il cittadino tanto dal lato attivo – con i diritti – quanto dal lato passivo – con i doveri.

Non a caso i Padri Costituenti hanno rubricato la Parte I "Diritti e Doveri dei Cittadini" e proprio sull'art. 53 Cost. vi fu una discussione molto approfondita, specialmente ad opera dell'On. Scoca [60], che evidenziò le particolarità e le difficoltà nella gestione dell'attuazione dell'articolo così come proposto – e poi approvato – in sede costituente.

Invero, in quella sede, nella giornata del 23 maggio 1947, si discusse di proporzionalità e progressività del sistema tributario, in considerazione delle caratteristiche delle varie tipologie di imposte. Concetti che, tuttavia, rimangono lettera morta se non si procede a riorganizzare il sistema anche attraverso l'attività di accertamento.

Già l'On. Scoca, nel parlare di progressività, disse quanto segue:

"*L'onorevole Corbino ha detto che se dobbiamo attuare la progressività dobbiamo abolire le imposte speciali sui redditi per dirigerci verso l'imposta unica. Io direi che non è necessario far questo per applicare il principio della progressività, così come noi l'abbiamo inteso e come l'onorevole Presidente della Commissione lo ha illustrato. Basta capovolgere la situazione attuale del rapporto fra imposte reali e personali. Dicevo dianzi che oggi il nostro sistema tributario è imperniato principalmente sulle imposte dirette reali, ad aliquota proporzionale e che l'imposta complementare, che è l'unica imposta diretta di carattere progressivo, è comparativamente una ben minima cosa. Ma si può e, a mio avviso, si deve invertire questa situazione. Possiamo mantenere le imposte dirette reali (e si debbono mantenere, almeno come necessaria base di accertamento dell'imposta personale che colpisce il reddito complessivo del cittadino) purché si attui una riduzione notevolissima delle loro aliquote, e si determinino gli imponibili nella loro consistenza effettiva. Se ciò faremo, potremo potenziare l'imposta progressiva sul reddito e farla diventare la spina dorsale del nostro sistema tributario. Con l'alleggerire la pressione delle imposte proporzionali, che colpiscono separatamente le varie specie di redditi, avremo margine per colpire unitariamente e progressivamente il reddito globale. Per tal modo si potrà informare il nostro sistema fiscale al criterio della progressività senza far sparire le imposte reali e senza attuare la imposta unica, che sarebbe, almeno per ora, esperimento pericoloso.*"

Già allora si rese chiaro che, a prescindere dal sistema di tassazione adottato, un elemento imprescindibile era l'attività di determinazione della consistenza effettiva dell'imponibile.

Eppure, non sembra che la questione dei doveri costituzionali sia stata affrontata intensamente, quantomeno non negli ultimi anni, in cui pure si sono combattute battaglie politiche alquanto intense, tra *flat tax*, condoni e nuove ipotesi di tassazione.

[60] Vedasi per esempio Assemblea Costituente, Verbale della Seduta del 23/05/1947, pagg. 4202 ss. degli atti preparatori alla Costituzione, disponibile al link http://legislature.camera.it/_dati/costituente/lavori/Assemblea/sed130/sed130nc_4193.pdf

Per esempio, può rendersi necessario risalire al 2006 per trovare gli atti di un evento specificamente impostato sul concetto di "dovere costituzionale"[61].

In quella sede diversi relatori trattarono sotto diversi profili proprio la questione del dovere di contribuzione ex art. 53 Cost.

È così che, per esempio, BASCHERINI[62], MARZUILLO e WOJTEK PANKIEWICZ hanno chiarito come la formulazione della disposizione estenda detto dovere anche agli apolidi e agli stranieri residenti in Italia e proprietari di beni o che vi svolgano attività lavorative.

Altri ancora – VIOLINI e SPADARO – poi, ne hanno evidenziato l'intima interconnessione con il principio di solidarietà e con i fenomeni di globalizzazione, evidenziando i rischi sottesi all'attuale – si parla di quasi vent'anni fa! – situazione economica e sociale a livello mondiale[63].

Eppure, tali discorsi sono rimasti alquanto nell'ombra e sono stati affrontati dalla dottrina costituzionalistica a fasi alterne, per quanto siano stati ripresi circa un decennio fa[64].

Una spiegazione circa tale tendenza è fornita dal RIMOLI[65], il quale attribuisce la negligenza nell'analizzare tale tematica "*alla natura impervia del tema stesso, un po' "scomodo", scarsamente attrattivo e sottilmente inclinato verso un'impostazione illiberale della complessiva forma dello Stato*", nonché alla concezione del costituzionalismo moderno come processo di affrancamento degli individui dal potere, considerazione, quest'ultima, espressa anche dal GEMMA[66].

---

[61] R. BALDUZZI, M. CAVINO, E. GROSSO E J. LUTHER (a cura di), *I DOVERI COSTITUZIONALI: LA PROSPETTIVA DEL GIUDICE DELLE LEGGI – Atti del convegno di Acqui Terme-Alessandria svoltosi il 9-10 giugno 2006*, Giappichelli Editore, 2007, disponibile su https://www.gruppodipisa.it/images/pubblicazioni/2007_I_doveri_costituzionali_la_prospettiva_del_giudice_delle_leggi.pdf

[62] Quest'ultimo è pure autore di una voce sulla Treccani, nella sezione Diritto on line, datata 2014 e intitolata *Doveri costituzionali*, al link https://www.treccani.it/enciclopedia/doveri-costituzionali_%28Diritto-on-line%29/

[63] Non a caso A. SPADARO ha intitolato il proprio contributo "*Sul necessario carattere «globale» (e non solo interno) dei doveri*" e quello di L. VIOLINI si intitola "*I doveri inderogabili di solidarietà: alla ricerca di un nuovo linguaggio*"

[64] F. RIMOLI, *Appunti per uno studio sulla dimensione funzionale dei doveri pubblici*, su www.federalismi.it, 01/07/2015. L'autore evidenzia che "*questi ultimi non potrebbero in alcun modo essere garantiti senza il rispetto di un nucleo consistente di doveri, i quali costituiscono in certo modo l'essenza dell'obbligazione politica e il presupposto primario della convivenza civile, in stretta connessione con il pervadente principio di solidarietà, e, ancor prima, con quel concetto di fraternité che ispirò la cultura rivoluzionaria francese, insieme a quelli di libertà ed eguaglianza*". Quando, poi, nella nota n. 1 elenca diverse pubblicazioni, arriva addirittura al 1967 per individuare contributi alla trattazione del tema. Si riportano di seguito le opere menzionate dall'autore nella nota: "G.M. LOMBARDI, *Contributo allo studio dei doveri costituzionali*, Giuffrè, Milano, 1967 (si veda anche ID., *Doveri pubblici* (diritto costituzionale), in *Enc.dir.*, agg., VI, Giuffrè, Milano, 2002, 357 ss.); nonché in C. CARBONE, *I doveri pubblici individuali nella Costituzione*, Giuffrè, Milano, 1968; di recente, F. GRANDI, *Doveri costituzionali e obiezione di coscienza*, Editoriale scientifica, Napoli 2014; L. VIOLANTE, *Il dovere di avere doveri*, Einaudi, Torino, 2014; G. BASCHERINI, *Doveri costituzionali*, in www.treccani.it; si vedano anche i saggi contenuti in R.BALDUZZI-M.CAVINO-E.GROSSO-J.LUTHER (a cura di), *I doveri costituzionali: la prospettiva del giudice delle leggi*, Giappichelli, Torino, 2007."

[65] *Op. cit.*

[66] G. GEMMA, *Doveri costituzionali e giurisprudenza della Corte*, in R. BALDUZZI, M. CAVINO, E. GROSSO E J. LUTHER (a cura di), *I DOVERI COSTITUZIONALI: LA PROSPETTIVA DEL GIUDICE DELLE LEGGI – Atti del convegno di Acqui Terme-Alessandria svoltosi il 9-10 giugno 2006*, Giappichelli Editore, 2007, p. 370, che richiama l'approccio post Locke che ha dato vita all'età "dei diritti", riprendendo la formula di N. BOBBIO

Eppure, è un argomento ineludibile, nonostante la sua intrinseca "scomodità"[67].

Infatti, vale ricordare che:

"*La profonda attenzione con la quale si è riflettuto sull'affermazione dei diritti dell'uomo e sulle loro garanzie giurisdizionali non è stata accompagnata da un'eguale elaborazione teorica dello statuto dei doveri e delle relative responsabilità. L'asimmetrica attenzione riservata ai diritti e ai doveri ha generato uno squilibrio tra elementi che sono in eguale misura chiamati a caratterizzare le finalità primarie che il sistema sociale e politico ha la necessità di perseguire, posto che non solo i diritti, ma anche i doveri si inseriscono nel nucleo duro della teoria costituzionale. Si avverte quindi l'esigenza di una sistemazione generale nella quale le varie figure di dovere costituzionale abbiano adeguata ricognizione, prossima a quella che ha interessato le libertà costituzionali.*"[68].

Ciò, invero, diventa ancor più rilevante alla luce di quella che è la "solidarietà intergenerazionale"[69].

Conclusioni: "ri-bilanciare" il diritto alla privacy con il dovere di contribuzione e i principi solidaristici.

Alla luce di quanto esposto finora, è evidente come alcuni diritti, nati – o meglio, sviluppati – di pari passo con le nuove tecnologie, possano inficiare notevolmente la serenità e l'armonia (se mai ve ne fosse) della società, con particolar riferimento alle dinamiche socioeconomiche e anche generazionali.

Tuttavia, i difetti – se così possono esser definiti – di siffatti diritti sono contemperabili, se non addirittura eliminabili, se si adottano due approcci, differenti ma al contempo complementari.

In primo luogo, è necessario prendere nuovamente le mosse dalla dialettica che connota il rapporto tra diritti e doveri, considerando che i primi hanno senso di esistere solo laddove messi in relazione ai secondi, in un ideale dualismo, come quello intercorrente tra luce ed ombra, tra il singolo e il tutto.

Poi, va tenuta in debita considerazione la posizione della CGUE in tema di trattamento dei dati fiscali, la quale richiede unicamente il rispetto dei principi di proporzionalità e minimizzazione. Principi che, come dimostra la

---

[67] Il RIMOLI ricorda come già nella *Politica* di Aristotele e nel *De officiis* di Cicerone si rifletta profondamente su queste tematiche.

[68] F. POLACCHINI, *Doveri costituzionali e Principio di solidarietà*, Bononia University Press, 2016, https://buponline.com/az13zg/uploads/woocommerce_uploads/cicu-285-polacchini_-digital.pdf, p. 3. Si noti, di nuovo, come si ricolleghino il principio di solidarietà e il complesso dei doveri costituzionali… Ciò vale a connotare funzionalmente detti doveri, volti non tanto a consentire il funzionamento dello Stato nel suo complesso, quanto, piuttosto, a porre le basi per una crescita quanto più possibile armoniosa della società e dell'ordinamento. A p. 163 l'autrice ripercorre alcuni momenti in cui la giurisprudenza ha utilizzato la locuzione "dovere costituzionale". A p. 171, circa la titolarità del dovere ex art. 53 Cost., sembra porsi su posizioni parzialmente differenti rispetto a quelle di coloro che l'hanno preceduta 10 anni prima, tant'è che afferma: "*Circa il dovere tributario, di cui all'art. 53 Cost., esso si traduce in un semplice obbligo qualora la legge attribuisca al non cittadino gli stessi obblighi fiscali che operano per il cittadino. Acquista, invece, dignità di dovere costituzionale qualora chiami il non cittadino a concorrere alle spese pubbliche in ragione della sua capacità contributiva, presupponendo in tal modo la sua appartenenza ad un gruppo sociale che bilancia e ridistribuisce benefici e oneri dell'appartenenza.*"

[69] F. POLACCHINI, *op cit.*, di L. VIOLINI, *I doveri inderogabili di solidarietà: alla ricerca di un nuovo linguaggio*, in R. BALDUZZI, M. CAVINO, E. GROSSO E J. LUTHER (a cura di), *op. cit.*

recentissima pronuncia del 2022, vanno attuati su base molto pragmatica e avendo cura di considerare le peculiarità del caso concreto (difatti, la CGUE riserva al giudice del rinvio il compito di verificarne il rispetto in concreto, non potendosi determinare un parametro astrattamente valido per ogni situazione).

Il tutto senza dimenticare che ci si trova ad affrontare un fenomeno particolarmente insidioso – non solo l'evasione ma pure l'elusione e l'abuso del diritto [70] – che fa grande uso delle tecnologie, in particolare di quelle emergenti[71].

Laddove tali approcci non dovessero essere ripresi, il rischio sarebbe quello di fomentare – sia pur non volendo – le già esistenti disuguaglianze sociali (si pensi a chi, con un reddito alto, ha modo e mezzi di nasconderlo e chi, invece, non può) se non addirittura di crearne di nuove (per esempio, quella tra vecchie e nuove generazioni oppure tra particolari categorie di lavoratori).

Non sarebbe, invero, neppure possibile condurre un qualsivoglia intervento di riduzione del carico fiscale, anzi!

In sintesi, ben vengano i diritti, anche quelli nuovi.

Ciò, però, a condizione di contemperarli – questa è la "parola magica" – con i propri doveri e con i corrispondenti diritti dei consociati.

In caso contrario, dall'eccesso da cui si è partiti – la preminenza assoluta dello Stato – è facile giungere in quello opposto, che altro non sarebbe se non un individualismo talmente sfrenato da porre a rischio le fondamenta della democrazia stessa e in totale contrasto con quella solidarietà cui siamo stati richiamati dal Presidente della Repubblica nel discorso di fine anno, il quale ha ricordato che "*La Repubblica è nel senso civico di chi paga le imposte perché questo serve a far funzionare l'Italia e quindi al bene comune.*", nonché "*[…] Nello spirito di solidarietà di chi si cura del prossimo.*", per poi concludere che "*La Repubblica vive della partecipazione di tutti. È questo il senso della libertà garantita dalla nostra democrazia.*"[72].

Senso civico, solidarietà e doveri del cittadino sono stati indicati, pertanto, come le stelle polari cui far riferimento nelle future evoluzioni di questo Sistema Paese, senza le quali sarebbe impossibile attuare pienamente i vari diritti previsti dalla nostra Carta Costituzionale.

Indicazione proveniente, tra l'altro, dal Garante della Costituzione e che consentirebbe di attuare anche il principio di proporzionalità della tassazione. Non va scordato, come sopra menzionato, che proprio il concetto di "proporzionalità fiscale", quello di progressività della tassazione e le ipotesi per la relativa attuazione hanno occupato gran parte del dibattito dei Padri Costituenti in merito all'art. 53 Cost.

---

[70] In tema di abuso del diritto in ambito fiscale vedasi la pagina tematica della Camera dei Deputati al link https://temi.camera.it/leg17/post/app_labuso_del_diritto#:~:text=L'abuso%20del%20diritto%20in,utilizzo%20distorto%20di%20schemi%20giuridici. Anche tale fenomeno, con un corretto utilizzo dei dati, verrebbe pesantemente ridimensionato.

[71] M. CARDILLO, S. RAPUANO, *Le criptovalute: tra evasione fiscale e reati internazionali, in Diritto e Pratica Tributaria* n. 1/2019, https://www.altalex.com/documents/2019/05/16/le-criptovalute-tra-evasione-fiscale-e-reati-internazionali

[72] PRESIDENTE DELLA REPUBBLICA S. MATTARELLA, *Messaggio di fine anno del Presidente della Repubblica*, 31/12/2022, su https://www.quirinale.it/elementi/75654

Ma era un dibattito incentrato soprattutto sulle tipologie di imposte – dirette e indirette – e su cosa considerare ai fini dell'imponibile, senza apparentemente tenere in conto l'effetto dovuto all'evasione.

E lo stesso fu un dibattito vivace e complesso.

Pertanto, a maggior ragione è necessario giungere a un contenimento dell'evasione e il trattamento dei dati personali è essenziale in tale aspetto, essendo propedeutico alla riduzione del carico fiscale che caratterizza lo Stato italiano.

Soltanto attraverso tale strumento è possibile conoscere realmente l'imponibile e la capacità fiscale effettiva di ognuno nonché avere i dati necessari per una rimodulazione dell'ordinamento tributario e dei relativi prelievi che assicuri, tutto insieme: il rispetto del principio di progressività ex art. 53, co. 2 Cost. e del principio di solidarietà ex art. 2 Cost.; il finanziamento di una spesa pubblica idonea a garantire pienamente i diritti costituzionalmente previsti; un rilancio dell'economia mediante una riespansione dell'iniziativa economica privata e della capacità di spesa di quanti compongono il cd. "mercato interno" di un Paese.

Razzante R, 'L'attribuzione degli attacchi informatici' (2022) 2 EJPLT, 215-241.
DOI : https://doi.org/10.57230/EJPLT222RR

EJPLT
ISSN 2704-8012



L'attribuzione degli attacchi informatici

The attribution of cyberattacks

RANIERI RAZZANTE
Contract Professor of Techniques for Anti-Money Laundering Risk Management at Alma Mater Studiorum Università di Bologna,
Contract Professor of Techniques and Rules of Cybersecurity, at Università degli Studi Suor Orsola Benincasa

Abstract

Il presente approfondimento si pone l'obiettivo di evidenziare gli attuali limiti del diritto nell'individuazione, e quindi della possibilità di sanzionare, gli attacchi informatici. Infatti, l'evoluzione tecnologica e le nuove frontiere della comunicazione hanno portato alla proliferazione di nuove condotte penalmente rilevanti, nonché ad una significativa espansione delle attività illecite, anche nel Metaverso, difficilmente controllabili. della materia.

The purpose of this paper is to highlight the current legal limitations in the identification and the possibility of sanctioning cyber-attacks. In fact, technological evolution and new frontiers of communication have resulted in the proliferation of new criminally relevant conducts, as well as a significant increase in illicit activities. This increase is affecting also the Metaverse, and today it appears to be hardly controllable.

© The author(s) 2022, 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: attribuzione; attacco informatico; cybersicurezza; cybersecurity; metaverso; cyberlaundering.

Summary: Introduzione: Il Metaverso: un locus commissi delicti atipico. – 1. Gli attacchi informatici: le minacce del nuovo millennio. – 2. Le tre fasi dell'attribuzione. La fase tecnica. – 3. (Segue) La fase politica. – 4. (Segue) La fase giuridica. – 5. La normativa europea: il Regolamento 2019/796/UE. – 6. Il nuovo volto del riciclaggio nell'era digitale: il cyberlaundering. – 7. Il fenomeno del cyberterrorismo. – 8. (Segue) La cybersicurezza in Italia: sviluppi del 2022. – 9. Direttiva NIS (Network and Information Security). – 10. (Segue) Direttiva NIS 2: i cambiamenti. – Conclusioni: Attacchi informatici ed attuale panorama sanzionatorio italiano: prospettive de iure condendo.

Introduction: Il Metaverso: un locus commissi delicti atipico.

Il Metaverso è una realtà digitale, risultante dall'insieme di dimensioni virtuali e reali interconnesse, in cui gli utenti vengono rappresentati da propri *alter ego*, definiti avatar [1].

Questo nuovo mondo fa sorgere molti interrogativi in merito alla possibilità di applicarvi le tradizionali categorie del diritto, ponendo l'interprete davanti a questioni quali la perseguibilità di azioni ivi poste in essere, la relativa qualificazione e la possibilità di effettiva comminazione della pena.

La prima ambiguità che si pone è la plausibilità o meno del ritenere che il Metaverso[2] possa rappresentare un vero e proprio *locus commissi delicti*, ed è ormai pacifico che una realtà diversa da quella fattuale sia idonea alla commissione di reati. È legittimo chiedersi come sciogliere il nodo dell'individuazione della competenza per territorio e, a tal fine, giova richiamare le considerazioni della Corte di Cassazione in merito alle ipotesi di diffamazione[3] a mezzo Internet, a detta della quale, ai fini «dell'individuazione della competenza, sono inutilizzabili, in quanto di difficilissima, se non impossibile individuazione, criteri oggettivi unici (…) Ne consegue che non possono trovare applicazione né la regola stabilita dall'art. 8 c.p.p., né quella fissata dall'art. 9 c.p.p., comma 1. (…) In tale articolato contesto è, quindi, imprescindibile fare ricorso ai criteri suppletivi fissati dal predetto art. 9 c.p.p., comma 2, ossia al luogo di domicilio dell'imputato»[4].

Inoltre, le condotte realizzate sul web si estrinsecano nell'emanazione o nella captazione di una serie di impulsi elettronici, interconnessi tra loro, indifferentemente dalla concreta ubicazione del soggetto agente. Per questa ragione il reato assume una connaturata ed inevitabile dimensione transnazionale.

---

[1] Termine che sta ad indicare la rappresentazione grafica e virtuale di un visitatore di sito web.

[2] F. SARZANA DI SANT'IPPOLITO, I.O. EPICOCO, M. PIERRO, *Il diritto del metaverso*, Torino, 2022 e D. DELFINO, *La corsa al metaverso e le criticità giuridiche*, in *Filodiritto*, 18 novembre 2022. Consultabile al sito: https://www.filodiritto.com/la-corsa-al-metaverso-e-le-criticita-giuridiche.

[3] Sul tema si veda anche P. ZARRA, *L'evoluzione applicativa della diffamazione via e-mail nell'era dello smart-working, commento a Cass. Pen., Sez. V, 8 aprile 2021, n. 13252*, in *Diritto di Internet*, 2021, IV, 733-735.

[4] Cass. Pen., sez. I, sent. 21.12.2010, n. 2739, in *Guida al diritto*, 2011, 23, 92.

In secondo luogo, sarebbe possibile rispondere positivamente alla possibilità di qualificare le condotte poste in essere sulla base delle ordinarie figure di reato, come dimostra l'ampia gamma dei crimini informatici già tipizzati. Ad esempio, la giurisprudenza ha ricondotto al concetto di luogo aperto al pubblico, rilevante ai fini dell'integrazione dell'art. 660 c.p., una pagina Facebook, equiparandola ad una pubblica agorà virtuale. Ad ulteriore dimostrazione dell'esaustività del catalogo di fattispecie, si possono riportare le ipotesi di abuso sessuale, di istigazione al suicidio, di revenge porn, di minaccia, ecc.

Un ulteriore quesito interessa il rispetto del principio di materialità e, in merito, si è ipotizzato che, nel Metaverso, non potesse mai concretizzarsi un'azione in senso stretto e che, dunque, l'inquadramento del fatto dovesse sempre avvenire in termini di mera intenzionalità. Tuttavia, come già sottolineato, c'è una connessione tra la realtà reale e quella virtuale; difatti, per accedervi sono necessari appositi strumenti (visori, caschetti e occhiali), una valuta virtuale e connessioni idonee a supportare l'esperienza immersiva.

Alla luce di queste considerazioni è opportuno interrogarsi, altresì, sulla possibilità concreta che un'azione estrinsecata nel Metaverso, laddove lesiva di un bene giuridicamente protetto attraverso norme penalistiche, possa dar vita a responsabilità.

Da ultimo, è opportuno sottolineare[5] come, in taluni casi, sono stati ritenuti integrati reati, quale la violenza sessuale, pur a fronte dell'assenza di contatto fisico; in merito, si richiama una pronuncia della Corte di Cassazione la quale, condividendo le considerazioni del Tribunale del Riesame, concludeva per l'applicazione dell'art 609-*bis* c.p., atteso che: «La violenza sessuale risultava pienamente integrata, pur in assenza di contatto fisico con la vittima, quando gli atti sessuali coinvolgessero la corporeità sessuale della persona offesa e fossero finalizzati e idonei a compromettere il bene primario della libertà individuale nella prospettiva di soddisfare o eccitare il proprio istinto sessuale»[6]. C'è chi riconosce in questa impostazione una continuità rispetto ai casi di illecito perpetrati nel Metaverso, propendendo a favore di una punibilità di tali condotte. A sfavore di tale impostazione milita chi[7], al contrario, ritiene che le ipotesi in esame ricadrebbero nell'ambito dell'art. 49 c.p., cioè che si tratterebbe di reati impossibili[8].

Venendo alla possibilità di sovrapposizione della figura dell'avatar a quella del soggetto persona fisica, è da rilevare come, nel Metaverso, non operi concretamente e direttamente l'individuo, bensì una sua proiezione; la paternità delle azioni, dunque, dovrebbe essere ascrivibile al soggetto che,

---

[5] Si veda, A. CONTINIELLO, *Le nuove frontiere del diritto penale nel Metaverso. Elucubrazioni metagiuridiche o problematica reale?*, in *Giur. Pen.,* 2022, V; V. IMPROTA, *Metaverso e reati nell'ordinamento giuridico italiano*, in *Filodiritto*, 6 giugno 2022. Consultabile al sito: https://www.filodiritto.com/metaverso-e-reati-nellordinamento-giuridico-italiano; C. CRISCI, *Metaverso: brevi riflessioni sui profili di diritto penale*, in *Filodiritto*, 30 novembre 2022. Consultabile al sito: https://www.filodiritto.com/metaverso-brevi-riflessioni-sui-profili-di-diritto-penale.

[6] Cass. Pen., sez. III, sent. 08.09.2020, n. 25266 in *Foro It.,* 2020; si veda anche, L. PICOTTI, *La violenza sessuale via whatsapp, commento a Cass. Pen., Sez. III, 8 settembre 2020, n. 25266*, in *Diritto di Internet*, 2020, IV, 683-685.

[7] D. INGARRICA, *Metaverso criminale. Quali interazioni nel presente nazionale e quali sfide globali del prossimo futuro*, in *Giur. Pen.*, 2022, IX.

[8] G. FIANDACA, E. MUSCO, *Diritto Penale. Parte generale,* 8ª ed., Torino, 2019.

attraverso input informatici, determina l'avatar – rappresentazione di sé stesso – ad agire. La soluzione non pare essere così lineare, in ragione della evidente discrasia tra le due figure, dalla quale discende un verosimile contrasto con il principio di personalità della responsabilità penale. Tuttavia, il Legislatore ha contezza dei rischi derivanti dal mancato riconoscimento di una responsabilità personale per le ipotesi in cui si dovrebbe accettare una *fictio* iuris, come avvenuto per le società e per l'adozione del D. Lgs. 8 giugno 2001, n. 231. In ragione della similarità delle due situazioni, ben potrebbero essere superati i timori in merito al rispetto del principio di personalità della pena rispetto al fatto di reato.

In conclusione, sarebbe opportuno porsi a metà strada tra la rilevanza di condotte *contra legem* poste nel Metaverso e, al contrario, una loro assoluta irrilevanza. Una soluzione di compromesso potrebbe, eventualmente, essere il rafforzamento di una responsabilità di natura civile.

1. Gli attacchi informatici: le minacce del nuovo millennio.

Si definisce, con i limiti attuali del diritto, attacco informatico: «un'operazione informatica, di natura offensiva o difensiva, che sia ragionevolmente prevedibile e che cagioni lesioni o morte a persone o danni o distruzione a oggetti»[9]. Trattasi, dunque, di operazioni condotte attraverso l'impiego di strumenti informatici o telematici, che implicano atti di violenza.

Per valutare se un atto costituisca un attacco informatico, è necessario porre l'attenzione sul rapporto causale tra la condotta ed i danni cagionati, quindi porre l'attenzione sul piano delle conseguenze.

A venire in rilievo non sono esclusivamente le conseguenze dirette sul supporto informatico ma anche quelle indirette, consequenziali e ragionevolmente prevedibili, che insistano su persone o cose che, pertanto, costituiranno l'oggetto dell'attacco.

I cyberattacks, attualmente, rappresentano la modalità di attacco più funzionale nei confronti di uno Stato, grazie ad alcune peculiarità proprie degli strumenti informatici, tra cui l'anonimato, l'a-spazialità e l'a-temporalità[10].

Per questa ragione, è essenziale che gli Stati si dotino di sistemi di prevenzione e, in particolar modo, di rilevazione di tali minacce, con la finalità di individuare prontamente il soggetto a cui attribuire l'attacco.

In questa delicata fase si inserisce il problema dell'attribuzione, intesa quale procedimento volto a risalire al soggetto mittente dell'operazione[11]; a tal fine, risulta dirimente disporre di risorse tecnologiche congrue, sia fisiche che umane, e di potersi avvalere di strumenti di collaborazione internazionale che favoriscano lo scambio di informazioni rilevanti.

Si tratta, ora, di delineare le fasi del processo di attribuzione dell'atto informatico ostile.

---

[9] M. N. SCHMITT (a cura di), *Tallinn Manual 2.0 on the international law applicable to cyber operations,* Cambridge, 2017.

[10] R. RAZZANTE, A. CRISTALLINI, *Cybercrime*, Pisa, 2021, 15. Per ulteriori approfondimenti, si veda L. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, Bologna, 2018, I, 69.

[11] T. RID, B. BUCHANAN, *Attributing Cyber Attacks*, in *The Journal of Strategic Studies*, 2015, 5 – 37.

2. Le tre fasi dell'attribuzione. La fase tecnica.

Si può tentare di declinare il processo dell'attribuzione in tre macro-fasi: tecnica, politica-pubblica e giuridica.

La prima fase ha come obiettivo l'individuazione della strumentazione utilizzata per condurre l'attacco, tramite elaboratori in grado di analizzare, quantificare e manipolare dati informatici. All'esito di questo procedimento, si giungerà a circoscrivere la fonte responsabile.

In questo stadio, ci si avvale dei cc.dd. indicatori di compromissione (indicators of compromise, IoC), quali malware, virus, signature, domain name ed indirizzi IP.

Nella maggior parte delle ipotesi, la ricostruzione *sic et simpliciter* delle modalità tecniche della violazione può non condurre a risultati esaustivi, dunque si ricorre ad un'analisi incrociata con le *TTP* (tattiche, tecniche e procedure) che più di frequente trovano impiego nel cyberspazio.

Di recente, si è assistito ad una maggior frequenza nell'impiego di tool standardizzati e non personalizzati, che aggravano ulteriormente la fase di individuazione del soggetto responsabile. Pertanto, entra in gioco un'analisi di natura empirica per il tramite di modelli comportamentali a supporto degli strumenti ordinari.

La fase tecnica, certamente la più delicata, dovrebbe poter contare su risorse che permettano, quanto più possibile, una riduzione dei tempi di rilevamento, per evitare una dispersione di elementi e di dati rilevanti.

3. (Segue) La fase politica.

La fase politica consiste nella raccolta di informazioni attraverso canali interstatali – ufficiali e non – per giungere all'individuazione delle potenziali ragioni (spesso, geopolitiche) sottese all'attacco e al soggetto, ovvero all'organizzazione da cui esso proviene.

Questo secondo step ha una connotazione fortemente pubblica[12]; spesso, difatti, si mira ad individuare il soggetto colpevole, diffondendo la notizia attraverso i mass media, per disincentivare l'eventuale reiterazione degli attacchi[13], con finalità, dunque, eminentemente deterrente.

Da ultimo, la diffusione della notizia, tramite canali di comunicazione ufficiale, costituisce una forte presa di posizione, nel panorama internazionale, nei casi in cui l'attribuzione di un attacco avvenga congiuntamente da parte di più Stati.

[12] Per approfondimenti, F. J. EGLOFF, M. SMEETS, *Publicly attributing cyber-attacks: a framework*, in *Journal of Strategic Studies*, 2021.

[13] A. BENDIEK, M. SCHULZE, *Attribution: A Major Challenge for EU Cyber Sanctions, German institute for International and Security Affairs*, in *SWP Research Paper*, 2021.

4. (Segue) La fase giuridica.

Nell'ultima fase, prettamente giuridica, l'attacco è imputato ad un soggetto, ad un'organizzazione o ad uno Stato.

Nei casi in cui viene individuata come responsabile una persona fisica o un'organizzazione, ne deriverà l'imputazione sulla base della fattispecie penale prevista all'interno del singolo Stato.

Nelle ipotesi in cui l'attacco sia riconducibile ad uno Stato, tuttavia, si rilevano difficoltà nell'attribuzione, derivanti dall'assenza di una normativa internazionale, dovendosi risolvere la questione in via interpretativa.

Da una minaccia informatica, in queste ipotesi, potrebbe derivare una responsabilità internazionale dello Stato a cui essa si attribuisce, come prevista dal Progetto di articoli sulla responsabilità degli Stati del 2001[14].

Affinché si possa ritenere sussistente un illecito internazionale, è necessaria l'integrazione del relativo elemento oggettivo, il cui fondamento risiede nella violazione di un obbligo parimenti internazionale facente capo allo Stato.

A tal fine, potrebbe addursi come referente giuridico l'art. 2, par 4, della Carta delle Nazioni Unite, che dispone: «I Membri devono astenersi, nelle loro relazioni internazionali, dalla minaccia o dall'uso della forza, sia contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite».

È possibile inquadrare i casi in esame, dunque, nel concetto di uso della forza, riconducendovi le ipotesi di attacchi cyber, con conseguente applicabilità della legittima difesa di cui all'art 51 della Carta. Ammettendo tale soluzione, si riterrebbe integrato l'elemento oggettivo di un illecito internazionale, consistente nella violazione dell'obbligo giuridico avente ad oggetto il generale dovere di astensione dall'uso della forza[15]. Inoltre, la Rule 11 del Manuale di Tallinn delinea i requisiti affinché un attacco cyber possa essere ascrivibile all'ipotesi di uso della forza, stabilendo che: «A cyber operation consitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force».

Si esige, dunque, che dall'attacco derivino conseguenze analoghe e qualitativamente equivalenti a quelle che si verificherebbero a seguito di un attacco tradizionalmente inteso, focalizzando l'attenzione dalla convenzionale fenomenologia dell'uso della forza al piano dei concreti effetti pregiudizievoli che ne possono derivare, pur a fronte di modalità di azione atipiche e nuove.

Tuttavia, non manca chi milita a favore di un'impostazione più rigorosa e meno soggetta ad una fluidità interpretativa, sulla base di argomentazioni che ruotano attorno alla risalente posizione espressa a suo tempo – nel 1927 – dalla Corte permanente di giustizia internazionale, secondo la quale: «The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement

[14] M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014, 35.

[15] A tal proposito, è utile il richiamo alla Rule 10 del Manuale di Tallin, secondo cui: «A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of a State, or that is in any other manner inconsistent with the purposes of the United Nation, is unlawful».

of common aims. Restrictions upon the independence of States cannot therefore be presumed»[16].

Da tale prospettiva, la responsabilità di uno Stato potrebbe sorgere solo a fronte della violazione di un obbligo esplicito, da cui *a contrario* si ricaverebbe la legittimità di ogni condotta non vietata. Tale seconda impostazione, a ben vedere, rispetto alla prima, restringerebbe ulteriormente le ipotesi di attribuzione, azzerandole del tutto, visto che, a livello internazionale, tale obbligo esplicito non sussiste in tema di attacchi informatici.

Pertanto, l'interprete constaterà l'assenza, come anticipato, di una normativa puntuale volta a disciplinare il fenomeno in esame e, salvo ammettere un *vulnus* di tutela a fronte di attacchi che sovente si dirigono verso infrastrutture critiche[17] statali, la prima soluzione interpretativa parrà essere preferibile.

A supporto di tale conclusione, infatti, si ricorda che, all'interno del Progetto di articoli sulla responsabilità degli Stati del 2001, l'art. 14 stabilisce che una violazione si può verificare tramite: «an act of that State is not in conformity with what is required of it by that obligation, regardless of its origin or character».

Concludendo, dunque, che un attacco informatico costituisca uso della forza, si apre la possibilità di agire in legittima difesa, ai sensi dell'art. 51 della Carta delle Nazioni Unite, che dispone: «Nessuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale. Le misure prese da Membri nell'esercizio di questo diritto di autotutela sono immediatamente portate a conoscenza del Consiglio di Sicurezza e non pregiudicano in alcun modo il potere e il compito spettanti, secondo il presente Statuto, al Consiglio di Sicurezza, di intraprendere in qualsiasi momento quell'azione che esso ritenga necessaria per mantenere o ristabilire la pace e la sicurezza internazionale».

5. La normativa europea: il Regolamento 2019/796/UE.

Con il Regolamento 2019/796/UE del 17 maggio 2019, concernente Misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, l'Unione europea ha inteso predisporre un sistema volto a limitare l'ingresso ed il transito sul territorio unico europeo, unitamente a misure di congelamento di fondi e di risorse economiche, nei confronti di soggetti «quali identificati dal Consiglio a norma dell'art. 5, par. 1, della Decisione (PESC)

[16] Corte Permanente di Giustizia Internazionale, 07.09.1927, *France vs Turkey, The Case of the S.S. "Lotus"*.

[17] Definizione calzante di infrastruttura critica la si può rintracciare nella Direttiva 114/08/CE del Consiglio dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, che definisce « "Infrastruttura Critica" un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni».

2019/797: a) persone fisiche o giuridiche, entità o organismi che sono responsabili di attacchi informatici o tentati attacchi informatici; b) persone fisiche o giuridiche, entità o organismi che forniscono sostegno finanziario, tecnico o materiale per attacchi informatici o tentati attacchi informatici, o che sono altrimenti coinvolti in tali attacchi o tentati attacchi, anche pianificandoli, preparandoli, partecipandovi, dirigendoli, assistendoli o incoraggiandoli, o agevolandoli per azione o omissione; c) persone fisiche o giuridiche, entità o organismi associati alle persone fisiche o giuridiche, alle entità o agli organismi di cui alle lettere a) e b) del presente paragrafo».

In particolare, all'art. 1 vengono individuate le azioni che integrano un cyberattacco, quali l'accesso o l'interferenza a sistemi informatici e l'intercettazione di dati; tali attacchi sono sferrati dall'esterno dell'Unione o impiegano infrastrutture esterne alla stessa. Per quanto riguarda i soggetti agenti, rilevano quali attacchi informatici quelli compiuti da una persona fisica o giuridica, un'entità o un organismo stabiliti oppure operanti al di fuori dell'Unione o commessi con il sostegno, sotto la direzione o sotto il controllo di tali soggetti.

Nel successivo par. 4 dell'art. 1, si circoscrivono quali attacchi implicanti una minaccia per l'Unione quelli che insistono sulle infrastrutture critiche essenziali per il mantenimento delle funzioni vitali della società, della salute, dell'incolumità, della sicurezza e del benessere economico o sociale della popolazione. Inoltre, vi si ricomprendono quelli che attaccano i servizi necessari, quali l'energia, i trasporti, il settore sanitario, la distribuzione di acqua potabile.

La rilevanza delle azioni che presentino i requisiti dell'art. 1 sono stabilite sulla base degli effetti che da esse derivano; in particolare, l'art. 2 dispone che, al fine di determinare se l'attacco abbia avuto un effetto significativo, bisogna aver riguardo a: «a) portata, entità, impatto o gravità delle turbative causate, anche per quanto riguarda le attività economiche e sociali, i servizi essenziali, le funzioni statali essenziali, l'ordine pubblico o la sicurezza pubblica; b) numero di persone fisiche o giuridiche, entità o organismi interessati; c) numero di Stati membri interessati; d) importo della perdita economica causata per esempio mediante furti su larga scala di fondi, risorse economiche o proprietà intellettuale; e) vantaggio economico ottenuto dall'autore dell'atto per se stesso o per terzi; f) quantità o natura dei dati oggetto del furto o entità delle violazioni dei dati; o g) natura dei dati sensibili sotto il profilo commerciale cui si è avuto accesso».

Nell'ambito della politica estera e della sicurezza comune dell'Unione europea, possono essere, altresì, impiegati strumenti alternativi, modulabili sulla base dell'intensità dell'attacco. Fermo restando che le sanzioni entrano in gioco a fronte di un evento connotato da un alto grado di gravità, in ipotesi ordinarie si può, anzitutto, ricorrere all'adozione di misure preventive, spesso in accordo con Paesi terzi, grazie ad interlocuzioni politiche che consolidino, ad esempio, una posizione comune o che giungano a misure di cooperazione. È possibile, inoltre, che la presa di posizione avvenga già in seno al Consiglio (in tali casi, tuttavia, si esigerebbero maggioranze qualificate) e, in ipotesi di particolare gravità, come le operazioni militari e di difesa.

6. Il nuovo volto del riciclaggio nell'era digitale: il cyberlaundering.

L'evoluzione tecnologica e le nuove frontiere della comunicazione hanno portato, come anticipato, alla proliferazione di nuove condotte penalmente rilevanti, nonché ad una significativa espansione delle attività illecite[18].

Difatti, la rete è diventata terreno fertile per la realizzazione dei propositi criminosi delle organizzazioni nel più breve tempo possibile. Queste ultime, per sopravvivere ed operare, necessitano di ingenti risorse finanziarie che, tramite il *web*, possono essere facilmente reperite, per poi essere reinvestite: Internet ha consentito la diffusione e la perpetrazione di frodi informatiche, favorendo il reperimento di importanti somme e, di conseguenza, il riciclaggio di denaro "sporco"[19].

Il cyberlaundering rappresenta la trasformazione digitale di un fenomeno già esistente, che ha quale obiettivo primario quello di: «allontanare il denaro dalle relative origini illecite, ostacolando la tracciabilità dell'origine dei proventi. E alcuni delitti, quali estorsioni informatiche, furti di identità, phishing e spamming, vengono, a loro volta, adoperati per concretizzare e agevolare il riciclaggio online»[20].

Il phishing, ad esempio, è l'attività illecita in base alla quale, attraverso vari artifici, - si pensi allo spamming di messaggi o all'utilizzo di malware -, un soggetto riesce ad impossessarsi, fraudolentemente, dei codici elettronici di un dato utente, allo scopo di utilizzarli, successivamente, per frodi informatiche considerevoli, quali, ad esempio, l'accesso ai conti correnti bancari o postali al fine di trarne profitto.

Nello specifico, l'autore del phishing invia un messaggio piuttosto credibile, nel cui testo si rappresentano urgenti ragioni di sicurezza per le quali sarebbe assolutamente necessario che il destinatario clicchi sul link indicato, allo scopo di inserire o modificare le proprie credenziali di accesso ai conti online. Il link, in realtà, rimanda ad una pagina web contraffatta ma identica, almeno graficamente, a quella originale dell'istituto di credito[21].

Ebbene, il phisher si impossesserà dei dati immessi dall'utente raggirato, e li utilizzerà per accedere al conto corrente della vittima, al fine di sottrarne denaro.

Si segnala, altresì, la presenza di un altro soggetto, il financial manager, sul cui conto verranno accreditate le somme di cui il phisher si sia impossessato abusivamente, al fine poi di trasferirle all'estero con operazioni di money transfert.

---

[18] Sul punto si confronti R. RAZZANTE, A. CRISTALLINI, *op. cit.*, 5 ss.

[19] Per approfondire si veda R. RAZZANTE, *Le insidie di blockchain e bitcoin*, in *Formiche*, 2019, 153, 20-22 e R. RAZZANTE, L. CUOMO, *La nuova disciplina dei reati informatici*, Torino, 2009.

[20] In merito, per approfondire, si veda, R. RAZZANTE, *Manuale di legislazione e prassi dell'antiriciclaggio*, 2ª ed., Torino, 2023.

[21] In questo senso, S. BATTAGLIA, *Criminalità informatica al tempo di internet: rapporti tra* phishing *e riciclaggio*, in *Altalex,* 18 settembre 2014. Consultabile al sito: https://www.altalex.com/documents/news/2014/03/28/criminalita-informatica-al-tempo-di-internet-rapporti-tra-phishing-e-riciclaggio; E. BASSOLI (a cura di), *I crimini informatici, il dark web e le web room*, Pisa, 2021 e, da ultimo, F. CORONA (a cura di), *Reati informatici e investigazioni digitali*, Pisa, 2021. Alcune interessanti ricerche in tal senso sono state pubblicate sui siti di Mandiant e di Visa; L. PICOTTI, *"Nuovi" crimini cibernetici e possibile rilevanza dell'intelligenza artificiale*, in *Stati Generali del Diritto di Internet*, Atti del Convegno Luiss, Roma, 16, 17, 18.12.2022, I.

La posizione giuridica del financial manager ha sollevato un importante interrogativo: invero, il dibattito dottrinale e giurisprudenziale verte sulla configurabilità o meno, in capo allo stesso, del delitto di riciclaggio.

La giurisprudenza di legittimità[22] ha chiarito che questi risponde a titolo di concorso nei medesimi delitti realizzati dal phisher solo se abbia agito con la consapevolezza del disegno criminoso posto in essere.

Al contrario, il financial manager risponderà di ricettazione o di riciclaggio, a seconda che si sia limitato a ricevere le somme di denaro, consapevole della loro provenienza illecita, ovvero le abbia anche trasferite all'estero con modalità idonee ad ostacolare l'identificazione di tale provenienza[23].

Questo orientamento è stato autorevolmente sancito con la sentenza 1° luglio 2011, n. 25960, ove la Suprema Corte ha richiamato l'orientamento delle Sezioni Unite in tema di compatibilità del dolo eventuale con il delitto di ricettazione[24].

Quanto appena segnalato è soltanto un esempio di utilizzo abusivo delle nuove tecnologie informatiche per la realizzazione di propositi criminosi: l'origine del cyberspace, dimensione sconfinata e multiforme, pertanto difficilmente controllabile, ha comportato uno spostamento online delle attività delle organizzazioni criminali. Nascono, così, nuove forme di ipotesi delittuose, minacce concrete della sicurezza economica e sociale, nazionale ed internazionale.

I criminali che operano sul web sfruttano anche l'anonimato (sostanzialmente) garantito dalle monete virtuali, le quali consentono trasferimenti rapidi e di cui è difficile rintracciare gli autori. Difatti, il Bitcoin viene ampiamente utilizzato, così come le nuove tipologie di virtual assets[25] che si avvalgono della blockchain, proprio per riciclare denaro. La blockchain si presta infatti a soddisfare le principali esigenze dei riciclatori, quindi «globalizzazione, dematerializzazione ed anonimizzazione delle transazioni»[26], e allo stesso tempo garantisce anche l'occultamento del valore del trasferimento. Queste caratteristiche sono corollario della struttura delle transazioni, non supervisionate da un intermediario ma gestite tra utenti (peer to peer)[27].

È stato osservato che più che di anonimato sarebbe corretto parlare di "pseudoanonimato", dal momento che le transazioni sono registrate in un

[22] *Cass. Pen., sez. II, sent. 17.06.2011, n. 25960, in Guida al diritto*, 2011, 44, 76.

[23] Si veda, A. SCIRÈ, *In tema di riciclaggio informatico, dolo eventuale e frode informatica mediante 'phishing', nota a Cass. Pen., Sez. II, 17.06.2011 (dep. 01.07.2011), n.* 25960, in *Dir. Pen. Cont.*, 2011 e R. RAZZANTE, *Riciclaggio e reati connessi. Applicazioni giurisprudenziali e di vigilanza,* Milano, 2023.

[24] Cfr. Cass. Pen., SS.UU., sent. 26.11.2009, n. 12433, in *Guida al diritto*, 2010, 20, 80.

[25] Per approfondire, R. RAZZANTE, *Tracciabilità e riciclaggio: binomio indissolubile tra gli artt. 648 bis e ter c.p. e la recente entrata in vigore del delitto di autoriciclaggio, nota a Cass. Pen., Sez. II, 22 ottobre 2014, n. 43881*, in *Arch.Pen.*, 2014; S. BONFANTE, *Quella incerta linea di confine tra il phishing ed il riciclaggio*, in *Il Penalista*, 28 aprile 2017 e, da ultimo, R. RAZZANTE, *Bitcoin e criptovalute. Profili fiscali, giuridici e finanziari*, Santarcangelo di Romagna, 2018. In giurisprudenza, si veda Cass. Pen., sez. II, sent. 09.02.2017, n. 10060, in *Diritto & Giustizia*, 2017.

[26] Così A. LAUDATI, *Cybercrime e cryptovalut*e, in R. RAZZANTE (a cura di), *Dizionario dell'antiterrorismo,* Roma, 2022, 211-230; R. RAZZANTE, A. CRISTALLINI, *op.cit.*, 5 ss.

[27] Per ulteriori approfondimenti sul tema si veda R. RAZZANTE., *Bitcoin tra diritto e legislazione,* in *Notariato*, 2018, IV.

distributed ledger pubblico [28] ; tuttavia, l'esistenza di un registro delle operazioni, sebbene utile per la tracciabilità, non garantisce la rintracciabilità delle persone fisiche o giuridiche celate dietro i wallet[29].

Anche a livello giurisprudenziale [30] è aumentata la sensibilità rispetto ai potenziali impieghi delle valute virtuali per porre in essere reati di riciclaggio e autoriciclaggio.

A tal proposito è stato osservato, infatti, che concettualmente la dimensione "virtuale" dei reati compiuti con criptovalute non incide sulla formazione della fattispecie criminosa: il fatto che le condotte di occultamento di proventi illeciti abbiano luogo nel cyberspace non esclude il reato di autoriciclaggio, così come se il reato presupposto avviene online e il riciclaggio è offline si avrà comunque l'imputazione per riciclaggio.

La Suprema Corte ha esplicitato come anche la moneta virtuale, se impiegata per investire profitti di origine delittuosa in operazioni finanziarie speculative [31], possa essere ricondotta alla fattispecie di autoriciclaggio [32]: «Anche la moneta virtuale (cosiddetto bitcoin) può rientrare tra gli strumenti finanziari e speculativi presi in considerazione dalla norma incriminatrice dell'autoriciclaggio, in quando l'indicazione normativa di cui all'articolo 648 ter.1 del Cp delle attività (economiche, finanziarie, imprenditoriali e speculative) in cui il denaro, profitto del reato presupposto, può essere impiegato o trasferito individua delle macro aree tutte accomunate dalla caratteristica dell'impiego finalizzato al conseguimento di un utile e, in questa prospettiva, le valute virtuali ben possono essere ricondotte nell'ambito della dizione di "attività speculativa" in quanto possono essere utilizzate per scopi diversi dal pagamento e comprendere prodotti di riserva di valore a fini di risparmio ed investimento. Del resto, il sistema di acquisto di bitcoin si presta ad agevolare condotte illecite, in quanto è possibile garantire un alto grado di anonimato, senza tra l'altro alcun controllo sulla provenienza del denaro convertito» (cfr. Cass. Pen., Sez. II, 13 luglio 2022, n. 27023).

Si può osservare, da ultimo, che la giurisprudenza si è trovata a dover svolgere una funzione definitoria a proposito dell'impiego delle criptovalute, per scopi leciti o illeciti, anche al di fuori dell'ambito del riciclaggio e dell'autoriciclaggio. Si sta verificando un progressivo avvicinamento della moneta virtuale al denaro; tuttavia, ancora ci sono degli aspetti in via di definizione.

---

[28] In tal senso, L. STURZO, *Bitcoin e riciclaggio*, in *Dir. Pen. Cont.*,2018, V, 21 e R. RAZZANTE, *Autoriciclaggio con bitcoin: nuove impostazioni criminali e giurisprudenziali*, in *Il Penalista*, 28 febbraio 2022.

[29] A tal proposito L. LA ROCCA, *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*, in *Analisi Giuridica dell'Economia,* 2015, I, 201 -222.

[30] La tematica delle criptovalute è stata affrontata per la prima volta nel 2017 dalla giurisprudenza nazionale, vedi Trib. Verona, sent. 26.01.2017, n. 195, in *Foro It.*, 2017.

[31] Cfr. F. COLAZZO, *Investire i profitti della truffa per acquistare criptovalute integra il reato di autoriciclaggio*, *nota a Cass. Pen., Sez. II, 13 luglio 2022, n. 27023*, in *Antiriciclaggio & Compliance,* 2022.

[32] Si raccomanda G. J. SICIGNANO, *La responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali*, Pisa, 2021.

7. Il fenomeno del cyberterrorismo.

Il cyberterrorismo, come il terrorismo tradizionale, presenta un notevole problema definitorio. Questa lacuna deriva, a monte, dall'incertezza nell'inquadrare il fenomeno già da un punto di vista fattuale e reale.

Il dibattito in merito alla questione terminologica si amplia se si tiene conto dei pareri degli esperti: alcuni di essi negano azioni di cyberterrorismo, mentre altri ritengono che alcuni gruppi ricorrano sistematicamente alla rete [33]. È indubbio come la stessa società dell'era digitale, impiegando la tecnologia informatica e telematica in settori sempre più ampi, abbia consentito ai gruppi terroristici di poter accedere con maggiore facilità alle informazioni circa le cc.dd. infrastrutture critiche, quali sistemi di difesa nazionali, sistemi di controllo e di trasporto di persone e merci, sistemi di controllo di fonti energetiche, sistemi sanitari e circuiti economico-finanziari. Di fatto, dunque, il livello di progresso tecnologico che una società riesce a raggiungere si affianca, parallelamente e proporzionalmente, ad una maggiore vulnerabilità rispetto ai potenziali rischi cyber.

È così che due dei più rilevanti rischi che gli Stati sono chiamati a prevenire e ad affrontare sono il pericolo cyber ed il terrorismo; quest'ultimo, in particolare, rappresenta un fattore di destabilizzazione degli assetti internazionali, soprattutto sul versante della sicurezza interstatale, anche alla luce delle sue nuove modalità di manifestazione, che si sono adeguate senza fatica alla rivoluzione digitale.

I singoli Stati e, più in generale, l'intera compagine mondiale, si trovano, infatti, a fronteggiare un fenomeno *sui generis*, che presenta caratteri e modalità di manifestazione indeterminati, volatili e ubiquitari, in grado di penetrare le strutture delle moderne società occidentali, anche tramite canali informatici. Per queste ragioni è sentita l'esigenza di approntare strumenti di cooperazione sinergica sia da un punto di vista esterno (tra Stati, federazioni e organizzazioni internazionali), sia interno (tramite la predisposizione di un sistema sanzionatorio nazionale idoneo a contrastare queste minacce).

Proprio grazie allo sviluppo della rete si è affermato il c.d. cyberterrorismo, una particolare declinazione del terrorismo tradizionale, che ha cambiato la natura e le modalità delle minacce alla sicurezza internazionale, rendendole più dinamiche e fluide rispetto al passato. È il caso del terrorismo c.d. globalizzato di matrice islamica, la cui prima manifestazione risale agli attentati dell'11 settembre 2001, destinato a divenire un modello più efficiente e incisivo delle forme ordinarie di criminalità terroristica.

É noto come le organizzazioni terroristiche fondamentaliste, tipo Daesh o Al Quaeda, utilizzino strumenti informatici e di comunicazione per finalità non solo propagandistiche ma anche operative, come ad esempio il controllo o il comando dei cc.dd. 'lupi solitari' e delle cc.dd. 'cellule dormienti'; inoltre, nello

[33] Si vedano sul punto, F. SPIEZIA, S. ORLANDI, *Misure antiterrorismo del Consiglio d'Europa,* in R. RAZZANTE (a cura di), *Dizionario dell'antiterrorismo*, Roma, 2022, 479-506, i quali osservano che: «L'uso della rete è il mezzo principale attraverso cui i terroristi perseguono i propri fini. Esso ingloba sia la fattispecie dei reati di cybercrime indirettamente collegati alle finalità di terrorismo (e per questo difficili da etichettare con il termine di cyberterrorismo in senso stretto), sia quelli direttamente finalizzati al terrorismo. Per tale motivo, cybercrime e cyberterrorismo necessitano di pari attenzione, essendo due fenomeni molte volte potenzialmente correlati tra loro».

stesso modo, si trasmettono le guide e le informazioni utili per la radicalizzazione e l'addestramento dei cc.dd. foreign fighters[34].

La rete, dunque, figura in ogni aspetto dell'organizzazione stessa e diviene essenziale per attività quali il reclutamento, il finanziamento e la propaganda.

In questo scenario, può osservarsi come gli attentati dell'11 settembre 2001[35] abbiano dato vita ad un nuovo paradigma di guerra, che si basa su una forma di conflittualità poco prevedibile nelle sue manifestazioni, nelle sue modalità, nei suoi tempi. Tale paradigma riflette la nuova strategia terroristica che, da nazionale a transazionale, è diventata di tipo globalizzato. Questa transizione è stata in larga parte agevolata dall'impiego di strumenti informatici, grazie ai quali le organizzazioni terroristiche hanno potuto raggiungere un'audience mondiale. La rete accresce la forza e la propagazione del terrorismo perché riesce a trasformare un evento geograficamente delimitato in un evento aspaziale e atemporale di risonanza globale.

Da ultimo, la rete consente una diffusione della propaganda ad un bacino di utenti sempre più ampio – soprattutto giovani. È divenuto, infatti, imprescindibile ricorrere a siti Internet, anche all'interno del c.d. dark web, per garantire stabilità a tutte le attività strumentali all'organizzazione stessa, quali l'affiliazione, il finanziamento, la promozione di iniziative criminose, le raccolte di fondi attraverso collegamenti tra le singole organizzazioni.

Per quanto concerne il reclutamento, anch'esso avviene tramite l'impiego di strumenti informatici, in particolare delle piattaforme quali Facebook, Twitter, Instagram, ma anche blog e siti di dating online; successivamente, la fase della radicalizzazione si consuma in un ambiente virtuale privato, terreno fertile per familiarizzare con l'organizzazione. Inoltre, il web consente l'estrazione di dati – c.d. data mining – che permettono di reperire non solo informazioni su infrastrutture critiche, quali trasporti, edifici pubblici, aeroporti e porti, ma anche informazioni sulla predisposizione di armi chimiche ed esplosivi. Per concretizzare una minaccia sarebbero necessari degli attacchi simultanei a differenti obiettivi strategici e una loro protrazione nel tempo; successivamente, si dovrebbe generare un riverbero mediatico tale da destabilizzare l'opinione pubblica e la società tutta.

L'impiego abituale di strumenti tecnologici nello scambio di informazioni[36], nella raccolta dati e nel reclutamento da parte delle organizzazioni criminali è confermato da alcune investigazioni svolte in seguito agli attentati dell'11 settembre 2001. È necessario, però, sottolineare come non sempre queste azioni siano sic et simpliciter di natura terroristica, potendo rientrare anche nell'uso ordinario della rete. A tal proposito, in dottrina si sono delineati due orientamenti definitori del cyberterrorismo; nel primo, target oriented, la rete è intesa come obiettivo e come arma, e ne sono un esempio i casi di danneggiamento, di distruzione o di compromissione di sistemi informatici e di strutture critiche di un Paese; nel secondo, tool oriented, la rete è considerata uno strumento e un supporto, come nelle operazioni di gestione, propaganda,

[34] *Ibidem*, 481 ss.

[35] P. ANGELOSANTO, *Unità antiterrorismo*, in R. RAZZANTE (a cura di), *Dizionario dell'antiterrorismo*, Roma, 2022, 605 ss.

[36] Si rinvia a R. INCUTTI, *Il contrasto al terrorismo attraverso la cooperazione giudiziaria internazionale*, in R. RAZZANTE (a cura di), *Dizionario dell'antiterrorismo*, Roma, 2022, 155 ss.

reclutamento e raccolta fondi. A fronte di questa distinzione, è opportuno rilevare come ancora non si verifichino attacchi ascrivibili al primo orientamento; mentre l'impiego del cyberspazio come strumento per perseguire gli scopi delle associazioni terroristiche è ormai un *modus operandi* ineludibile.

Dorothy Denning, nel qualificare il terrorismo informatico, lo definisce come «[…] la convergenza del concetto di cyberspazio e di terrorismo; generalmente è inteso come l'attacco illegale e/o minaccia di attacco contro i computer, le reti, e le informazioni in essi memorizzate, eseguito per intimidire o costringere un governo o la sua gente ad assoggettarsi a obiettivi politici o sociali. Inoltre, per qualificarsi come cyberterrorismo, un attacco dovrebbe essere caratterizzato da violenza contro persone o cose, o essere in grado di causare danni talmente ingenti, tali da generare paura. Sono da considerarsi esempi di attacchi gravi quelli che portano morte o lesioni, nonché esplosioni, incidenti aerei, contaminazione delle acque, o grave perdita economica. Analogamente, possono essere considerati gli attacchi contro le infrastrutture critiche, a seconda del loro impatto»[37].

Occorre, dunque, tracciare un confine tra i casi in cui, come riportato, si verificano attacchi che si risolvono in una lesione di beni giuridici primari della vita o in un danneggiamento di infrastrutture critiche, e i casi, di maggior tenuità, in cui si verificano danni economici meno rilevanti.

In conclusione, la rete svolge un ruolo primario nel mantenimento e nell'operatività delle organizzazioni criminali: dalla commistione tra il terrorismo e gli strumenti informatici nasce un nuovo pericolo, smaterializzato, delocalizzato e, spesso, imprevedibile.

A fronte della natura peculiare del fenomeno *de quo*, è utile analizzare gli strumenti approntati dal legislatore, nazionale e sovranazionale. La mancanza di efficaci misure di natura extra-penale rende possibile il ritorno ad una disciplina penalistica che ricalca la teoria del c.d. diritto penale del nemico[38] per contrastare le organizzazioni terroristiche islamiche.

In un ambito in cui è necessario attuare una tutela preventivo-repressiva, si concretizza il rischio di una risposta legislativa, sostanziale e processuale, non conforme ai principi costituzionali di riserva di legge, offensività e giusto processo, ex artt. 25 co. 2, 111 Cost. e artt. 6 e 7 CEDU, per un duplice ordine di ragioni. La prima si risolve nell'inadeguatezza dei sistemi di difesa informatici statali che, a monte, dovrebbero fungere da protezione[39]. La seconda è legata alla natura ibrida del fenomeno terroristico e cyberterroristico, che rende necessario trovare una sintesi tra discipline giuridiche ed extragiuridiche, come l'informatica.

Lo spazio virtuale, infatti, non presenta un substrato giuridico di riferimento che ne disciplini il funzionamento e i limiti; il legislatore, dunque, dovendosi

---

[37] D. E. DENNING, *Cyberterrorism*, Georgetown, 2000. Consultabile al sito: www.cs.georgetown.edu.

[38] Sul tema, U. NAZZARO, *Il diritto penale del nemico tra delitto di associazione politica e misure di contrasto al terrorismo internazionale*, Napoli, 2016; E. KALICA, *La pena di morte viva: Ergastolo, 41 bis e diritto penale del nemico*, Sesto San Giovanni, 2019; P. BRUNETTI, *Diritto penale del nemico: una lettura critica dei presupposti filosofici*, in *Penaledp*, 29 maggio 2020; R. PUCA, *La teoria del diritto penale del nemico di Günther Jakobs tra funzionalismo luhmanniano e populismo penale*, in D. RONCO, A. SBRACCIA, V. VERDOLINI (a cura di), *La violenza penale: conflitti, abusi e resistenze nello spazio penitenziario*, in *Riv. Antigone,* 2020, II.

[39] Ancora, P. ANGELOSANTO, *op. cit.*, 524.

interfacciare con una dimensione non retta da uno Stato di diritto, opta, talvolta, per un arretramento della soglia di rilevanza penale, mediante la previsione, quali reati consumati, di condotte meramente preparatorie rispetto ad eventuali successivi delitti od effettive lesioni dei beni giuridici protetti, come nei casi di detenzione o in cui l'illiceità dipende soltanto dal fine specifico dell'agente. Questa anticipazione, se ben si concilia con le citate esigenze preventivo-repressive, potrebbe confliggere con il principio di offensività.

Alla luce di queste considerazioni, il bilanciamento tra interessi rilevanti e meritevoli di tutela è lo strumento primario di cui il legislatore si deve servire, per evitare, da un lato, che le finalità repressive eclissino i diritti costituzionali degli individui e, dall'altro, che le esigenze di tutela contro i fenomeni terroristici non trovino realizzazione.

In particolare, ponendo l'attenzione sulla predisposizione delle singole fattispecie incriminatrici, il rischio da paventare è quello che la risposta sanzionatoria sia parametrata non già sul fatto di reato, quanto piuttosto sull'autore e, nella maggior parte dei casi, su alcune manifestazioni di pensiero o di religione.

Sul piano del diritto penale sostanziale ancora non è stata prevista una fattispecie unitaria che tipizzi il terrorismo cibernetico, fenomeno che presenta denominatori comuni alla criminalità informatica e al terrorismo tradizionale. Questa convergenza è evidente negli attacchi informatici a motivazione politica, attuati con la finalità di cagionare gravi e, spesso irreversibili, danni all'istituzioni, all'economia, alla vita e all'integrità fisica.

Si tratta ora di delineare, se pur brevemente, l'*excursus* normativo e gli interventi del Legislatore dell'UE sulla tematica che si sta trattando.

La Convenzione di Budapest sul Cybercrime del 2001 è stata ratificata con la legge 18 marzo 2008, n. 48, e ha introdotto nuove fattispecie, in alcuni casi apportando modifiche alle preesistenti. In particolare, si ricordano l'art. 635-*bis* c.p., recante Danneggiamento di informazioni, dati e programmi informatici, l'art. 635-*ter* c.p., recante Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stati e da altro ente pubblico o comunque di pubblica utilità; l'art. 635-*quater* c.p., recante Danneggiamento di sistemi informatici e telematici e l'art 635-*quinquies* c.p., recante Danneggiamento di sistemi informatici o telematici di pubblica utilità.

In seno all'Unione europea, il fenomeno terroristico viene in considerazione già all'interno del Trattato sul funzionamento dell'Unione Europea, che al suo art. 222 inserisce una clausola di solidarietà, prevedendo che l'Unione e i singoli Stati agiscano congiuntamente laddove «uno Stato membro sia oggetto di un attacco terroristico». Pacificamente, si possono far rientrare nella disposizione i casi in cui l'effetto dell'attacco si sostanzi nell'impiego di strumenti informatici.

Per quanto concerne la ripartizione delle competenze tra legislatore nazionale e sovranazionale, nell'art 83, par. 1, del Trattato di Lisbona del 2009, la criminalità informatica e il terrorismo figurano tra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione europea ha competenza penale.

Con la Direttiva 2013/40/UE del 12 agosto 2013[40], relativa agli attacchi contro i sistemi di informazione, che ha imposto un irrigidimento sanzionatorio ed una cooperazione di polizia e giudiziaria tra gli Stati membri, l'Unione ha posto l'attenzione anche sulla salvaguardia delle cc.dd. infrastrutture critiche, vulnerabile punto di apertura per le organizzazioni criminali.

La successiva Direttiva 2017/541/UE del 15 marzo 2017, sulla lotta conto il terrorismo, ha recepito il concetto di cyberterrorismo come crasi tra lo spazio cibernetico e il terrorismo. L'art 21 della Direttiva, recante Misure per contrastare i contenuti online riconducibili alla pubblica provocazione, imponeva agli Stati di predisporre strumenti per intervenire rapidamente nella rimozione di contenuti online che rappresentano, per l'appunto, una provocazione a commettere reati di terrorismo; tale disposizione è sintomatica della ormai consolidata consapevolezza che le organizzazioni terroristiche si avvalgono di Internet per attività di inneggiamento e di reclutamento.

Nella disposizione in esame si ha riguardo anche delle richiamate esigenze di bilanciamento, prevedendo, al par. 3, che tali misure debbano in ogni caso essere stabilite secondo procedure trasparenti e fornire idonee garanzie, in particolare al fine di assicurare che tali misure siano limitate allo stretto necessario e proporzionate e che gli utenti siano informati del motivo di tali misure.

Nel contesto descritto, deve aggiungersi l'utilizzo delle valute virtuali per scopi illeciti che, progressivamente, ha assunto una dimensione sempre più vasta, come testimonia ad esempio l'operazione condotta dal Dipartimento di Giustizia americano (DoJ) nel 2020. In quella sede, si rilevava come Al-Quaeda e Al-Quassam invitassero, tramite social network - tra cui, apertamente, Facebook – ad effettuare donazioni in Bitcoin per il finanziamento di attività quali l'acquisto di armi; l'esito delle indagini ha visto sequestrati 3 milioni di dollari, 300 account di criptovalute, 4 siti web e 4 pagine Facebook.

Il legislatore interno, per far fronte al fenomeno de quo, ha introdotto, con la Legge 17 aprile 2015, n. 43, l'art. 470-*quinquies* 1, c.p., rubricato Finanziamento di condotte con finalità di terrorismo; la disposizione, rappresentativa della tendenza all'anticipazione della soglia di rilevanza penale per comportamenti apparentemente solo prodromici al compimento di atti terroristici, prevede che «Chiunque, al di fuori dei casi di cui agli articoli 270-bis e 270-quater 1, raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo di cui all'articolo 270-*sexies*, è punito con la reclusione da sette a quindici anni, indipendentemente dall'effettivo utilizzo dei fondi per la commissione delle citate condotte».

[40] La Direttiva 2013/40/UE del Parlamento e del Consiglio del 12 agosto 2013 è consultabile su www.eur-lex.europa.eu. Si rinvia, altresì, a F. SPIEZIA, A. CONTINISIO, *Misure antiterrorismo del Consiglio d'Europa*, in R. RAZZANTE (a cura di), *Dizionario dell'antiterrorismo*, Roma, 2022,., 458, a detta dei quali: «Il Consiglio d'Europa apporta un particolare valore aggiunto agli sforzi regionali e globali per prevenire e reprimere il terrorismo attraverso le sue attività di definizione di standard, che mirano a fornire quadri giuridici efficaci, e compatibili con i diritti umani e lo stato di diritto, per la cooperazione tra gli Stati membri, ma anche attraverso le altre attività volte a prevenire la radicalizzazione che porta al terrorismo e, più in generale, a consolidare la democrazia. Il Consiglio d'Europa è determinato a proseguire gli sforzi per promuovere i suoi standard, sia a livello regionale che globale, in stretta cooperazione e coordinamento con gli Stati membri e con altre organizzazioni regionali e globali, comprese le Nazioni Unite».

Nella predisposizione della fattispecie è stata inserita una clausola di apertura rispetto al quomodo della realizzazione del bene o denaro, che consente di farvi rientrare anche le criptovalute, attesa ormai la loro pacifica natura di bene virtuale[41].

Successivamente, il Consiglio d'Europa, su impulso del Comitato per la lotta al Terrorismo (CDCT), ha adottato, sempre nel 2018, una Strategia quinquennale contro il terrorismo; questa si declina in tre punti principali: la prevenzione del fenomeno, il perseguimento dei reati ad esso connessi e la protezione degli Stati membri. In particolare, si auspicava l'adozione sia di misure di law enforcement per rilevare ed impedire attacchi terroristici, sia di un sistema in grado di prevenire fenomeni di radicalizzazione. Inoltre, si individuava, tra gli obiettivi prioritari, quello di approntare un sistema di cooperazione giudiziaria ed internazionale al fine di assicurare non soltanto l'effettività della pena per i responsabili, ma anche la sicurezza degli Stati membri.

Il Legislatore sovranazionale, conscio di come l'attività di addestramento sia ormai agevolata – e quindi, amplificata - dalla rete, nell'undicesimo considerando della Direttiva 2017/541/UE[42], precisava che: «La qualificazione come reato dell'atto di ricevere un addestramento a fini terroristici integra il reato esistente consistente nell'impartire addestramento […] L'atto di ricevere addestramento a fini terroristici comprende l'acquisizione di conoscenze, documentazione o abilità pratiche. L'autoapprendimento, anche attraverso Internet o la consultazione di altro materiale didattico, dovrebbe altresì essere considerata ricevere addestramento a fini terroristici qualora derivi da una condotta attiva e sia effettuato con l'intento di commettere o di contribuire a commettere un reato di terrorismo».

Con la seguente Risoluzione del 13 giugno 2018 sulla cyberdifesa[43], il Parlamento europeo constatava come il cyberspazio sia uno strumento «a basso costo», in grado di flettersi ad ogni esigenza delle reti transnazionali criminali, dando vita ad una minaccia senza precedenti. Occorreva ribadire l'opportunità di predisporre una cooperazione più intensa e strutturata con le forze di Polizia, in una prospettiva di prevenzione rispetto a minacce connesse alla jihad informatica, il terrorismo informatico, la radicalizzazione online e il finanziamento di organizzazioni estremiste o radicali.

Un ulteriore apporto è rappresentato dalla Direttiva 2018/1808/UE del 14 novembre 2018, con la quale si prescriveva agli Stati di approntare un sistema di vigilanza sui contenuti audiovisivi volto ad impedire che siano veicolati contenuti che inneggino alla commissione di reati di terrorismo tramite strumenti di comunicazione di massa. Sebbene non si tratti di un intervento afferente al versante degli strumenti informatici strictu sensu, è comunque sintomatico della consapevolezza da parte dell'Unione della necessità di adottare un approccio onnicomprensivo nei confronti delle minacce terroristiche.

---

[41] In proposito si veda A. LAUDATI, *Cybercrime e criptovalute*, *op. cit.*, 212 ss.

[42] Direttiva 2017/541/UE sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la Decisione 2005/671/GAI del Consiglio.

[43] Si veda, Risoluzione del Parlamento europeo sulla ciberdifesa (2018/2004(INI)). Consultabile al sito: www.eur-lex.europa.eu, 13 giugno 2018.

Inoltre, l'11 dicembre 2018, la Commissione europea ha presentato una proposta di Regolamento, COM/2018/845, in cui si propone di inserire nell'alveo dei contenuti terroristici online una serie di condotte, quali «(a) istigazione, anche mediante l'apologia del terrorismo, alla commissione di reati di terrorismo, generando in tal modo il pericolo che tali reati siano effettivamente commessi; (b) incitamento a contribuire a reati di terrorismo; (c) promozione delle attività di un gruppo terroristico, in particolare incoraggiando la partecipazione o il sostegno a un gruppo terroristico […] (d) istruzioni su metodi o tecniche allo scopo di commettere reati di terrorismo».

La Commissione europea, il 14 aprile 2021, ha presentato la Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025[44], in cui particolare riguardo è riservato ai crimini informatici; a tal proposito, infatti, si sottolinea come: «Oltre l'80 % dei reati ha oggi una componente digitale» e, a seguire, che «Le autorità di contrasto e giudiziarie devono stare al passo con le tecnologie in rapido sviluppo utilizzate dai criminali e con le loro attività transfrontaliere. Ciò richiede un coordinamento nello sviluppo di strumenti e formazioni tra gli Stati membri». Ciò che emerge è l'ambizione di rafforzare la cooperazione comunitaria, varando anche un Codice unico europeo nell'ambito della lotta al riciclaggio al fine di espungere dal circuito economico gli utili generati alla criminalità organizzata e prevenirne l'infiltrazione nell'economia digitale e nella società.

La Commissione si mostra sensibile rispetto alla problematica del finanziamento delle associazioni criminali attraverso le moderne valute virtuali. Infatti, il punto di convergenza tra la dimensione terroristica e quella del cyberspazio è, oggi, emblematicamente rappresentato dalle criptovalute. Questo strumento vanta, tra i suoi punti di forza, l'anonimato e l'immediatezza nell'effettuare transazioni, peculiarità che ne rendono l'impiego particolarmente appetibile nelle attività di finanziamento delle organizzazioni criminali.

Due settimane dopo la presentazione della strategia della Commissione, il 29 aprile 2021 è stato approvato il Regolamento 2021/784/UE, recante disposizioni di Contrasto della diffusione di contenuti terroristici online. In particolare, in capo ai prestatori di servizi di hosting sono prescritti, all'art. 6, degli obblighi volti a prevenire la diffusione di contenuti terroristici all'interno delle relative piattaforme; eventuali contenuti illeciti dovranno essere conservati presso gli stessi per sei mesi dalla rimozione o dalla disabilitazione, per consentirne il vaglio da parte delle Autorità competenti. Laddove i prestatori non dovessero procedere alla rimozione, l'art. 3 riconosce alle autorità competenti del singolo Stato il potere di emettere un ordine di rimozione del contenuto, che dovrà essere adempiuto prontamente, entro un'ora dal suo ricevimento[45].

Sempre in ottica sovranazionale, è doveroso porre l'attenzione sull'attualità della problematica del cyberterrorismo, alla luce del conflitto tra Russia e Ucraina che si sta consumando in Occidente. In particolare, già il 13 gennaio

[44] Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025. Consultabile al sito: www.eur-lex.europa.eu

[45] Si veda sul tema, F. SPIEZIA, S. ORLANDI, *Misure antiterrorismo dell'Unione Europea*, *op.cit.*, 493 ss.

2022 era stato rilevato un malware – WhisperGate[46] – che aveva coinvolto alcune istituzioni governative ucraine. Successivamente, alcuni ricercatori di sicurezza rilevavano un'operazione di attacco da parte del collettivo russo Gamaredon – anche noto come Armageddon o Shuckworm[47]. Dall'inizio della guerra, il 20 febbraio 2022 l'attività di hackeraggio da parte della Federazione russa nei confronti delle infrastrutture rilevanti dell'Ucraina pare non essersi mai arrestata, ed anzi secondo il Servizio delle Comunicazioni Speciali e della Protezione dell'Informazione dello Stato Ucraino (SSSCIP), gli attacchi rilevati si aggirano intorno ai 1123, a danno dei siti governativi, del Ministero delle Infrastrutture, degli Esteri, degli Affari e dell'Educazione e della Banca Nazionale ucraina. La cyber-war si consuma attraverso attacchi DDoS, campagne di disinformazione e attività distruttive di sabotaggio con malware. L'Ucraina, tramite l'Ukraine Cyber Troops, una divisione del Ministero della Difesa, ha portato a compimento numerose operazioni informatiche offensive contro gli obiettivi governativi russi[48].

L'ACN – Agenzia per la Cybersicurezza Nazionale italiana – si è attivata tramite lo CSIRT che, già nel 24 febbraio 2022, aveva segnalato un significativo rischio cyber derivante da possibili impatti collaterali a carico di infrastrutture ITC interconnesse con il cyberspazio ucraino. Altri paesi, quali Lituania, Croazia, Polonia, Estoni, Romania e Paesi Bassi, hanno attivato un Cyber Rapid Response Team, in risposta alla richiesta di sostegno ucraina.

8. (Segue) La cybersicurezza in Italia: sviluppi del 2022.

Da ultimo, è utile segnalare le ultime novità del 2022 in tema di sicurezza cibernetica in Italia, compresa tra i progetti finanziati dal Piano nazionale di ripresa e resilienza (PNRR), in attuazione del quale è stato adottato il decreto - legge n. 82 del 2021, che ha definito la governance del sistema nazionale di sicurezza cibernetica.

Il sistema ha, al suo vertice, il Presidente del Consiglio dei ministri cui è attribuita l'alta direzione e la responsabilità generale delle politiche di cybersicurezza e a cui spetta l'adozione della relativa strategia nazionale e la nomina dei vertici della nuova Agenzia per la cybersicurezza nazionale. Il Presidente del Consiglio dei ministri può delegare alla Autorità delegata per il sistema di informazione per la sicurezza della Repubblica le funzioni che non sono a lui attribuite in via esclusiva. Presso la Presidenza del Consiglio dei ministri, è istituito il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza. L'Agenzia per la cybersicurezza nazionale (ACN) è istituita a tutela degli interessi nazionali nel campo della cybersicurezza.

---

[46] P. TAVARES, *WhisperGate: A destructive malware to destroy Ukraine computer systems*, in *Infosec*, 25 maggio 2022. Consultabile al sito: www.resources.infosecinstitute.com.

[47] *Shuckworm: Russia-Linked Group Maintains Ukraine Focus*, in *Symantec*, 15 agosto 2022. Consultabile al sito: www.symantec-enterprise-blogs.security.com.

[48] Si rinvia a *Russia's war on Ukraine: Timeline of cyber-attacks*, in *ThinkTank European Parliament*, 21 giugno 2022. Consultabile al sito: www.europarl.europa.eu.

Su questa specifica materia è intervenuto il decreto - legge 9 agosto 2022, n. 115 (c.d. DL Aiuti-bis), recante Misure urgenti in materia di energia, emergenza idrica, politiche sociali e industriali (c.d. Aiuti-*bis*), in particolare per il tramite dell'art. 37 e dell'art. 37-*quater.*

L'art. 37 prevede che il Presidente del Consiglio dei ministri possa autorizzare l'adozione di misure di intelligence di contrasto in ambito cibernetico, in caso di crisi o emergenza, anche con la cooperazione del Ministero della difesa.

L'autorizzazione è basata sulla valutazione che escluda, alla luce delle più aggiornate cognizioni informatiche e fatti salvi i fattori imprevisti e imprevedibili, che possa essere messa in pericolo o lesa la vita, l'integrità fisica, la personalità individuale, la libertà personale, la libertà morale, la salute o l'incolumità di una o più persone.

Nell'adottare le misure di intelligence, si prevede: la cooperazione del Ministero della difesa; il ricorso alle garanzie funzionali, di cui all'art. 17 della Legge 124/2007 (si tratta di una speciale causa di giustificazione che prevede la non punibilità del personale dei servizi che ponga in essere condotte previste dalla legge come reato, legittimamente autorizzate di volta in volta in quanto indispensabili alle finalità istituzionali di tali servizi, nel rispetto di limiti tassativi previsti dal medesimo articolo).

Le misure sono attuate dall'Agenzia informazioni e sicurezza esterna (AISE) e dall'Agenzia informazioni e sicurezza interna (AISI), con il coordinamento del Dipartimento delle informazioni per la sicurezza (DIS), ossia gli organismi operativi dei servizi di intelligence.

Il Presidente del Consiglio dei ministri informa il Comitato parlamentare per la sicurezza della Repubblica (Copasir) delle misure adottate con le modalità di cui all'art. 33, comma 4, della Legge 124/2007. Il richiamato art. 33 stabilisce che il Presidente del Consiglio dei ministri informa il Copasir circa le operazioni condotte dai servizi di informazione per la sicurezza nelle quali siano state poste in essere condotte normalmente previste dalla legge come reato, ma autorizzate da disposizioni di legge, quali l'art. 18 della Legge 124/2007 e l'art. 4 del D. L. n. 144/2005. In particolare, si prevede che le informazioni devono essere inviate al Copasir entro 30 giorni dalla data di conclusione delle operazioni.

A sua volta il Copasir, dopo ventiquattro mesi, trasmette alle Camere una relazione sull'efficacia delle suddette disposizioni.

Restano ferme le competenze del Ministero della difesa ai sensi dell'art. 88 del Codice dell'ordinamento militare e del Ministero dell'interno di cui all'art. 7-*bis* del decreto-legge n. 144/2005, recante Misure urgenti per il contrasto del terrorismo internazionale.

A ben vedere, si tratta di una nuova arma contro gli hacker e questa innovazione non può che considerarsi positiva e rivolta al futuro: i sistemi di difesa devono azionarsi per preservare e proteggere anche lo spazio virtuale, e non solo quello fisico, aereo e terrestre, come già suggerito da tempo, e sotto il coordinamento dell'intelligence e della difesa.

Degno di nota è anche l'art. 37-*quater* del c.d. DL Aiuti-*bis*, posto che estende gli obblighi di notifica attualmente previsti per gli incidenti aventi impatto su beni destinati a essere impiegati nel Perimetro di sicurezza nazionale

cibernetica (beni ICT), anche agli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (diversi quindi dai beni ICT), ma che sono di pertinenza di soggetti inclusi nel Perimetro *de quo*. Viene fatta salva la disciplina vigente per gli incidenti a reti del Ministero della difesa.

A ben vedere, l'art. 37-*quater* interviene in particolare sull'articolo 1 del decreto legge n. 105 del 2019 (c.d. decreto Perimetro), inserendo un nuovo comma 3-*bis* che, nel dettaglio, prevede che i soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica (P.A., enti e operatori pubblici e privati che svolgono funzioni istituzionali o essenziali per gli interessi dello Stato, individuati con apposito atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del CIC) notifichino anche gli incidenti, che hanno un impatto su reti, sistemi informativi e servizi informatici di propria pertinenza, pur non riguardando direttamente beni ICT.

Le novità sono di particolare importanza e si inseriscono nel solco già tracciato dal decreto-legge 17 maggio 2022, n. 50 (c.d. DL Aiuti), che aveva recentemente modificato l'art. 88 del Codice dell'ordinamento militare, al fine di inserire tra gli ambiti tutelati dalla difesa nazionale, quale funzione propria e principale dello strumento militare, oltre ai domini tradizionali (terrestre, marittimo ed aereo), anche i domini cibernetico e aero-spaziale. Come precisato dal Governo, la disposizione relativa alla difesa dello spazio cibernetico opera nel pieno rispetto delle competenze di tutte le altre amministrazioni coinvolte nello specifico settore: cyber resilience, in capo all'Agenzia per la Cybersicurezza Nazionale, cyber intelligence, di competenza del Dipartimento Informazioni per la Sicurezza e le collegate Agenzie, cyber crime & investigation, attestata al Ministero degli Interni. Allo stesso modo, afferendo esclusivamente ai profili di tutela militare delle infrastrutture spaziali (antenne, satelliti, strutture per la comunicazione satellitare, ecc.) strettamente connessi alla funzione di difesa nazionale, anche l'inclusione del dominio aero-spaziale non implica contrasti o sovrapposizioni di competenze, ma solo l'adeguamento dell'ambito di interesse della difesa nazionale.

9. Direttiva NIS (Network and Information Security).

La Direttiva NIS (Network and Information Security) è stata recepita dallo Stato italiano con il D. Lgs. 18 maggio 2018, n. 65, perseguendo l'obiettivo di proteggere le reti e i sistemi informatici sul territorio. L'esigenza di introdurre una Direttiva espressamente dedicata all'istituzione di un sistema uniforme sul piano europeo si è consolidata a seguito dell'aumento dell'incidenza degli attacchi cibernetici, in grado di paralizzare sistemi profondamente connessi, come le banche dati digitali o i dati raccolti su cloud.

Con la Direttiva NIS è stata messa in piedi una struttura preventiva e riparativa, per potenziare il livello globale di cybersicurezza nei Paesi membri, ampliando le tutele degli operatori dei servizi essenziali tramite strumenti normativi di garanzia e di prevenzione delle minacce cyber.

Invero, la NIS ha il merito di aver dotato gli Stati membri di una cornice legislativa, lasciando a ciascun Paese l'onere di specificare come gestire

l'attuazione degli obblighi previsti in sede UE[49]. In Italia è emersa, in occasione dell'attuazione della Direttiva, la necessità di prestare attenzione soprattutto alle risorse digitali della Pubblica Amministrazione, ai target di attacchi informatici così come agli enti e agli operatori nazionali pubblici e privati che forniscono servizi imprescindibili per il funzionamento della macchina statale.

Inoltre, è necessario ricordare che, a livello nazionale, gli interventi recenti in materia di cybersicurezza, sulla scia delle indicazioni del legislatore comunitario, sono stati in realtà molteplici; si pensi al decreto - legge 14 giugno 2021, n. 82, con cui è stata determinata l'architettura nazionale di cybersicurezza [50] ed è stata completata l'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN)[51]. Ancora, è stata valorizzata l'importanza di misure di cybersicurezza nel Piano nazionale di ripresa e resilienza (PNRR)[52].

10. (Segue) Direttiva NIS 2: i cambiamenti.

A rendere ancora più efficace la protezione di questi settori chiave hanno contribuito ulteriori disposizioni della Direttiva NIS2, approvata [53] dal Parlamento Europeo e, in via definitiva, dal Consiglio il 27 dicembre 2022, e, da ultimo, entrata in vigore il 17 gennaio 2023. Attraverso tale Direttiva si prevede una collaborazione potenziata tra Stati dell'Unione europea, al fine di prevenire e neutralizzare gli attacchi cyber.

La Direttiva NIS 2[54] si è resa indispensabile per fornire alle imprese strumenti in grado di fronteggiare le sfide di un futuro interconnesso e tecnologicamente complesso. Pertanto, da un lato, attraverso il coordinamento delle azioni messe in campo con l'istituzione di organismi di governo del meccanismo di protezione, di raccolta di segnalazioni di incidenti e di indirizzo della reazione; dall'altro lato, incentivando un'adesione delle aziende su base volontaria, rendendole così consapevoli del rischio cibernetico

Si prevede, quindi, anche il supporto fornito dalla rete CyCLONe (Cyber Crisis Liaison Organisation Network), nata nel 2020 per attuare una risposta

[49] A partire dal 2018 la Direttiva NIS (Network and Information System Security) ha rappresentato una pietra miliare per la costruzione di un sistema comune di difesa digitale. Si veda, E. PEZZUTO, *NIS2: l'evoluzione del quadro normativo UE per un livello comune di cybersicurezza*, in *Intelligence e Sicurezza*, 2022, IV.

[50] Il provvedimento prevede l'istituzione del Comitato interministeriale per la cybersicurezza (CIC) presso la Presidenza del Consiglio dei ministri e del Nucleo per la cybersicurezza presso l'ACN.

[51] L'Agenzia è l'autorità nazionale che si occupa di sicurezza cibernetica, sia in attuazione delle misure introdotte dalla Direttiva NIS che per svolgere le funzioni ispettive e irrogare per le sanzioni previste nel D. Lgs. 18 maggio 2018, n. 65 che ha recepito la normativa comunitaria.

[52] L'ultima versione del PNRR è stata trasmessa dal Governo alla Commissione europea il 30 aprile 2021, e definitivamente approvata il 13 luglio 2021.

[53] A. CANDINI, *Il Parlamento europeo approva la Direttiva NIS2 - Nuove e più stringenti misure per la Cybersecurity nell'Unione,* in *Il Sole 24 Ore*, 28 novembre 2022. Consultabile al sito: https://ntplusdiritto.ilsole24ore.com/art/il-parlamento-europeo-approva-direttiva-nis2-nuove-e-piu-stringenti-misure-la-cybersecurity-unione-AETUJnKC?refresh_ce=1.

[54] E. PEZZUTO, *op. cit.,* 2022; G. MARINO, *Cybersecurity comune nell'UE: ecco le ragioni di una NIS 2*, in *Agenda Digitale*, 24 novembre 2022. Consultabile al sito: https://www.agendadigitale.eu/sicurezza/cybersecurity-comune-nellue-ecco-le-ragioni-di-una-nis2/; F. CERCIELLO, *Direttiva NIS 2: ecco come prepararsi a recepire i nuovi obiettivi di cyber security,* in *Cybersecurity360*, 9 gennaio 2023. Consultabile al sito: https://www.cybersecurity360.it/cybersecurity-nazionale/direttiva-nis-2-ecco-come-prepararsi-a-recepire-i-nuovi-obiettivi-di-cyber-security/.

collettiva a livello europeo in caso di crisi informatiche ed assicurare uno scambio celere di informazioni in caso di necessità.

La Direttiva mira ad introdurre anche meccanismi per favorire la cooperazione tra le autorità competenti di ciascun Paese dell'UE, ampliando l'elenco formulato nella Direttiva NIS dei settori tenuti al rispetto di obblighi di cybersicurezza.

Ad ogni modo, a livello nazionale, nell'ambito della Direttiva NIS sono gli Stati membri a dover incoraggiare e vigilare sull'adozione, da parte dei soggetti pubblici e privati a capo delle infrastrutture critiche, di misure in grado di recuperare la funzionalità in breve tempo in caso di attacchi, e di strumenti di prevenzione e tutela di dette strutture[55].

La prevenzione nelle infrastrutture strategiche è stata ripesa anche nella Direttiva NIS2[56], secondo la quale è imprescindibile il perfezionamento delle tecniche di prevenzione e di esistenza ai fenomeni cyber all'interno dell'UE[57]; si propone, infatti, di integrare e di aggiornare le misure per la cybersicurezza al fine di ostacolare opportunamente le minacce informatiche.

Inoltre, la nuova Direttiva NIS2 rende obbligatoria la segnalazione degli incidenti di rilievo aventi ad oggetto strutture strategiche; le segnalazioni dovranno avere luogo entro 24 ore all'Autorità nazionale competente, dando modo di comprendere la gravità dell'attacco e informando anche gli utenti del servizio.

È previsto, inoltre, un obbligo di attivazione immediata, e un report più approfondito all'Autorità pubblica competente da consegnare entro 72 ore dall'incidente. Sulla base delle segnalazioni ricevute, l'Agenzia UE per la cybersicurezza (ENISA) dovrà realizzare delle raccolte di dati per individuare le maggiori criticità, al fine di poterle risolvere.

Ebbene, gli Stati membri hanno tempo fino all'ottobre 2024 per recepire le disposizioni della Direttiva in esame.

Si introducono più stringenti misure di controllo, vigilanza e sanzioni armoniche per tutta l'Unione Europea, a fronte anche di una semplificazione degli obblighi di comunicazione. Inoltre, la Direttiva in esame necessita di una reinterpretazione delle disposizioni al fine di attuare un'opera di adeguamento ai flussi digitali, a fronte di un aumento di traffico in rete a seguito anche della pandemia.

Attraverso i nuovi provvedimenti si mira, inoltre, ad ampliare i settori di attività, coinvolgendo un variegato numero di organizzazioni. Tale ampliamento contribuisce ad incrementare il livello di sicurezza informatica in tutto lo spazio europeo.

Rilevante è il perfezionamento del situational awareness e delle capacità di risposta attraverso misure che aumentino la collaborazione e la fiducia tra le

---

[55] Così D. MAISTO, *Infrastrutture critiche, l'UE ha il Piano d'azione*, in *Qui finanza*, 2 novembre 2022. Consultabile al sito: https://quifinanza.it/innovazione/infrastrutture-critiche-lue-ha-il-piano-dazione/673923/.

[56] Sul punto F. BORDONE, *Cybersicurezza, l'Ue accelera: norme, obiettivi e prossimi step*, in *Agenda digitale,* luglio 2022. Consultabile al sito: https://www.agendadigitale.eu/sicurezza/cybersicurezza-lue-accelera-norme-obiettivi-e-prossimi-step/.

[57] La NIS2 introduce adempimenti ulteriori per i destinatari una serie di prescrizioni, in particolar modo in tema di sicurezza della catena di approvvigionamento, reazione agli incidenti e certificazione di prodotti per la cybersecurity.

autorità, mediante la condivisione del maggior numero di informazioni e prevedendo regole in caso di crisi estese a livello europeo.

Uno dei più rilevanti aspetti della NIS 2 è l'ampliamento dei settori di mercato ad "elevata criticità" e di quelli cc.dd. "importanti". Vi rientrano pertanto, oltre ai settori compresi nella precedente Direttiva, anche la gestione dei servizi ICT, la Pubblica Amministrazione, le Acque Reflue e l'ambito Spazio.

Critici sono ritenuti anche i gestori di rifiuti, le aree di fabbricazione, di distribuzione e produzione di prodotti chimici, l'area manifatturiera, i corrieri e le organizzazioni di ricerca[58].

In riferimento a quelli che vengono chiamati enti "importanti" viene operata una distinzione da quelli qualificati, invece, come "essenziali"[59]. La differenza risiede nei diversi regimi di vigilanza e di applicazione.

A differenza della precedente Direttiva NIS, viene qui introdotto la Size-cap, cioè la regola del massimale dimensionale, quale parametro per l'identificazione delle entità regolamentate. Ad essere esclusi sono, invece, tutti quegli enti svolgenti attività di difesa e sicurezza nazionale, oltre che le banche centrali, i parlamenti e la magistratura.

Viene istituita, in via formale, la rete europea di organizzazioni di collegamento per le crisi informatiche, come strumento di supporto della gestione connessa degli incidenti di sicurezza informatica. Ciò al fine di raggiungere un elevato livello comune di cybersicurezza.

Da ultimo, occorre considerare che tale nuova Direttiva si è posta necessariamente in coordinamento con altre e specifiche norme di settore, tra tutte DORA e la CER[60].

Conclusions: Attacchi informatici ed attuale panorama sanzionatorio italiano: prospettive de iure condendo.

Alla luce di quanto emerge dal rapporto relativo al primo semestre del 2022 dell'Associazione Italiana per la Sicurezza Informatica[61], gli attacchi informatici rivolti in via diretta ad infrastrutture critiche, operatori di servizi essenziali ed aziende si attestano, nel solo mese di maggio, a quota 1380. Se si ha considerazione, in aggiunta, degli effetti indiretti che ne discendono, quali, tra tutti, il possibile riverbero dei danni economici nella catena di produzione, una quantificazione effettiva risulta impossibile. Da questi rilievi si denota la natura endemica del fenomeno in esame e diviene doveroso procedere ad una disamina del perimetro di tutela che l'ordinamento italiano ha approntato nei confronti degli attacchi cyber, al fine di vagliarne l'adeguatezza e l'esaustività.

---

[58] Sul punto e per un più esaustivo elenco, si veda A. VALENTINI, *Dentro la NIS 2, più obblighi e regole per la cybersecurity europea*, in *Cybersecurity 360*, 20 dicembre 2022. Consultabile al sito: https://www.cybersecurity360.it/outlook/dentro-la-nis-2-piu-obblighi-e-regole-per-la-cybersecurity-europea/.

[59] Quelle aziende che, secondo la definizione dell'Anssi, «forniscono un servizio essenziale la cui interruzione avrebbe un impatto significativo sull'andamento dell'economia o della società».

[60] D. DELL'ARIA, M. ROSSI, *Direttive NIS 2 e CER: così l'Europa metterà in sicurezza le sue infrastrutture critiche*, in *Cybersecurity 360*, 20 gennaio 2023. Consultabile al sito: https://www.cybersecurity360.it/cybersecurity-nazionale/direttive-nis-2-e-cer-cosi-leuropa-mettera-in-sicurezza-le-sue-infrastrutture-critiche/.

[61] *Rapporto Clusit sulla sicurezza ICT in Italia 2022.* Consultabile al sito: www.clusit.it.

Anzitutto, con la Legge 23 novembre 1993, n. 547, il Legislatore ha introdotto tre fattispecie – gli artt. 615-*ter,* 615-*quater* e 615-*quinquies* – a presidio dell'inviolabilità del domicilio, ivi inteso quello informatico; in particolare, in merito al reato di accesso abusivo a sistema informatico di cui all'art. 615-*ter* c.p.[62], la Corte di Cassazione, in un orientamento ormai risalente del 1999, ha affermato che esso non mira a tutelare esclusivamente i dati personalissimi contenuti nei sistemi informatici, anzi «si concreta nello *ius excludendi alios* […] e la tutela della legge si estende anche i profili economico-patrimoniali dei dati»[63]. Occorre puntualizzare che, benché quella del 1999 non sia una pronuncia delle Sezioni Unite, tale orientamento è rimasto costante ed inalterato, atteso che le successive pronunce appaiono conformi.

I successivi artt. 615-*quater* e 615-*quinquies* c.p. [64] , con l'obiettivo di perseguire il *possesso* di strumenti quali apparecchiature, codici ed altri mezzi idonei a consentire l'accesso, la distruzione o l'interruzione di sistemi informatici, svolgono una funzione incriminatrice imprescindibile[65]; difatti, uno dei canali privilegiati per la realizzazione di attacchi è rappresentato dal malware – un software deleterio, inserito in un computer al fine di danneggiarne un secondo collegato alla stessa rete – e si stima che ad esso si ricorra nel 38% dei casi[66]. In prima battuta troverà certamente applicazione l'art. 615-*quinquies* c.p.*,* che opera a prescindere dalla verificazione di un danno; laddove questo dovesse concretizzarsi, entreranno in gioco gli artt. 635-*bis* ss. c.p.

Successivamente, all'art. 617-*bis* c.p., è disposta la punibilità dell'installazione di apparecchiature atte a captare o ad impedire comunicazioni telefoniche o telegrafiche altrui. Nel panorama del cybercrime, anche queste condotte trovano frequente impiego, spesso in funzione prodromica e strumentale rispetto ad un disegno criminoso più ampio. È il caso della tecnica BEG (Business E-mail Compromised), attraverso la quale si realizzano frodi a danno delle aziende: dapprima si accede abusivamente ad una casella di posta elettronica, successivamente si carpiscono informazioni in merito alle richieste di pagamento, sino a dirottare transazioni o comunicare nuove coordinate bancarie.

Tra delitti contro il patrimonio si annoverano le fattispecie di cui agli artt. 635 *bis* [67] e seguenti, i quali presentano quale denominatore comune la

---

[62] M. BORGOBELLO, *Il reato di accesso abusivo a sistema informatico di cui all'art. 615-ter c.p. alla luce della giurisprudenza più recente*, in *Giur. Pen. Web*, 2021, II. Consultabile al sito: https://www.giurisprudenzapenale.com/2021/02/21/il-reato-di-accesso-abusivo-a-sistema-informatico-di-cui-allart-615-ter-c-p-alla-luce-della-giurisprudenza-piu-recente/ e, da ultimo, V. IORIO, *I reati informatici ex d.lgs. 231/2001,* in F. CORONA (a cura di), *Reati informatici e investigazioni digitali*, *op.cit*, 187-236.

[63] Cass. Pen., sez. VI, sent. 04.10.1999, n. 3067, in *CED Cassazione Penale*, 2000.

[64] Rubricati rispettivamente Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici e Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

[65] Per approfondimenti, C. PARODI, *Reati patrimoniali*, in C. PARODI, V. SELLAROLI, *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, 2020, 103-178.

[66] *Rapporto Clusit sulla sicurezza ICT in Italia*, 2022. Consultabile al sito: https://www.saccani.net/wp-content/uploads/2022/03/Rapporto-Clusit-marzo-2022_b_web.pdf.

[67] Introdotto con la Legge 23 novembre 1993, n. 547, successivamente modificato ad opera della Legge 14 marzo 2008, n. 48.

condotta di danneggiamento [68], che si sostanzia nella distruzione, deterioramento, cancellazione, alterazione e soppressione di informazioni, dati o programmi informatici. Queste disposizioni operano, ad esempio, in ipotesi particolari di attacchi attuati nell'ambito della c.d. information warfare[69], per il tramite delle CNOs (Computer Network Operations), con cui si procede alla distruzione delle informazioni presenti sui sistemi informativi avversari, alla distruzione delle reti e dei sistemi a presidio della difesa nazionale.

È opportuno, altresì, attenzionare le fattispecie in cui il danneggiamento abbia come oggetto materiale sistemi informatici o telematici di pubblica utilità – quale l'art 635-*quinquies* c.p. – oppure informazioni, dati e programmi utilizzati da Stato, enti pubblici o comunque di pubblica utilità, *ex* art. 635-*ter* c.p.

Ai fini dell'integrazione del requisito di "pubblica utilità" non si esige una formale titolarità da parte dello Stato o dell'ente pubblico, essendo sufficiente che i dati, programmi e sistemi siano soltanto impiegati o, eventualmente, nella semplice disponibilità di questi.

Le disposizioni in esame dimostrano la presa di coscienza da parte del Legislatore della particolare appetibilità, da parte dei criminali informatici, delle infrastrutture statali.

Dal 19 maggio 2022, l'Italia – unitamente ad altri Paesi con posizioni di sostegno all'Ucraina – ha subito numerosi attacchi (e tentativi), perpetrati da gruppi di dichiarata appartenenza russa, diretti verso le infrastrutture critiche di numerosi Paesi occidentali. In Italia, tali attacchi si sono tradotti, tra l'altro, nella minaccia di danneggiamenti significativi a pubbliche amministrazioni, ivi compresi i sistemi informatici del Governo, del Ministero dell'Interno e della Difesa.

Dall'analisi della normativa penale italiana in tema di attacchi informatici, può dedursi che le problematiche circa l'attribuzione dei reati non attengano al piano legislativo, bensì interpretativo.

Benché sarebbe utile un riordino della normativa attualmente in vigore, non si ritiene di dover sostenere uno stravolgimento delle fattispecie previste nel Codice penale. Resta, tuttavia, il problema dell'attribuzione, non ancora risolto a livello europeo o nazionale. In questo senso, come anticipato, si tratta di spostarsi sul piano interpretativo, poiché è rimessa al Giudice l'attribuzione concreta del reato all'autore.

È imprescindibile una considerazione in merito al legame di interdipendenza che intercorre tra il diritto alla prova e l'effettività della tutela penale. Nell'ambito dei reati informatici, infatti, pur disponendo di un corpus sanzionatorio esaustivo, questo dovrà necessariamente essere sorretto dall'impiego di conoscenze tecniche specializzate. Pertanto, occorre ampliare il

[68] Come affermato dalla Corte di Cassazione, il danneggiamento risulta integrato anche laddove l'operazione sia reversibile «È ravvisabile il reato di cui all'art. 635-*bis* c.p., in caso di cancellazione di file da un sistema informatico sia quando la cancellazione sia stata provvisoria, mediante lo spostamento dei files nel cestino, sia quando la cancellazione sia stata definitiva», cfr. Cass. Pen., sez. V, sent. 18.11.2011, n.8555, in *Guida al diritto*, 2012, 13, 76.

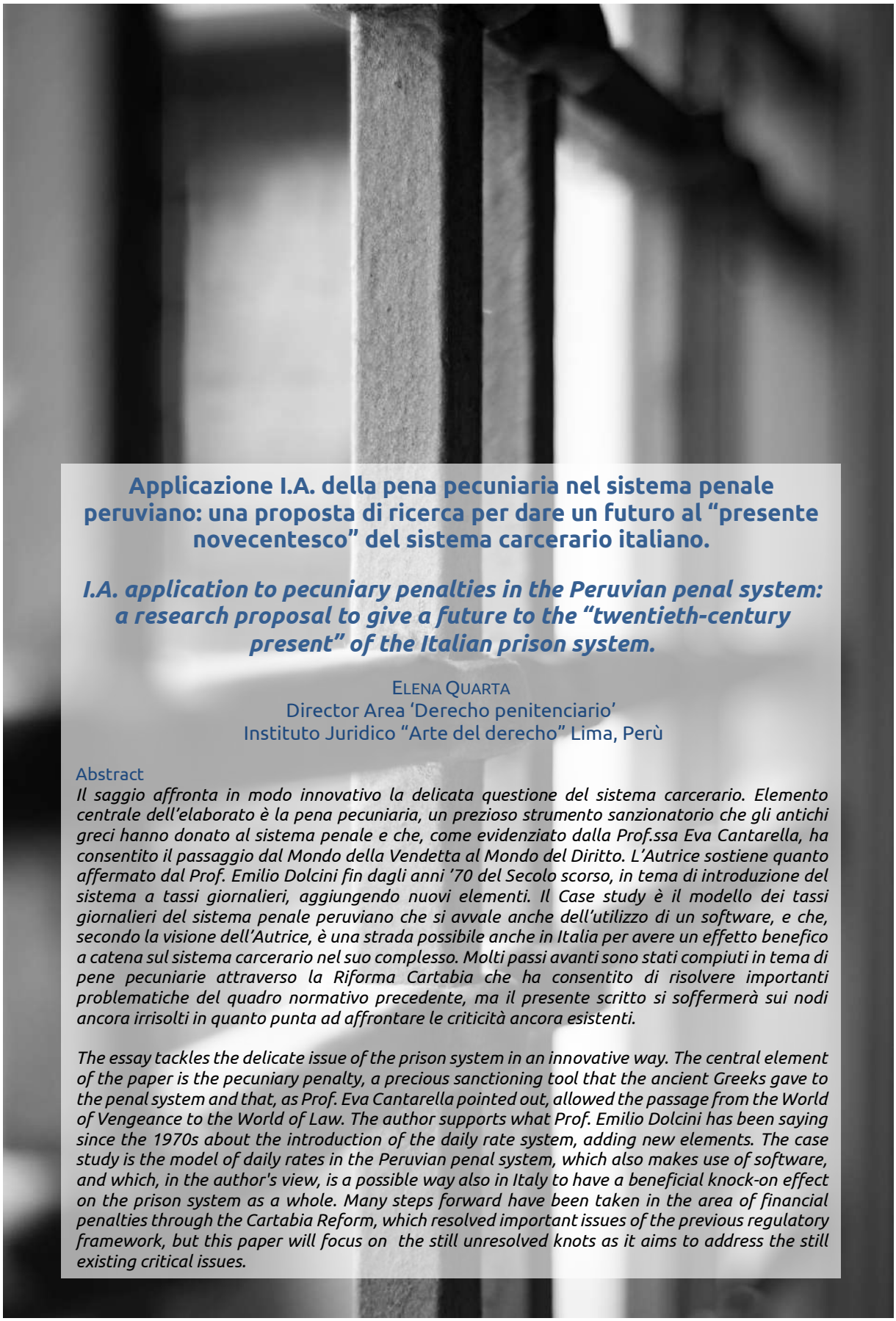
[69] Per approfondimenti, U. Gori, L. S. Germani, *Information Warfare. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana*, Milano, 2011; M. Iaselli, G. B. Caria, *Cybesecurity & Cyberwarfare*, Roma, 2023.

ruolo rivestito dai consulenti tecnici. Non sarebbe inopportuno, allora, ipotizzare la presenza di un consulente stabile presso le aule giudiziarie, che coadiuvi le parti ed il giudice.

In questo senso, potrebbe pensarsi anche ad un albo professionale apposito: ancora una volta la realtà ed il mondo propongono sfide che il diritto deve riuscire ad accogliere ed affrontare.

Quarta E, 'Applicazione I.A. della pena pecuniaria nel sistema penale peruviano: una proposta di ricerca per dare un futuro al «presente novecentesco» del sistema carcerario italiano' (2022) 2 EJPLT, 242-263.
DOI: https://doi.org/10.57230/EJPLT222EQ

EJPLT
ISSN 2704-8012



Applicazione I.A. della pena pecuniaria nel sistema penale peruviano: una proposta di ricerca per dare un futuro al "presente novecentesco" del sistema carcerario italiano.

I.A. application to pecuniary penalties in the Peruvian penal system: a research proposal to give a future to the "twentieth-century present" of the Italian prison system.

ELENA QUARTA
Director Area 'Derecho penitenciario'
Instituto Juridico "Arte del derecho" Lima, Perù

Abstract

Il saggio affronta in modo innovativo la delicata questione del sistema carcerario. Elemento centrale dell'elaborato è la pena pecuniaria, un prezioso strumento sanzionatorio che gli antichi greci hanno donato al sistema penale e che, come evidenziato dalla Prof.ssa Eva Cantarella, ha consentito il passaggio dal Mondo della Vendetta al Mondo del Diritto. L'Autrice sostiene quanto affermato dal Prof. Emilio Dolcini fin dagli anni '70 del Secolo scorso, in tema di introduzione del sistema a tassi giornalieri, aggiungendo nuovi elementi. Il Case study è il modello dei tassi giornalieri del sistema penale peruviano che si avvale anche dell'utilizzo di un software, e che, secondo la visione dell'Autrice, è una strada possibile anche in Italia per avere un effetto benefico a catena sul sistema carcerario nel suo complesso. Molti passi avanti sono stati compiuti in tema di pene pecuniarie attraverso la Riforma Cartabia che ha consentito di risolvere importanti problematiche del quadro normativo precedente, ma il presente scritto si soffermerà sui nodi ancora irrisolti in quanto punta ad affrontare le criticità ancora esistenti.

The essay tackles the delicate issue of the prison system in an innovative way. The central element of the paper is the pecuniary penalty, a precious sanctioning tool that the ancient Greeks gave to the penal system and that, as Prof. Eva Cantarella pointed out, allowed the passage from the World of Vengeance to the World of Law. The author supports what Prof. Emilio Dolcini has been saying since the 1970s about the introduction of the daily rate system, adding new elements. The case study is the model of daily rates in the Peruvian penal system, which also makes use of software, and which, in the author's view, is a possible way also in Italy to have a beneficial knock-on effect on the prison system as a whole. Many steps forward have been taken in the area of financial penalties through the Cartabia Reform, which resolved important issues of the previous regulatory framework, but this paper will focus on the still unresolved knots as it aims to address the still existing critical issues.

© The author(s) 2022, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: artificial intelligence; pecuniary penalty; daily rate system; peruvian criminal system.

Summary: 1. Introduzione: la pena pecuniaria nel mondo omerico. – 2. La scelta carcero-centrica del Legislatore del 1930: un passato ancora attuale. – 3. L'errata percezione della Pena pecuniaria come "ancella" della pena detentiva. – 4. Sostenibilità in Italia del Sistema peruviano a tassi giornalieri delle pene pecuniarie e relativo software. – 5. Pregi e Criticità della Riforma Cartabia e proposta di ritorno al Codice Zanardelli in tema di conversione. – 6. Proposta di ricerca: Valorizzazione della pena pecuniaria come volano per il superamento delle problematiche del sistema carcerario. – 7. Modello ipotizzato per rendere moderno il sistema sanzionatorio italiano. – 8. Conclusioni: la pena pecuniaria contribuisce a costituire la pena principale del reato.

Introduzione: la pena pecuniaria nel mondo omerico.

Storicamente, i termini "ποινή" e "*poena*" nel loro originario significato etimologico indicano la sola sanzione pecuniaria. La voce utilizzata dai Romani per designare la pena è appunto "poena", vocabolo di cui è dimostrata la parentela etimologica con il verbo greco, che significa pagare, e con il termine greco ποινή (CONTI 1910). La pena pecuniaria, infatti, era conosciuta e ampiamente applicata accanto alla pena di morte e alle pene corporali nel sistema penale dei popoli più antichi. Nell'antichità la pena pecuniaria consentì il superamento della legge del taglione, soppiantando il sistema della vendetta privata, personale o familiare: si pensi al diritto germanico ove il Wergeld (guidrigildo) rappresentava la somma che veniva corrisposta ai famigliari della vittima in caso di omicidio in cambio della rinuncia di questi ultimi alla «vendetta di sangue» o faida (Manzini 1942; Del Giudice 1905)[1]. In tal senso, lentamente nel mondo omerico si era venuta affermando una prassi sociale che, in misura dapprima limitata e via via sempre più estesa, aveva numericamente ridotto le vendette private2. Questa prassi era l'offerta di una poine, vale a dire di un riscatto, in un primo momento in natura, quindi in denaro, che l'offensore faceva all'offeso, e che costui poteva liberamente accettare o respingere, Ricevendo la poine, scrive Omero, «si placa il cuore superbo e l'animo dell'altro/ che ha ricevuto il riscatto». L'offeso che ha ricevuto la riparazione e può recedere dalla sua "ira" non è solo un sentimento; è anche espressione della sua nobiltà, del suo coraggio e della sua forza (…) Stanca dello stato continuo di belligeranza inevitabilmente provocato da una catena incontrollata di vendette, la coscienza sociale non solo aveva preso a considerare positiva la scelta di chi accettava il riscatto, ma aveva stabilito che, una volta fatta, essa doveva essere definitiva: in altri termini la pone era alternativa alla vendetta. Il

[1] L. Goisis, *Le pene pecuniarie. Storia, comparazione, prospettive*, in Diritto Penale Contemporaneo, 22 novembre 2017, pag. 2-3 consultabile al link https://www.penalecontemporaneo.it/upload/4199-goisis2017a.pdf.
[2] Particolarmente significativa è la strage dei Proci per mano di Ulisse, scena dipinta da Omero nel canto XXII dell'Odissea.

valore fondamentale di questa regola era consacrato dall'introduzione di un organo giurisdizionale, rappresentato dal consiglio dei gerontes, chiamato a risolvere le eventuali controversie in materia. A chiarire come venisse esercitata questa giurisdizione interviene la descrizione del processo scolpito da Efesto sullo scudo di Achille e descritto nel XVIII canto dell'Iliade (..) Un uomo aveva ucciso un altro uomo. Gli appartenenti alla famiglia del morto volevano esercitare la vendetta su un appartenente al gruppo dell'omicida. Ma costui affermando di aver già pagato una pone, aveva fatto ricorso ai gerontes. Dinanzi al popolo raccolto nella piazza, ciascuno dei due contendenti aveva deposto un talento d'oro. Al termine della lite i due talenti sarebbero stati assegnati a colui che aveva detto la verità. I gerontes, dunque, dovevano accertare se il riscatto era stato pagato o meno. Ma le conseguenze non erano solo pecuniarie (l'assegnazione dei due talenti). Il loro giudizio di accertamento dei fatti, in realtà, conteneva implicitamente un comando: se la poine era stata pagata, il tentativo di vendetta- da parte di chi aveva affermato di averla ricevuta- dove va cessare. Se la poine non era stata pagata, invece, colui che non aveva ricevuto o non aveva voluto accettare la compensazione aveva il diritto di condurre a termine la rappresaglia[3].

2. La scelta carcero-centrica del Legislatore del 1930: un passato ancora attuale.

La dottrina internazionale di fine '800 andava affermando l'idea di abolire le pene detentive brevi nei vari congressi nazionali ed internazionali Nella discussione di fine ottocento si sottolineava come queste ultime pene non riuscissero nei loro compiti general e specialpreventivi e come esse avessero all'opposto effetti criminogeni, favorendo la recidiva. Per queste ragioni si propugnava l'abolizione delle pene detentive brevi e la loro sostituzione con altri strumenti penali, tra i quali in primis la pena pecuniaria (Goisis 2008) I legislatori europei, in risposta alle proposte della dottrina penalistica, iniziarono ad adottare alcuni provvedimenti volti a valorizzare il ruolo della pena pecuniaria nell'ambito del sistema sanzionatorio.Il Legislatore Rocco decise di andare in controtendenza. Infatti, quanto all'Italia, il Codice Rocco, anziché valorizzare alcune previsioni innovative del Codice Zanardelli, come appunto il lavoro libero a favore della collettività quale sanzione di conversione della pena pecuniaria non pagata, operò nel senso di non accogliere le ampie possibilità politico-criminali offerte dalla pena pecuniaria, inclusa la sua idoneità a divenire strumento efficace contro le pene detentive brevi, rifiutando, in particolare, l'idea di adeguare la pena pecuniaria, intrinsecamente diseguale, alle condizioni economiche del reo (Padovani 1981)[4]. Era il 1974, quando Giorgio Marinucci riportava – nel saggio Politica criminale e riforma del diritto penale[5] – l'«opinione unanime» della scienza penalistica internazionale, per la quale «il compito futuro della politica criminale non risiederà nel miglioramento della pena detentiva, bensì nella sua progressiva eliminazione:

[3] E. CANTARELLA, *I supplizi capitali in Grecia e a Roma* Rizzoli, Milano, 1991 pag. 63 e ss.
[4] L. GOISIS, *Le pene pecuniarie. Storia, comparazione, prospettive*, in Diritto Penale Contemporaneo, 22 novembre 2017, pag. 4-5.
[5] G. MARINUCCI, *Politica criminale e riforma del diritto penale*, Jus, 1974, Vita e pensiero, pag. 486 e ss.

ogni privazione della libertà personale in qualunque tipo di stabilimento, anche pensato con la più ampia fantasia rinnovatrice, provoca danni psicologici e sociali così certi da rendere difficile qualunque obiettivo di risocializzazione»[6].
Anche sul terreno della pena pecuniaria si manifestò quella «chiusura autoritaria-culturale verso una politica criminale dai tratti più liberali e più umani» (Musco 1984, 9): essa venne comminata raramente come pena unica e solo per reati minori, mentre venne prevista come pena cumulativa in aggiunta alla pena detentiva per rendere quest'ultima più deterrente. Come notato dalla dottrina d'oltralpe, il legislatore Rocco, non utilizzando le potenzialità politico-criminali della pena pecuniaria, «ha fatto invecchiare di mezzo secolo il codice penale in uno dei suoi punti decisivi» (Bosch[7] 1978, 468) [8] Già nel lontano 1977 lo studioso Franco Bricola sottolineava che: «Un'effettività di tipo "rinnegante" è di per sé innegabilmente connessa ad un tipo di normativa qual è quella penitenziaria: è, infatti, uno dei settori più esposti alle varie pratiche nelle quali, nello Stato di diritto, si realizza l'illegalità ufficiale attraverso la non applicazione e la manipolazione amministrativa delle norme. Nel caso della nuova legge, tuttavia, sintomi di un'effettività "rinnegante" erano già latenti nel tessuto normativo e nelle contingenze storico-politiche che caratterizzavano il momento della sua entrata in vigore. E infatti: varare una riforma dell'ordinamento penitenziario senza avere previamente risolto gli ardui temi della decriminalizzazione di vasti settori e della configurazione di sanzioni alternative alla pena detentiva e alla carcerazione preventiva, e cioè, senza avere preliminarmente riformato i codici penali (sostanziale e processuale), significava porre le premesse di un sovraffollamento delle carceri e, quindi, dell'esplosione di quelle contraddizioni che si sono poi clamorosamente delineate» [9] . Gli effetti della scelta carcero-centrica si riflettono sulla contemporaneità, in quanto il Codice Rocco è ancora oggi in vigore. E, del resto, la sopravvivenza del nostro codice Rocco si rivela un fenomeno sostanzialmente isolato nel panorama europeo, in cui nel dopoguerra sono stati rinnovati o sostituiti pressoché tutti i codici penali dell'Europa sia occidentale che orientale, seppure in tempi più o meno prossimi ai mutamenti costituzionali e in modo variamente condizionato dalle nuove costituzioni del dopoguerra e del dopo Muro di Berlino[10].

3. L'errata percezione della Pena pecuniaria come "ancella" della pena detentiva.

[6] C. PERINI, *Prospettive attuali dell'alternativa al carcere tra emergenza e rieducazione*, Diritto penale contemporaneo n. 4/ 2017 https://dpc-rivistatrimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_4_17_Perini.pdf.
[7] J. BOSCH, *Die Geldstrafe in Italien*, in H. H. JESCHECK, G. GREBING, *Die Geldstrafe in deutschen und ausländischen Recht*, BadenBaden, 1978, 46.
[8] L. GOISIS, *Le pene pecuniarie. Storia, comparazione, prospettive*, in Diritto Penale Contemporaneo, 22 novembre 2017, pag. 4-5.
[9] F. BRICOLA, *Introduzione* a Aa.Vv., *Il carcere "riformato"*, Bologna, 1977 costituzionalismo.it Fascicolo2 |2015 IDIRITTIDEIDETENUTI, consultabile al seguente indirizzo url https://www.costituzionalismo.it/costituzionalismo/download/Costituzionalismo_201502_512.pdf.
[10] F. PALAZZO, *Codice penale 1930: un passato (ancora) senza futuro*, in *Diritto penale contemporaneo*, 15 settembre 2011, pp. 1-5 consultabile al seguente indirizzo url https://archiviodpc.dirittopenaleuomo.org/d/851-codice-penale.1930-un-passato-ancora-senza-futuro.

La Corte costituzionale italiana ha considerato centrale nel nostro sistema la funzione rieducativa della pena; al quale principio potrebbe darsi attuazione almeno nella forma di un reinserimento sociale, o, se si vuole, di un ritorno alla legalità. Occorre chiedersi tuttavia se già l'idea di re-inserimento, non sia un punto di partenza equivoco, se non compresa nel migliore dei suoi significati. Perché reinserire può anche significare il tener "fuori" la persona per poi reimmetterla nel contesto sociale. In realtà molti di coloro che abbiano violato la legge penale potrebbero aver commesso reati del tutto occasionali, senza con ciò dover concludere che si tratti di persone, per così dire, "decontestualizzate". No, il condannato va considerato quale parte del contesto sociale e si deve far di tutto perché non ne esca; soprattutto che non venga 'cacciato' da esso a causa di un sistema carcerario non in sintonia con i tempi, visto che nessuno può ignorare come il carcere risulti, allo stato, a rischio di un incisivo effetto di 'desocializzazione', in mancanza di strutture e programmi di trattamento davvero all'altezza [11]. Negli ultimi anni, infatti, sempre più sta emergendo la necessità di ripensare all'intero sistema penitenziario [12] ,rinforzando sempre di più le misure di esecuzione extra muraria, focalizzate su programmi rieducativi, rispetto alla classica misura detentiva, che dovrebbe essere riservata a situazioni estreme, ove sono estremamente forti i bisogni di prevenzione sociale (condannati per reati associativi di stampo mafioso e terroristico o per gravi delitti di sangue) (S. Pazienza)[13]. Affinché la pena carceraria risulti pertanto davvero come *extrema ratio* e non integri al contrario un astratto ma vuoto slogan, va ripensato l'intero armamentario di carattere sanzionatorio penale, cercando di individuare pene del tutto diverse dal carcere, che quindi possano integrare reali alternative a quest'ultimo. In questo ambito viene in primo luogo in considerazione la pena pecuniaria, che tuttavia dal codice penale Rocco in poi e forse anche prima, è sempre stata considerata un'ancella della pena detentiva, soprattutto per il sistema di commisurazione della stessa[14]. Per quanto concerne la percezione che il condannato ha della pena pecuniaria: Nel corso della mia intervista all'Avv Antonella Crippa la stessa ha dichiarato: «In genere nella prassi giudiziaria l'imputato ed il difensore pongono maggiore attenzione alla pena detentiva rispetto alla pena pecuniaria. Innanzitutto per una ragione evidente, la pena detentiva comporta un rischio di restrizione della libertà personale (carcerazione). (…) Un segnale che la pena pecuniaria richiama un livello di "allerta" nel condannato inferiore, lo potremmo verificare con un sondaggio tra i detenuti, chiedendo loro se hanno contezza nella loro condanna dell'ammontare della multa a loro comminata in sentenza. Molto probabilmente la maggior parte non saprebbe indicarne la misura. E quando si

[11] A. FIORELLA, *La codificazione penale in Italia e le sue prospettive di riforma** ARCHIVIO PENALE 2019, n. 2 consultabile al seguente indirizzo url https://archiviopenale.it/File/DownloadArticolo?codice=8c291557-ad4c-489e-97c4-9128b3d36c9f&idarticolo=19644.

[12] L. MANCONI, S. ANASTASIA, V. CALDERONE F. RESTA, *Abolire il carcere: Una ragionevole proposta per la sicurezza dei cittadini*, Chiarelettere, 2022.

[13] S. PAZIENZA, E. QUARTA, *Sovraffollamento, il ruolo di organo di controllo internazionale della CEDU e costi economici della detenzione*, in E. QUARTA, *Il procedimento di conversione delle pene pecuniarie inevase*, vol. II, Universitalia, 2022.

[14] A. MANNA, *È configurabile un sistema penale non carcero-centrico?,* Sistema penale, 10 marzo 2021, consultabile al seguente indirizzo url https://www.sistemapenale.it/it/articolo/adelmo-manna-e-configurabile-un-sistema-penale-non-carcero-centrico.

pensa al fine pena, sicuramente non è contemplato l'aver sanato il debito di giustizia tradotto in termini pecuniari. E altresì quando si discute dell'esecuzione penale, si discute in termini di giorni/mesi e anni di detenzione. Nel momento in cui si aprono le porte del Carcere chiaramente la percezione è quella di aver concluso l'esecuzione penale in senso stretto»[15]. Eppure, è solo un'errata percezione in quanto come anche emerso nel corso dell'intervista esiste un interesse all'adempimento spontaneo anche da parte del condannato ossia l'interesse alla riabilitazione. Spesso il condannato non è consapevole, infatti, che anche la pena pecuniaria costituisce, allo stesso titolo della pena detentiva, la pena principale del reato.
In forza dell'art. 178 c.p. «la riabilitazione estingue le pene accessorie e ogni altro effetto penale della condanna, salvo che la legge non disponga altrimenti». L'art. 179 c.p. come modificato dall'art. 3 della legge 11 giugno 2004 n. 145, dispone che il beneficio può essere concesso decorsi almeno 3 anni (8 per il recidivo) dal giorno in cui la pena principale sia stata eseguita o si sia comunque estinta 16 . L'importanza della pena pecuniaria è stato anche evidenziato dalla Sezione Prima Penale della Corte di Cassazione: «*Nell'ipotesi di applicazione di pena detentiva congiunta a quella pecuniaria, ai fini del calcolo del termine previsto per la riabilitazione occorre avere riguardo non solo alla data di espiazione della pena detentiva , ma anche a quella di pagamento della pena pecuniaria, giacchè anche quest'ultima contribuisce , allo stesso titolo, a costituire la pena principale del reato*» (Cass. Pen., sez. I, 15 ottobre 2004, n. 47715 C.E.D. Cass. n. 230408; in senso analogo in dottrina v. Manzini, Trattato III 767 secondo cui in caso di pena detentiva e di pena pecuniaria cumulativamente inflitte, il termine decorre dal giorno in cui tutte furono estinte)[17].

4. Sostenibilità in Italia del Sistema peruviano a tassi giornalieri delle pene pecuniarie e relativo software.

In un recente scritto il Prof. Emilio Dolcini ha evidenziato che: «La pena pecuniaria comminata *ex lege* rimarrà fedele al tradizionale modello della somma complessiva, solo apparentemente" orientato alla capacità economica del condannato», come in altri ordinamenti, in primis nell'ordinamento tedesco, disposizioni quali quella dell'art. 133 bis c.p. sono da sempre lettera morta, e producono l'unico effetto di tacitare la cattiva coscienza del legislatore. Ciò, tra l'altro, rende altamente problematico dar vita ad una razionale disciplina della conversione, che presuppone la visibilità del ruolo esercitato dalle condizioni economiche del condannato nella commisurazione della pena pecuniaria, così da scongiurare qualsiasi incidenza delle condizioni economiche sull'ammontare

[15] A.CRIPPA , E. QUARTA, *La visione teorica del sistema di riscossione delle pene pecuniarie al vaglio della critica kantiana della ragion pura. Intervista ad una penalista per coniugare teoria e prassi* in E. QUARTA, *Il procedimento di conversione delle pene pecuniarie inevase*, vol. II, Universitalia, 2022, pag. 92 e ss.
[16] G. PRELATI, *Manuale del Tribunale e dell'Ufficio di Sorveglianza*, Milano, 2005, pag. 253,
[17] R. GARGIULO, M. VESSICCHELLI, *Art. 179*, in G. LATTANZI, E. LUPO, *Codice penale. Rassegna di giurisprudenza e di dottrina*, Milano, 2010, pag. 681.

della pena da conversione"[18]. La Riforma Cartabia accanto alle condizioni economiche e reddituali, ha cercato di valorizzare le condizioni patrimoniali, ex art 133 BIS[19].
Secondo mio personale parere, sebbene la valutazione del giudice al complesso dell'intera posizione patrimoniale dell'imputato (ad es., beni mobili e immobili) appaia di pregevole utilità, affinché il sistema delle pene pecuniarie sia efficace è necessaria una adeguatezza della pena pecuniaria al Reddito del condannato. Talvolta, infatti, i beni mobili ed immobili possono essere gravati da pesi o vincoli.
Nella Relazione illustrativa alla riforma Cartabia si evidenzia che: «Altresì da valutare, per esigenze di giustizia sostanziale, non del tutto soddisfatte dal criterio di commisurazione di cui all'art. 133 bis c.p., sarebbe poi l'adozione del sistema dei tassi giornalieri (o quote giornaliere), previsto nel nostro ordinamento solo per la responsabilità da reato delle persone giuridiche, ai sensi del d.lgs. n. 231/2001, e che larga diffusione ha all'estero (ad esempio, in Germania e in Spagna) Tali interventi andrebbero ben oltre i limiti della legge delega e non possono pertanto essere realizzati in questa sede, alla quale è deputato un primo ma fondamentale passo nel processo di rivitalizzazione della pena pecuniaria, nella direzione di un recupero di effettività …»[20]. «Nel parere alla Riforma Cartabia reso dalla quinta Commissione dell'associazione *nazionale magistrati si afferma che nei confronti della soluzione consistente nel sistema delle quote giornaliere," non più prevista, si deve esprimere parere favorevole. Tuttavia, devono essere previsti criteri di agevole e snella applicazione per stabilire le condizioni economiche del condannato ai fini della commisurazione; in caso contrario si assisterebbe ad un appesantimento del processo, in contrasto con gli obiettivi di riforma. Il sistema delle quote giornaliere recherebbe con sé numerosi vantaggi, non ultimo l'equità del computo della pena detentiva nel caso di conversione, essendo separato concettualmente il quantum legato alla gravità del reato (determinazione del numero di quote giornaliere), dal quantum correlato alle condizioni economiche del reo (determinazione dell'ammontare della quota) ...*»[21].
Ad avviso della scrivente si potrebbe prendere come modello l'art. 41 del codice penale peruviano. La formulazione dell'articolo 41 del Codice Penale peruviano è molto chiara: L'importo della multa giornaliera è equivalente al

[18] E. DOLCINI, *Sanzioni sostitutive: la svolta impressa dalla riforma Cartabia* Sistema penale, 2 settembre 2021, consultabile al seguente indirizzo url https://www.sistemapenale.it/it/opinioni/dolcini-sanzioni-sostitutive-la-svolta-impressa-dalla-riforma-cartabia.
[19] Art. 133-bis c.p. "Condizioni economiche e patrimoniali del reo; valutazione agli effetti della pena pecuniaria. Nella determinazione dell'ammontare della multa o dell'ammenda il giudice deve tener conto, oltre che dei criteri indicati dall'articolo precedente, anche delle condizioni economiche e patrimoniali del reo. Omissis cfr. art. 1, co. 1, lett. d) dello schema di decreto REDAZIONE SISTEMA PENALE, *Riforma della giustizia penale: lo schema del decreto legislativo approvato dal Consiglio dei Ministri e la relazione illustrativa*, 10 agosto 2022 consultabile al seguente indirizzo url https://www.sistemapenale.it/it/documenti/riforma-processo-penale-testo-schema-decreto-e-relazione-illustrati
[20] REDAZIONE SISTEMA PENALE , *Riforma della giustizia penale: lo schema del decreto legislativo approvato dal Consiglio dei Ministri e la relazione illustrativa*, 10 agosto 2022 consultabile al seguente indirizzo url https://www.sistemapenale.it/it/documenti/riforma-processo-penale-testo-schema-decreto-e-relazione-illustrativa.
[21] GIUDICE MAURO LAVRA (a cura di), *Art. 9 Disposizioni in materia pecuniaria*, in 5 COMMISSIONE ANM (a cura di) *Parere della Commissione sulla riforma Cartabia Illustrata al Cdc nella seduta del 11-12 settembre 2021*, https://www.associazionemagistrati.it/allegati/parere-commissione-penale-su-riforma-cartabia.pdf.

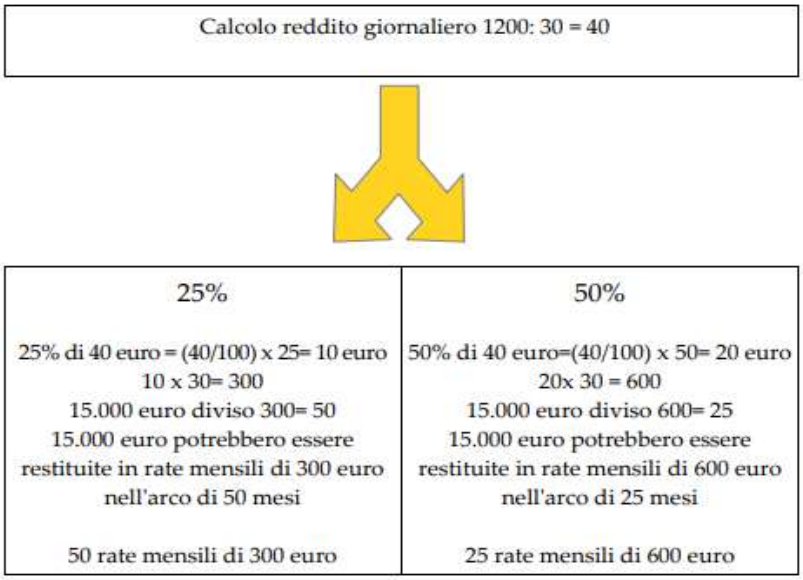
reddito medio giornaliero del condannato ed è determinato secondo il suo patrimonio, il reddito, la remunerazione, il livello di spesa e altri segni esterni di ricchezza[22].
Anche la formulazione dell'articolo 42 è ben definita: «La pena della multa va da un minimo di dieci giorni di multa a un massimo di trecentosessantacinque giorni di multa, salvo disposizioni contrarie della legge»[23]. E come ogni regola ha la sua eccezione, gli atti punibili più gravi o le circostanze aggravanti specifiche estendono il quantum, con una pena che va da 365 a 730 giorni[24].
La normativa più importante è senza *dubbio l'articolo 43 del Codice penale Peruviano,* secondo il quale: L'importo della multa giornaliera non può essere inferiore al venticinque per cento né superiore al cinquanta per cento del reddito giornaliero del condannato quando vive esclusivamente del suo lavoro[25]. Per il Prof. López Barja de Quiroga[26], Presidente della Quinta Sezione della Corte Suprema in Spagna, in uno dei suoi scritti sostiene che il sistema della multa giornaliera permette una migliore individualizzazione della multa tenendo conto del reato e della colpevolezza del colpevole così come della situazione economica del colpevole. Ha quindi sollecitato l'applicazione del modello della multa giornaliera per la legislazione straniera[27]. La sottoscritta è assolutamente d'accordo con questa impostazione.
Inoltre, è stato elaborato un software dal Fiscal Provincial de la 2da. Fiscalía Provincial Penal Corporativa de Piura Dr. Carlos Gutiérrez Gutiérrez un software[28] che è presente sul sito del Ministerio Público Fiscalía de la Nación. Il software consente di calcolare la pena pecuniaria da applicare inserendo i dati del reddito mensile del condannato, e la percentuale che appunto oscilla tra il 25 ed il 50% da applicare al reddito giornaliero ed il numero di giorni di multa.
Inserendo i suddetti dati appare nella schermata, il reddito giornaliero ed il relativo calcolo della percentuale per comprendere l'importo per ogni giorno e l'importo totale che il software ottiene moltiplicando per i giorni di multa.
Per esempio. A è stato condannato per un reato contro la pubblica amministrazione a [...] anni e 180 giorni di multa, se il reddito mensile di A è S/3000 soles, il suo reddito giornaliero (1/30) è S/100 soles; se oltre a quanto sopra la percentuale % della quota giornaliera è stata fissata al 25%, il 25% di S / 100 soles (il tuo reddito giornaliero) sono S / 25; Questo importo è quello che deve essere infine moltiplicato per il numero di giorni di multa inflitta (180 giorni-multa). Pertanto, l'importo da infliggere è (S/25 X 180) S/ 4500 a titolo di ammenda[29].

---

[22] Todos los artículos de esta contribución están tomados de https://lpderecho.pe/codigo-penal-peruano-actualizado/
[23] Todos los artículos de esta contribución están tomados de https://lpderecho.pe/codigo-penal-peruano-actualizado/
[24] DIEGO J. VALDERRAMA MACERA, *¿Cómo? calcular la pena multa en el derecho penal? Bien explicado*, LPDERECHO, 18/08/2021, disponible en la siguiente url: https://lpderecho.pe/calcular-pena-multa-derecho-penal/
[25] Todos los artículos de esta contribución están tomados de https://lpderecho.pe/codigo-penal-peruano-actualizado/
[26] J. LÓPEZ BARJA DE QUIROGA, *Derecho Penal, Parte General* Tomo III, Lima, 2004, p.30.
[27] D.J. VALDERRAMA MACERA, *¿Cómo? calcular la pena multa en el derecho penal? Bien explicado,* LPDERECHO, 18 agosto 2021, disponible en la siguiente url: https://lpderecho.pe/calcular-pena-multa-derecho-penal/
[28] Software consultabile al seguente indirizzo url https://www.mpfn.gob.pe/escuela/simulador/simulador_procesa.php?cod_supuesto=4
[29] D.J. VALDERRAMA MACERA, *¿Cómo? calcular la pena multa en el derecho penal? Bien explicado*, LPDERECHO, 18/08/2021, disponible en la siguiente url: https://lpderecho.pe/calcular-pena-multa-derecho-penal/

Personalmente considero ottimale questo sistema sviluppato in Perù. È ottimale perché non solo è proporzionale alle condizioni economiche del condannato, ma gli permette di avere una parte del reddito giornaliero per le sue necessità di sussistenza, che va da un minimo del 50% a un massimo del 75%, a seconda della percentuale applicata ai sensi dell'articolo 43 del codice penale peruviano.
La Riforma Cartabia ha altresì aumentato le rate ex art. 133 ter"[30] *da 6 a 60* (ante riforma da 3 a 30). Certamente l'aumento delle rate appare un primo passo avanti, ma talvolta può apparire strumento insufficiente affinché il condannato possa adempiere in quanto la pena pecuniaria non è calibrata al Reddito dello stesso.
A livello esemplificativo si consideri l'ipotesi di condanna prevista dall'articolo 518 *duodecies*, introdotto dalla legge 9 marzo 2022 n. 22 rubricato Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici
La legge 9 marzo 2022, n. 22 (in G.U. 22/03/2022, n.68157)31 ha disposto con l'art. 1, comma 1, lettera b) l'introduzione dell'art. 518-*duodecies*.
Art. 518-duodecies, rubricato Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici dispone che: *«Chiunque distrugge, disperde, deteriora o rende in tutto o in parte inservibili o non fruibili beni culturali o paesaggistici propri o altrui è punito con la reclusione da due a cinque anni e con la multa da euro 2.500 a euro 15.000. Chiunque, fuori dei casi di cui al primo comma, deturpa o imbratta beni culturali o paesaggistici propri o altrui, ovvero destina beni culturali a un uso incompatibile con il loro carattere storico o artistico ovvero pregiudizievole per la loro conservazione o integrità, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 1.500 a euro 10.000. La sospensione condizionale della pena è subordinata al ripristino dello stato dei luoghi o all'eliminazione delle conseguenze dannose o pericolose del reato ovvero alla prestazione di attività non retribuita a favore della collettività per un tempo determinato, comunque non superiore alla durata della pena sospesa, secondo le modalità indicate dal giudice nella sentenza di condanna*».
Nel caso di specie si consideri un soggetto condannato a 5 anni di reclusione e multa di euro 15.000. Consideriamo che il soggetto una volta terminata la pena detentiva, viva mantenendo la famiglia con uno stipendio di importo pari a 1200 euro. Anche volendo disporre della rata di 15 euro al mese, facendo un calcolo dovrebbe disporre di 1000 rate numero che è chiaramente escluso dalla normativa (15.000/15 =1000).

[30] Art. 133 ter c.p.p. "Pagamento rateale della multa e dell'ammenda. Il giudice, con la sentenza di condanna o con il decreto penale, può disporre, in relazione alle condizioni economiche e patrimoniali del condannato, che la multa o l'ammenda venga pagata in rate mensili (da 3 a 30) da 6 a 60. Ciascuna rata non può essere inferiore a euro 15. Non sono dovuti interessi per la rateizzazione. In ogni momento il condannato può estinguere la pena mediante un unico pagamento". REDAZIONE SISTEMA PENALE, *Riforma della giustizia penale: lo schema del decreto legislativo approvato dal Consiglio dei Ministri e la relazione illustrativa*, 10 agosto 2022 consultabile al seguente indirizzo url https://www.sistemapenale.it/it/documenti/riforma-processo-penale-testo-schema-decreto-e-relazione-illustrati
[31] Normattiva.it



Invece applicando il disposto suggerito si potrebbe effettuare il seguente calcolo:

Lo studioso A. Pagliaro ha evidenziato, poco più di un decennio fa, che purtroppo in Italia, lo stato dell'amministrazione tributaria non è altrettanto progredito come nei paesi che hanno adottato il sistema dei tassi giornalieri. Le gravissime difficoltà che si incontrerebbero nell'accertare le condizioni economiche dl condannato a pena pecuniaria farebbero sorgere, ove si seguisse il criterio dei tassi giornalieri, la figura dell'"evasore penale" accanto a quella dell'evasore fiscale[32].

Perché non ipotizzare l'applicazione della IA al fine di rendere le pene pecuniarie applicate al condannato proporzionali calibrate rispetto alla sua capacità economica? Nel bilanciamento di valori rendere una pena pecuniaria proporzionale alle capacità economiche del condannato dovrebbe essere l'interesse prevalente.

Anche la questione sulla inadeguatezza dell'Amministrazione Tributaria può essere rimessa in discussione dal fatto che, a riprova dell'Impegno della Magistratura Italiana pur in assenza di norme a sostegno, proprio nell'atto di promovimento della questione di illegittimità costituzionale dell'art. 53, secondo comma, della legge 24 novembre 1981 n. 689 (Modifiche al sistema penale), il Giudice delle Indagini Preliminari del Tribunale di Taranto aveva osservato che «la pena pecuniaria comminata sarebbe stata sostanzialmente pari ai redditi dichiarati nell'anno 2020 e, dunque, del tutto sproporzionata rispetto alle condizioni economiche dell'interessato» proprio, «alla luce della documentazione dell'Agenzia delle entrate versata in atti e attestante la situazione reddituale dell'imputato»[33] (Corte Cost. 1 febbraio 2022, n. 28). In

[32] A. PAGLIARO, *Il diritto penale tra norma e società. Scritti 1056-2008*, Giuffrè, Milano, 2009, pag. 992.

[33] Corte Costituzionale n. 28 del 2022 consultabile al seguente indirizzo url https://www.cortecostituzionale.it/. Si conceda il rinvio a E. QUARTA, *La Corte Costituzionale ridisegna l'architettura della pena pecuniaria sostitutiva della pena detentiva, sanando le fratture tra il volto iniquo della stessa e la società civile. (Nota a Corte Cost. Sent. n. 28/2022) Parte I e II* , 4-5 aprile 2022, Rivista di Magistratura

riferimento a ciò, volendo introdurre il sistema a tassi in Italia si potrebbe elaborare anche un software, come è stato elaborato in Perù.
Come evidenziato in dottrina (A. Uricchio) non va dimenticato l'utilizzo delle intelligenze artificiali nelle procedure di accertamento tributario, già previsto e in parte realizzato in altri paesi (Vedi Brasile) è oggetto di studio da parte della nostra Agenzia delle Entrate che peraltro già ad opera strumenti di raccolta e di interscambio delle informazioni anche di big data (cosiddetti anagrafe dei rapporti e sistema di interscambio dati-Sid) , o anche dalle agenzie doganali in sede di controllo merci, dichiarazione e destinazioni doganali. Particolarmente sofisticato e poi il controllo di saldi e movimentazione dei conti correnti oltre che di altre tipologie di rapporti, da parte degli intermediari finanziari e più di recente di fatturazioni ormai telematiche. Le caratteristiche tecnologiche del sistema consentiranno la progressiva estensione ad altre tipologie di flussi che si caratterizzano, prevalentemente, per i grandi volumi di dati scambiati. Fondamentale in questo contesto il ruolo della Sogei incaricata di gestire organizzare sistemi informativi per conto del Ministero dell'Economia e delle Finanze e anche della Corte dei Conti anche attraverso banche dati tematiche da utilizzare per le attività di intelligence, di verifica fiscale e per le decisioni di politica economica. In questo contesto, la Sogei ha sviluppato metodologie di controllo per dare Maggiore efficacia alle azioni di prevenzione e contrasto all'evasione e per migliorare la qualità dei controlli e delle verifiche nella fase dell'accesso e nella ricostruzione dei redditi e volume d'affari, segnalando gli elementi da rilevare e la documentazione da acquisire. Gli strumenti disponibili sono tra loro integrati rispondono al quadro normativo e organizzativo previsto per le attività di intelligence degli uffici dell'amministrazione e permettono di effettuare i controlli e di fornire supporto alla fase del contraddittorio con il contribuente dell'accertamento fiscale. Alla luce di quanto osservato appare chiaro che si aprono scenari nuovi che meritano di essere indagati senza esitazione e timori e che inducono alla sperimentazione dell'intero strumentario fiscale[34].
In relazione ad eventuali perplessità inerenti l'applicazione di un siffatto sistema ai fini della determinazione delle pene pecuniarie, si segnalano le recenti riflessioni della dottrina sul trattamento dei dati personali nei sistemi di I.A. per fini di interesse pubblico.
Lo studioso R. Trezza sottolinea che, nello spazio di sperimentazione normativa per l'I.A. i dati personali legalmente raccolti per altre finalità sono trattati ai fini dello sviluppo e delle prove nello spazio di sperimentazione di determinati sistemi di I.A. innovativi alle seguenti condizioni: a) i sistemi di I.A. innovativi sono sviluppati per salvaguardare un interesse pubblico rilevante in uno o più dei seguenti settori: i) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse, sotto il controllo e la responsabilità delle autorità competenti. Il trattamento si basa

online Giustizia Insieme , consultabile al seguente indirizzo url https://www.giustiziainsieme.it/ Richiamato in Consulta online https://www.giurcost.org/decisioni/2022/0028s-22.html
[34] A. URICCHIO, *Prospettive per l'introduzione di nuovi modelli di prelievo materia di intelligenza artificiale anche alla luce del coverplan*, in U. RUFFOLO (a cura di), *XXVI lezioni in diritto dell'intelligenza artificiale*, Giappichelli, Torino, 2021 pagina 447- 448.

sul diritto degli Stati membri o dell'Unione; ii) la sicurezza pubblica e la sanità pubblica, compresi la prevenzione, il controllo e il trattamento delle malattie; iii) un elevato livello di protezione e di miglioramento della qualità dell'ambiente; b) i dati non possono essere trattati con la procedura anonimizzata, sintetica o di altri dati non personali; c) esistono meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti fondamentali degli interessati durante la sperimentazione nello spazio di sperimentazione e meccanismi di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento; d) i dati personali da trattare nel contesto dello spazio di sperimentazione sono in un ambiente di trattamento dei dati funzionalmente separato, isolato e protetto sotto il controllo dei partecipanti e solo le persone autorizzate hanno accesso a tali dati; e) i dati personali trattati non devono essere trasmessi, trasferiti o altrimenti consultati da terzi; f) il trattamento di dati personali nel contesto dello spazio di sperimentazione non comporta misure o decisioni aventi ripercussioni sugli interessati; g) i dati personali trattati nell'ambito dello spazio di sperimentazione sono cancellati una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali; h) i *log* del trattamento dei dati personali nel contesto dello spazio di sperimentazione sono conservati per la durata della partecipazione allo spazio di sperimentazione e per un anno dopo la sua cessazione, al solo scopo di adempiere gli obblighi di rendicontazione e documentazione e solo per il tempo necessario per adempiere tali obblighi; i) una descrizione completa e dettagliata del processo e della logica alla base dell'addestramento, delle prove e della convalida del sistema di I.A. è conservata insieme ai risultati delle prove nell'ambito della documentazione tecnica; j) una breve sintesi del progetto di I.A. sviluppato nello spazio di sperimentazione, dei suoi obiettivi e dei risultati attesi è pubblicata sul sito *web* delle autorità competenti[35].

Ad ulteriore conferma si richiamano i Considerando della Direttiva (UE) 2016/680 del Parlamento europeo e del consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio[36]:

> (3) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della raccolta e della condivisione di dati personali è aumentata in modo significativo. La tecnologia, come mai in precedenza, consente il trattamento di dati personali, come mai in precedenza, nello svolgimento di

[35] R. TREZZA, *Artificial Intelligence Act Giudizio "ciclico" di meritevolezza e accountability intelligenti*, Universitalia, Roma, 2021, p.93-94.

[36] Direttiva (Ue) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 *relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio* consultabile al seguente indirizzo url indirizzo url https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016L0680.

attività quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali.

(4) La libera circolazione dei dati personali tra le autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, inclusi la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, all'interno dell'Unione e il trasferimento di tali dati personali verso paesi terzi e organizzazioni internazionali, dovrebbe essere agevolata garantendo al tempo stesso un elevato livello di protezione dei dati personali. Ciò richiede la costruzione di un quadro giuridico solido e più coerente in materia di protezione dei dati personali nell'Unione, affiancato da efficaci misure di attuazione.

(7) Assicurare un livello uniforme ed elevato di protezione dei dati personali delle persone fisiche e facilitare lo scambio di dati personali tra le autorità competenti degli Stati membri è essenziale al fine di garantire un'efficace cooperazione giudiziaria in materia penale e di polizia. Per questo sarebbe auspicabile un livello di tutela equivalente in tutti gli Stati membri dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento dei diritti degli interessati e degli obblighi di tutti coloro che trattano dati personali, nonché poteri equivalenti per controllare e garantire il rispetto delle norme di protezione dei dati personali negli Stati membri.

(26) Qualsiasi trattamento di dati personali dovrebbe essere lecito, corretto e trasparente nei confronti della persona fisica interessata e perseguire unicamente fini specifici previsti dalla legge. Ciò non impedisce di per sé alle autorità incaricate dell'applicazione della legge di svolgere attività quali operazioni di infiltrazione o videosorveglianza. Tali attività possono essere svolte a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, purché siano previste dalla legge e costituiscano una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei legittimi interessi della persona fisica interessata. Il principio di trattamento corretto proprio della protezione dei dati è una nozione distinta dal diritto a un giudice imparziale sancito nell'articolo 47 della Carta e nell'articolo 6 della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU). È opportuno che le persone fisiche siano sensibilizzate rispetto ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento dei loro dati personali, nonché alle modalità di esercizio dei loro diritti in relazione al trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta. I dati personali dovrebbero essere adeguati e pertinenti alle finalità del trattamento. Dovrebbe, in particolare, essere garantito che la raccolta dei dati personali non sia eccessiva e che i dati siano conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde garantire che i dati non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. Gli Stati membri dovrebbero stabilire garanzie adeguate per i dati personali conservati per periodi più lunghi per finalità di archiviazione nel pubblico interesse o per finalità scientifiche, storiche o statistiche.

(29) I dati personali dovrebbero essere raccolti per finalità determinate, esplicite e legittime rientranti nell'ambito di applicazione della presente direttiva e non dovrebbero essere trattati per finalità incompatibili con le finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. Se i dati personali sono trattati dallo stesso o da un altro titolare del trattamento per una finalità rientrante nell'ambito di applicazione della presente direttiva diversa da quella per la quale sono stati

raccolti, tale trattamento dovrebbe essere consentito purché sia autorizzato conformemente alle disposizioni giuridiche applicabili e sia necessario e proporzionato a tale altra finalità.

(34) Il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, dovrebbe riguardare qualsiasi operazione o insieme di operazioni compiute nei confronti di dati personali o insiemi di dati personali per tali finalità, con l'ausilio di strumenti automatizzati o in altro modo, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, il raffronto o l'interconnessione, la limitazione del trattamento, la cancellazione o la distruzione. In particolare, le norme della presente direttiva dovrebbero applicarsi alla trasmissione di dati personali ai fini della presente direttiva a un destinatario a essa non soggetto. Per tale destinatario si dovrebbe intendere la persona fisica o giuridica, l'autorità pubblica, l'agenzia o qualsiasi altro organismo a cui i dati personali sono comunicati in modo lecito dall'autorità competente. Se i dati personali sono stati inizialmente raccolti da un'autorità competente per una delle finalità della presente direttiva, il regolamento (UE) 2016/679 dovrebbe applicarsi al trattamento di tali dati per finalità diverse da quelle della presente direttiva, qualora detto trattamento sia autorizzato dal diritto dell'Unione o dello Stato membro. In particolare, le norme del regolamento (UE) 2016/679 dovrebbero applicarsi alla trasmissione di dati personali per finalità che non rientrano nell'ambito di applicazione della presente direttiva. Al trattamento di dati personali da parte di un destinatario che non è un'autorità competente o che non esercita tale funzione ai sensi della presente direttiva e a cui i dati personali sono comunicati in modo lecito da un'autorità competente, dovrebbe applicarsi il regolamento (UE) 2016/679. Nell'attuare la presente direttiva, gli Stati membri dovrebbero poter precisare ulteriormente l'applicazione delle norme del regolamento (UE) 2016/679, fatte salve le condizioni in esso stabilite.

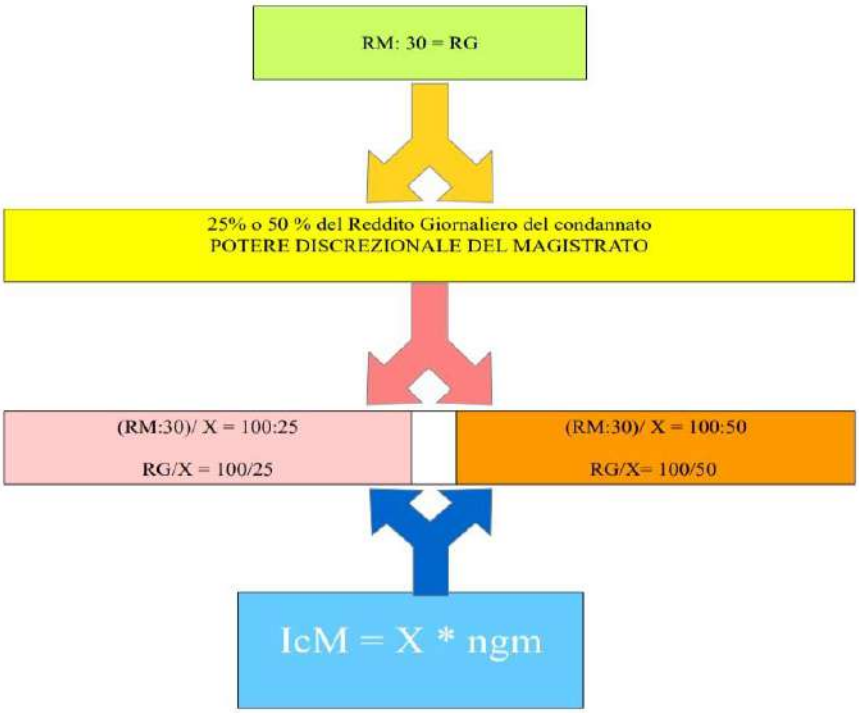
(35) Per essere lecito, il trattamento dei dati personali a norma della presente direttiva dovrebbe essere necessario per l'esecuzione di un compito svolto nell'interesse pubblico da un'autorità competente in base al diritto dell'Unione o dello Stato membro a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. Tali attività dovrebbero comprendere la salvaguardia degli interessi vitali dell'interessato. L'adempimento dei compiti di prevenzione, indagine, accertamento e perseguimento di reati, affidato istituzionalmente per legge alle autorità competenti, consente a queste ultime di richiedere od ordinare alle persone fisiche di dare seguito alle richieste formulate. In tal caso il consenso dell'interessato, quale definito nel regolamento (UE) 2016/679, non dovrebbe costituire la base giuridica per il trattamento di dati personali da parte delle autorità competenti. Qualora sia tenuto ad adempiere un obbligo legale, l'interessato non è in grado di operare una scelta autenticamente libera, pertanto la sua reazione non potrebbe essere considerata una manifestazione di volontà libera. Ciò non dovrebbe impedire agli Stati membri di prevedere per legge che l'interessato possa acconsentire al trattamento dei propri dati personali ai fini della presente direttiva, ad esempio per test del DNA nell'ambito di indagini penali o per il monitoraggio della sua ubicazione mediante dispositivo elettronico per l'esecuzione di sanzioni penali.

D’altronde si segnala il recente testo della dottrina (V. CARBONE) in materia di processo tributario in Cina in cui si segnala che si ha una forte telematizzazione dei processi in Cina. Da anni, infatti la Giustizia cinese si è spesa per creare un sistema nazionale di “Corti intelligenti” (智慧法院 Zhihui fayuan), le quali utilizzano sistemi di blockchain, cloud, big data ed intelligenza artificiale nelle varie attività processuali. L’utilizzo di tali strumenti integra l’attività del giudice

nell'individuare ed interpretare la legge applicabile alla fattispecie a lui sottoposta. L'impiego di una giustizia cd predittiva, apre indubbiamente nuovi scenari, garantendo maggior efficienza e certezza del diritto. Nel 2019, inoltre sono state istituite in Cina le cc.dd. "Corti mobili" (移动徵法院) Yi-dong zheng fayuan), le quali consentono a giudici e civili di accedere alle varie attività processuali in via del tutto telematica. Grazie ai sistemi di identificazione elettronica, quali il riconoscimento facciale, è possibile prendere parte ad udienza e scambiare documenti mediante il proprio *smartphone*[37].
Altro esponente della dottrina (A. DI PIETRO), dopo aver premesso che con Leva fiscale si introduce un carattere della visione dinamica del prelievo che ben si concilia con l'applicazione al campo tributario dell'intelligenza artificiale, ne valorizza il ruolo di garanzia del rispetto della capacità contributiva.
Gli esiti interpretativi ottenuti dalla applicazione dell'intelligenza artificiale dovranno pur sempre essere coerenti con quella Capacità contributiva sulla quale si regge la razionalità delle scelte impositive nazionali, quelle che attuano la leva fiscale. Una garanzia costituzionale destinata ad ispirare, naturalmente, gli esiti interpretativi dell'intelligenza artificiale e a valorizzarne un'ulteriore utilità. L'esito, infatti, di tale elaborazione può servire anche a mettere in evidenza aspetti di incoerenza nell'interpretazione giurisprudenziale o nell' applicazione amministrativa. Quando le soluzioni elaborate dalla giurisprudenza o adottate dalla prassi si possano porre in contrasto con la corretta applicazione della ragionevole distribuzione del carico tributario che la capacità contributiva intende forse sempre garantire. Un contrasto quindi, che l'intelligenza mette in evidenza, anche se, evidentemente, non può risolvere. Consente però alla leva fiscale di indirizzare responsabilmente i propri interventi per eliminare, con l'autorità che l'ordinamento le attribuisce, quelle irrazionali scelte normative che l'applicazione dell'intelligenza artificiale ha fatto emergere. Un conforto prezioso per una coerente ed efficace applicazione della leva fiscale, utile per sottrarre le scelte fiscali alle sollecitazioni della massima affermazione dell'interesse fiscale[38].

[37] J. BAI ,V. CARBONE, *Diritto commerciale e Tributario cinese*, Wolters Kluwer, Cedam, 2021 pag. 131-132.
[38] A. DI PIETRO, *Leva fiscale e divisione sociale del Lavoro*, in U. RUFFOLO (a cura di), *XXVI lezioni di diritto dell' intelligenza artificiale*, Giappichelli, Torino, 2021, pagina 452

RM = Reddito Mensile del condannato
RG = Reddito Giornaliero del condannato
X= 25 % o 50 % (in base alla valutazione del Magistrato) del Reddito Giornaliero del condannato
IcM = Importo complessivo multa
ngm = numero giorni multa



5. Pregi e Criticità della Riforma Cartabia e proposta di ritorno al Codice Zanardelli in tema di conversione.

Sicuramente la Riforma Cartabia in tema di pene pecuniarie ha risolto molte delle criticità che avevo rilevato nell'impianto normativo antecedente"[39] . Ai fini della proposta di ricerca in questa sede ci si soffermerà sull'unica criticità che ho avuto modo di rilevare. Nello specifico, il comma terzo della nuova formulazione dell'art. 660 cpp recita: "L'ordine di esecuzione contiene, altresì, l'intimazione al condannato a pena pecuniaria di provvedere al pagamento entro il termine di novanta giorni dalla notifica e l'avviso che, in mancanza, la pena pecuniaria sarà convertita nella *semilibertà sostitutiva* o, in caso di accertata insolvibilità, nel lavoro di pubblica utilità sostitutivo o nella detenzione domiciliare sostitutiva, ai sensi degli articoli 102 e 103 della legge 24 novembre 1981, n. 689, ovvero, quando deve essere eseguita una pena pecuniaria sostitutiva, nella detenzione domiciliare sostitutiva o, in caso di accertata insolvibilità, nel lavoro di pubblica utilità sostitutivo o nella detenzione domiciliare sostitutiva, ai sensi dell'articolo 71 della legge 24

[39] Si conceda il rinvio a E.QUARTA *Il procedimento di conversione delle pene pecuniarie inevase*, vol. I, II, III, IV, V, VI Universitalia 2022

novembre 1981, n. 689"[40]. La semilibertà sostitutiva[41] comporta l'obbligo di trascorrere almeno otto ore al giorno in un istituto di pena e di svolgere, per la restante parte del giorno, attività di lavoro, di studio, di formazione professionale o comunque utili alla rieducazione ed al reinserimento sociale, secondo il programma di trattamento predisposto e approvato.
Tuttavia, il carcere ha un impatto negativo sulla personalità del condannato, in ragione del fatto che la permanenza in carcere ha impatto criminogeno. A tal riguardo Marinucci sottolineava che: «*Il condannato a pena detentiva breve resta infatti in carcere troppo poco per poter partecipare anche a un ipotetico programma di risocializzazione, ma vi resta abbastanza per veder troncati i suoi legami con la vita sociale ed essere sottoposto ad influenze criminogene rovinose*»[42].
Rimangono famose le seguenti parole di von Liszt «*la pena detentiva breve non è solo priva di utilità; essa danneggia l'ordinamento giuridico più di quanto potrebbe fare la completa impunità del reo*» (CfrVon Liszt op. cit. p. 347), Scriveva.Boneville de Marsangy: «(…) l'amende est, de toutes les peines, la plus liberale, (…) la plus divisible, la plus èeconomique, la plus complètement rèmissibile, presque toujours la plus analogue au dèlit, et par consèquent la plus efficace» (Cfr. ID, op. cit., pp. 258-9) 8 (L. GOISIS)[43].
Anche alla luce delle criticità portate alla luce del Procuratore Generale di Brescia Guido Rispoli[44], secondo mio personale punto di vista si dovrebbe

[40] REDAZIONE SISTEMA PENALE, *Riforma della giustizia penale: lo schema del decreto legislativo approvato dal Consiglio dei Ministri e la relazione illustrativa*, 10 agosto 2022 consultabile al seguente indirizzo url https://www.sistemapenale.it/it/documenti/riforma-processo-penale-testo-schema-decreto-e-relazione-illustrativa

[41] Art. 55. Semilibertà sostitutiva. legge 24 novembre 1981, n. 68970 La semilibertà sostitutiva comporta l'obbligo di trascorrere almeno otto ore al giorno in un istituto di pena e di svolgere, per la restante parte del giorno, attività di lavoro, di studio, di formazione professionale o comunque utili alla rieducazione ed al reinserimento sociale, secondo il programma di trattamento predisposto e approvato ai sensi dei commi seguenti. I condannati alla semilibertà sostitutiva sono assegnati in appositi istituti o nelle apposite sezioni autonome di istituti ordinari, di cui al secondo comma dell'articolo 48 della legge 26 luglio 1975, n. 354, situati nel comune di residenza, di domicilio, di lavoro o di studio del condannato o in un comune vicino. Durante il periodo di permanenza negli istituti o nelle sezioni indicate nel primo periodo, il condannato è sottoposto alle norme della legge 26 luglio 1975, n. 354, e del decreto del Presidente della Repubblica 30 giugno 2000, n. 230, in quanto compatibili. Nei casi di cui all'articolo 66, il direttore riferisce al magistrato di sorveglianza e all'ufficio di esecuzione penale esterna. Il semilibero è sottoposto a un programma di trattamento predisposto dall'ufficio di esecuzione penale esterna ed approvato dal giudice, nel quale sono indicate le ore da trascorrere in istituto e le attività da svolgere all'esterno. Si applica in quanto compatibile l'articolo 101, comma 2, del decreto del Presidente della Repubblica 30 giugno 2000, n. 230. L'ufficio di esecuzione penale esterna è incaricato della vigilanza e dell'assistenza del condannato in libertà, secondo le modalità previste dall'articolo 118 del decreto del Presidente della Repubblica 30 giugno 2000, n. 230. Si applicano in quanto compatibili le disposizioni previste dall'articolo 101, commi 1, 6, 7 8 e 9, del decreto del Presidente della Repubblica 30 giugno 2000, n. 230. Al condannato alla pena sostitutiva della semilibertà non si applica l'articolo 120 del decreto legislativo 30 aprile 1992, n. 285. V. art. 71, co. 1, lett. b) dello schema di decreto REDAZIONE SISTEMA PENALE, *Riforma della giustizia penale: lo schema del decreto legislativo approvato dal Consiglio dei Ministri e la relazione illustrativa*, 10 agosto 2022 consultabile al seguente indirizzo url https://www.sistemapenale.it/it/documenti/riforma-processo-penale-testo-schema-decreto-e-relazione-illustrat

[42] C. PERINI, *Prospettive attuali dell'alternativa al carcere tra emergenza e rieducazione*, Diritto penale contemporaneo n. 4/ 2017 https://dpc-rivistatrimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_4_17_Perini.pdf.

[43] L. GOISIS, *La pena pecunaria, un'indagine storica e comparata: profili di effettività della sanzione*, Giuffrè, Milano, 2008, pag. 20-21.

[44] F. MANTI, *I pm diventano esattori. Chi non paga le sanzioni finisce dritto in galera* - ilGiornale.it 14 novembre 2022 consultabile al seguente indirizzo url https://www.ilgiornale.it/news/politica/i-pm-diventano-esattori-chi-non-pagasanzioni-finisce-dritto-2085049.html; F. MANTI, *Riforma Cartabia, ora è allarme. "Potenziare la*

optare in via esclusiva per la conversione delle pene pecuniarie non pagate in lavori di pubblica utilità. Da studiosa ho sempre optato per soluzioni che portassero alla prevalenza della sicurezza dei cittadini, ma in questo caso non si tratta di soggetti socialmente pericolosi, ma semplicemente di soggetti che non avendo adempiuto all'obbligo di pagamento delle pene pecuniarie devono pagare il proprio debito con la giustizia. Un ritorno al comma 4 dell'art. 19 del Codice Zanardelli andrebbe a vantaggio dello Stato, del condannato e anche della comunità. Certamente in ipotesi di rifiuto del condannato si potrebbe poi optare per la semilibertà. *L 'art. 19 comma 4° del Codice Zanardelli prevedeva che* «alla detenzione può essere sostituita, ad istanza del condannato, la prestazione di un'opera determinata a favore dello Stato, della Provincia o del Comune; e due giorni di lavoro sono ragguagliati ad un giorno di detenzione». Il legislatore del 1930, a differenza di quello del 1889, non prevedeva la possibilità di scontare la pena convertita lavorando a favore di enti pubblici od in opere di pubblica utilità, anche se il quasi coevo R.D. 18 giugno 1931, n. 787, il c.d. Regolamento per gli istituti di prevenzione e pena, successivamente abrogato, stabiliva per i detenuti da conversione l'assegnazione a sezioni speciali degli stabilimenti carcerari (art. 39), l'esclusione dal periodo di isolamento per osservazione (art. 49) e l'eventualità dell'assegnazione a lavori diversi da quelli organizzati nello stabilimento[45].
Ai sensi della vigente normativa lo svolgimento di attività lavorativa a beneficio della collettività può costituire:

- una forma di riparazione che il condannato pone in essere nei confronti della collettività quale parte offesa dal fatto criminoso commesso;
- un'attività di indubbia valenza per il reo, in quanto effetto e momento di un processo di reintegrazione sociale;
- una soluzione al rischio di recidiva[46].

Anche in Perù la dottrina penalistica (Abogado por la Universidad de San Antonio Abad del Cusco Germán Ramiro Alatrista Muñiz) sta analizzando la frontiera della Giustizia Riparativa. In particolare, a titolo esemplificativo ha richiamato il caso in cui un giovane ruba a una donna anziana, sottraendole la borsa, ma viene successivamente arrestato nei pressi del luogo in cui è avvenuto il furto. Dopo il furto, la donna aveva paura di uscire per strada da sola; grazie alla mediazione, è stata in grado di esprimere i suoi sentimenti al momento del crimine, e il ladro ha spiegato perché ha commesso il gesto e si è scusato con la donna. L'assunzione di responsabilità attraverso la mediazione ha comportato una riduzione della pena che il condannato doveva scontare[47].
Per recidere la catena produttiva dell'ingente recidivismo registrato per chi sconta la pena in carcere si deve risalire alla più evidente causa strutturale che

---

Sorveglianza" - ilGiornale.it 15 novembre 2022 consultabile al seguente indirizzo url https://www.ilgiornale.it/news/politica/riforma-cartabiaora-allarme-potenziare-sorveglianza-2085338.html

[45] M. SCHIAVI, *La conversione delle pene pecuniarie: dal principio di inderogabilità della pena al bilanciamento di interessi costituzionalmente rilevanti*, in *Riv. it. dir. e proc. Pen.*, 1989, pag. 722-723.

[46] A. ALDI , V. LO CASCIO, *Lavori di pubblica utilit: il progetto "Mi riscatto per il futuro"* in I. PICCININI, P. SPAGNOLO (a cura di), *Il Reinserimento dei detenuti Esperienze applicative e novità legislative* Giappichelli, Torino 2020, pag. 204.

[47] G.R. ALATRIST MUÑIZ, *Justicia Restaurativa Como Un Modo De sanción Alternativa*, in YachaQ: Revista de Derecho, 2021, 12, pagg. 97-105. https://doi.org/10.51343/yq.vi12.773; si segnala A. ZAPPULLA, *Giustizia e perdono: un connubio possibile*, Phôs 9 (2017) 1, 90-108; A. ZAPPULLA, "*Una Giustizia dal volto umano: pensieri e parole del Cardinal Carlo Maria Martini*", Synaxis XXXVI (2018) 2, 93- 104

è all'origine di tale fenomeno: e questa non può che essere la pena detentiva. Rieducare ai fini del reinserimento in ambito intramurario è operazione possibile, ma le condizioni non sono quelle ideali: problemi come il sovraffollamento, la promiscuità e la carenza di mezzi e persone specializzate rischiano alcune volte di trasformare – salvo lodevoli e meritorie eccezioni- la rieducazione in uno pseudo trattamento e il successivo reinserimento in una chimera: con buona pace del dettato costituzionale espresso dall'art. 27 Cost..
In generale anche lo stesso lavoro penitenziario ha effetto benefici. Fra i numerosi benefici del lavoro penitenziario sono da annoverare la rottura della cronicizzazione dei modi di pensare, che portano i soggetti a ripetere gli stessi comportamenti e, come comprovato dai dati statistici, il forte abbattimento della recidiva[48] In tal senso i criminologi si sono lungamente interrogati su quali fossero le "cause" che portano una persona a commettere un crimine, ovvero quali variabili incidono sulla probabilità che un individuo infranga la legge. Tra queste la mancanza di un impiego è riconosciuta come uno dei fondamentali fattori di rischio per la delinquenza. In questo senso, le attività lavorative e di formazione al lavoro svolte negli istituti possono avere un impatto significativo sulla recidiva[49].

6. Proposta di ricerca: valorizzazione della pena pecuniaria come volano per il superamento delle problematiche del sistema carcerario.

La nostra Costituzione all'art. 27 sostiene che «le pene non possono consistere in trattamenti contrari al senso di umanità e devono tendere alla rieducazione del condannato», sottintendendo che il carcere non sia l'unica pena. L'art. 27 Cost. non richiede né pentimento, né di uscire da un orizzonte morale, ma di ritornare nel contesto di natura costituzionale ovvero della convivenza [50] Relativamente alla necessità di dare nuova linfa alla pena pecuniaria si vedano le riflessioni anche dello stesso Ministro ROCCO che nel 1928 nella Relazione Ministeriale al Disegno di Legge aveva evidenziato: «Occorrerà anzitutto, sottoporre ad una revisione attenta e sagace il vigente sistema delle pene, dei surrogati e dei complementi penali, nonché degli effetti penali delle condanne. E ciò al fine precipuo di rinvigorire la scaduta efficacia e sminuita forza assicuratrice, intimidatrice, satisfattrice della pena, ora accentuandone, ove occorra, il rigore e la gravità; ora introducendo, in aggiunta, ovvero in sostituzione delle attuali sanzioni penali, nuove, più efficaci e più praticamente realizzabili specie di pene; ora, infine, facendo un diverso e più largo uso delle pene persistenti, come, ad esempio, delle pene pecuniarie»[51]

---

[48] G. CHIOLA, *Il sistema carcerario italiano. Profili Costituzionali*, Giappichelli Editore, Torino, 2020, pag. 142. L'Autore richiama i dati del MiniDossier openpolis, Dentro o Fuori, n. 9 del 2016, in cui il tasso della recidiva è pari al 68,45 %, mentre di coloro che vengono affidati prima della scarcerazione ai servizi sociali è di 19,02%.

[49] F. GIORDANO, *La misurazione d'impatto delle attività lavorative in carcere*, in I. PICCININI, P. SPAGNOLO (a cura di), *Il Reinserimento dei detenuti Esperienze applicative e novità legislative* Giappichelli, Torino 2020, pag. 262.

[50] G. CHIOLA, *I diritti dei detenuti sono ancora da intendersi uti persona, uti cives e uti captivus?* In G. CHIOLA. *Il sistema carcerario italiano Profili costituzionali* Giappichelli Editore 2020, pag. 30.

[51] MINISTERO DELLA GIUSTIZIA E DEGLI AFFARI DI CULTO, *Atti parlamentari della Legge 24 dicembre 1925, n. 2260, che delega al Governo del Re la facoltà di emendare i Codici penale e di procedura penale / Ministero della Giustizia e degli Affari di Culto Roma*: Provveditorato Generale dello Stato, Libreria, 1928, pag. 14.

7. Modello ipotizzato[52] per rendere moderno il sistema sanzionatorio italiano.

Come poc'anzi affermato la dottrina d'oltralpe, ha posto in evidenza che il legislatore Rocco, non utilizzando le potenzialità politico-criminali della pena pecuniaria, «ha fatto invecchiare di mezzo secolo il codice penale in uno dei suoi punti decisivi» (BOSCH [53] 1978, 468) [54] È diventato un vero e proprio Leitmotiv il passo del manuale di Jescheck [55] (edizione 1972), secondo cui «la pietra angolare di ogni sistema sanzionatorio moderno riposa nei surrogati della pena detentiva»[56]



Il Modello ipotizzato[57] si sostanzia in un raffronto tra i dati attuali relativi all' attuale sistema di applicazione delle pene pecuniarie e relative conversioni con

52 Si segnala per l'ambito civilistico che partendo dal testo Interpretazione della legge con modelli matematici. dello studioso Luigi Viola è stato elaborato GiuriMatrix è un Software giuridico dotato di Intelligenza Artificiale, per dare risposte normative a domande poste con linguaggio naturale. È dotato di Giurisprudenza e Dottrina che servono ad orientare il sistema sulla risposta normativa più pertinente; ciò in ragione del rilievo decisivo che solo la legge è vincolante per tutti, così risultando l'unica risposta "attendibile", mentre la giurisprudenza, avvinta dai limiti del giudicato, è solo orientativa. GiuriMatrix utilizza, in parte, l'algoritmo spiegato nel libro – Best Seller Amazon International Law (tradotto in 6 lingue) – Interpretazione della legge con modelli matematici L. Viola, GiuriMatrix, software giuridico con Intelligenza Artificiale - Scuola di Diritto Avanzato - Corsi Esame Avvocato scritto e orale 2017-2018, consultabile al seguente indirizzo url https://www.scuoladirittoavanzato.com/2022/03/25/giurimatrix-software-giuridico-con-intelligenza-artificiale-intervista-ai-fondatori

53 J. BOSCH, *Die Geldstrafe in Italien*, in H. H. JESCHECK, G. GREBING, *Die Geldstrafe in deutschen und ausländischen Recht, BadenBaden*, 1978, 468.

54 L. GOISIS, *Le pene pecuniarie. Storia, comparazione, prospettive*, in Diritto Penale Contemporaneo, 22 novembre 2017, pag. 4-5

55 JESCHECK, *Lehrbuch des Strafrecht*, A.T., 1972, pag. 576

56 C. PERINI, *Prospettive attuali dell'alternativa al carcere tra emergenza e rieducazione*, Diritto penale contemporaneo n. 4/ 2017 https://dpc-rivistatrimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_4_17_Perini.pdf

57 Le giornaliste Milena Gabanelli e Simona Ravizza evidenziano che: "Per fare le verifiche sul patrimonio e il redditore reale serve l'intervento della Guardia di Finanza con indagini approfondite e dispendiose" M. GABANELLI, S. RAVIZZA, *Criminalità quei 6 miliardi che l'Italia regala ai condannati,* 1 dicembre 2019, Corriere.it consultabile al seguente indirizzo url https://www.corriere.it/dataroom-milena-gabanelli/criminalita-giustizia-penepecuniarie-6-miliardi-euro-italia-regala-condannati/16e2f17c-1457-11ea-9463-2153cf12a84f-va.shtml

* Costi per lo Stato si v. Si veda contributo S. PAZIENZA, E. QUARTA, *Sovraffollamento, il ruolo di organo di controllo internazionale della CEDU e costi economici della detenzione* in E. QUARTA *Il procedimento di conversione delle pene pecuniarie inevase*, vol. II. Universitalia. 2022, pag, 177-179; E. QUARTA, *Conversione delle pene pecuniaria conseguenti a sentenza penale di condanna: pregi e criticità della Riforma Cartabia e*

ricadute su dati relativi a reinserimento sociale /recidiva (X e Y già noti) e raffronto con un valore futuro ottenuto inserendo delle variazioni ossia potenziamento della pena pecuniaria attraverso sistema tassi giornalieri e la relativa conversione delle pene pecuniarie in lavori di pubblica utilità). Valore futuro calcolato attraverso la funzione di previsione.
Altresì si ipotizza che la percentuale di riscossione delle pene pecuniarie aumenterebbe laddove ci fosse una maggiore sensibilizzazione, anche negli ambienti carcerari, sulla percezione che si dovrebbe avere della pena pecuniaria. La pena pecuniaria non è un'ancella della pena detentiva, ma la pena pecuniaria contribuisce, allo stesso titolo della pena detentiva, a costituire la pena principale del reato (Cass. Pen., sez. I, 15 ottobre 2004, n. 47715 C.E.D. Cass. n. 230408; in senso analogo in dottrina v. Manzini, Trattato III 767 secondo cui in caso di pena detentiva e di pena pecuniaria cumulativamente inflitte, il termine decorre dal giorno in cui tutte furono estinte)[58]

Attuale sistema di applicazione pene pecuniarie	MODELLO PROPOSTO
CAMPIONE Sistema a somma complessiva	Stesso CAMPIONE Sistema a Tassi Giornalieri (si ipotizza)
VALORE NOTO ATTUALE Tasso riscossione Costi accertamento Guardia di Finanza Costi derivanti da Conversione Sovraffollamento Casi Riabilitazione per il detenuti	VALORE FUTURO FUNZIONE DI PREVISIONE - Aumenta tasso di riscossione - Meno costi derivanti dall'Accertamento da parte della Guardia di Finanza - Meno costi per lo Stato derivanti dalla conversione (detenzione, spese mantenimento) - meno sovraffollamento - Aumento casi di Riabilitazione per il detenuto
Conversione pene pecuniarie inevase (ipotesi conversione in semilibertà, detenzione domiciliare)	Conversione pene pecuniarie inevase Sistema ipotizzato ripristino art. 19 comma 4 Codice Zanardelli « alla detenzione può essere sostituita, ad istanza del condannato, la prestazione di un'opera determinata a favore dello Stato, della Provincia o del Comune; e due giorni di lavoro sono ragguagliati ad un giorno di detenzione N.B.: ovviamente occorre tenere conto di ipotesi in cui il condannato rifiuti e quindi si ipotizza conversione in semilibertà o detenzione domiciliare)
VALORE ATTUALE NOTO Tasso di recidiva	***VALORE FUTURO FUNZIONE DI PREVISIONE*** ***Maggiore vicinanza alla Funzione rieducativa*** ***Diminuzione tasso di recidiva***

8. Conclusioni: la pena pecuniaria contribuisce a costituire la pena principale del reato.

Nell'Antichità Classica la pena pecuniaria, si è rivelato un prezioso strumento sanzionatorio che gli antichi greci hanno donato al sistema penale e che, come evidenziato dalla Prof.ssa Eva Cantarella, ha consentito di giungere ad uno switch dal Mondo della Vendetta al Mondo del diritto. In conclusione, secondo la scrivente ridando centralità alla pena pecuniaria, - come accade ad esempio

relative proposte di miglioramento rivolte al Governo Meloni, volume VI, Universitalia, Roma, 2022 pag. 96 e ss.

[58] R. GARGIULO, M. VESSICCHELLI, *Art. 179*, in G. LATTANZI, E. LUPO, *Codice penale. Rassegna di giurisprudenza e di dottrina*, Giuffrè, Milano, 2010, pag. 681.

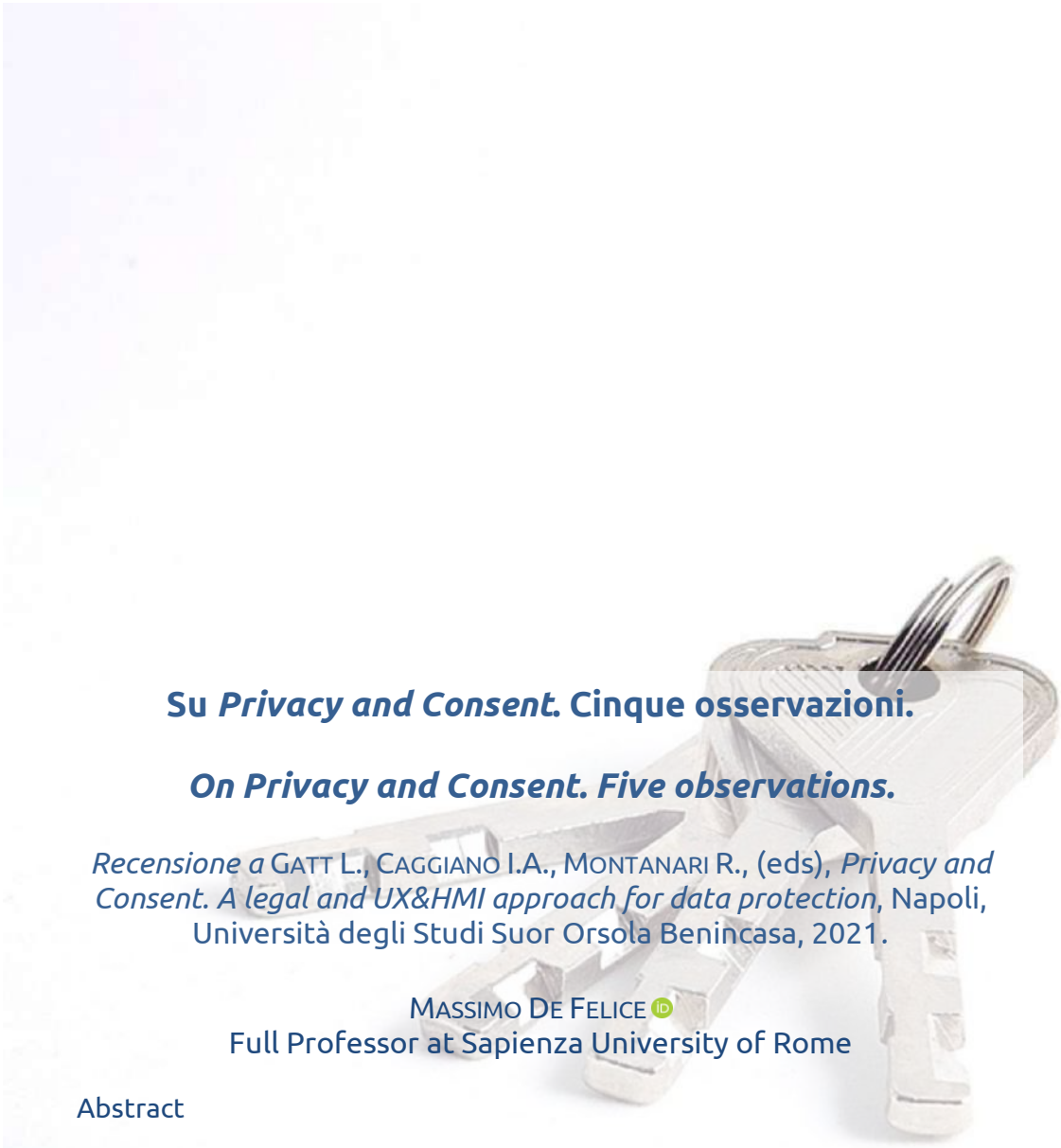
nel sistema tedesco-[59],anche nel XX Secolo la pena pecuniaria può nuovamente realizzare una transizione, proiettando il Codice penale del 1930 ed sistema penitenziario nel suo complesso nel futuro.

[59] Si conceda il rinvio a E.QUARTA, *Il procedimento di conversione delle pene pecuniarie inevase*, vol. I, II, III, IV, V, VI Universitalia 2022.

SECTION II
REVIEWS

De Felice M, 'Su Privacy and Consent. Cinque osservazioni' (2022) 2 EJPLT, 265-271.
DOI: https://doi.org/10.57230/EJPLT222MDF

EJPLT
ISSN 2704-8012



Su *Privacy and Consent*. Cinque osservazioni.

On Privacy and Consent. Five observations.

Recensione a GATT L., CAGGIANO I.A., MONTANARI R., (eds), *Privacy and Consent. A legal and UX&HMI approach for data protection*, Napoli, Università degli Studi Suor Orsola Benincasa, 2021.

MASSIMO DE FELICE
Full Professor at Sapienza University of Rome

Abstract

Si propongono brevi osservazioni in margine agli esiti del progetto di ricerca su "Privacy and Consent". Almeno cinque sono i collegamenti con dibattiti in corso: sulle "anomalie del comportamento", sul valore delle informazioni "involontarie", sulla cibersicurezza, sulla cosiddetta "intelligenza artificiale", sull'atteggiamento "anti-disciplinare" necessario per far fronte all'innovazione nelle "corporate technologies" (e eventualmente intervenire con «fundamental changes in the law»).

Brief notes are proposed to accompany the outcomes of the research project on "Privacy and Consent". There are at least five links to ongoing debates: on "behavioural anomalies", on the value of "involuntary" information, on cybersecurity, on "artificial intelligence", on the "anti-disciplinary" attitude required to tackle innovation in "corporate technologies" (and possibly intervene with «fundamental changes in the law»).

© The author(s) 2022, 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: privacy; cybersecurity; interdisciplinary approach.

Sommario: Premessa. – 1. Sulle incoerenze tra le risposte al questionario. – 2. Il «plusvalore documediale». – 3. Il "cyber risk". – 4. Anticipare i problemi, l'esigenza "anti-disciplinare". – 5. Il «legal design», l'"anti-disciplinare", la formazione.

Premessa.

Il progetto di ricerca su "Privacy and Consent" è stato finalizzato a valutare «Italian users' awareness and their sensitivity towards privacy (measured by their consenting to data processing) when installing an operating system on a personal computer»; e a verificare quanto la legislazione (italiana e europea) «can assure effective protection of users with regard to the processing of personal data and especially where the request for processing take place in a digital enviroment». La metodologia utilizzata è potente: rilevazione dei comportamenti «during the installing of the program and its use» (con raffinata strumentazione high-tech); verifica di conoscenze e attitudini dell'utente con un vasto questionario[1].

Sono stati coinvolti nell'indagine settatacinque «volunteer individuals from the Suor Orsola Benincasa University, including students, teachers and non-teaching staff, as well as volunteers from outside». Sebbene il campione non sia di "alta numerosità", i risultati dell'analisi offrono spunti preziosi per approfondimenti e prospettive di sviluppo della ricerca (anche con estensione dell'ambito problematico, a esempio nel campo delle cosiddette *CorpTech*, le "corporate technologies").

In questa breve nota si propongono cinque osservazioni (in parte collegate a dibattiti correlati), che potranno apparire anche "eccentriche"; hanno esclusivamente la valenza di "un fatto": son quelle annotate (in margine) da un lettore durante la lettura.

1. Sulle incoerenze tra le risposte al questionario.

In "Privacy and Consent" sono riportate e discusse le risultanze di un «questionario di profilazione», molto articolato (sono sessanta le chiavi di indagine). L'analisi di comparazione segnala incoerenze tra le risposte.

È situazione spesso rilevata: si ritrova anche nelle analisi dei questionari sul livello di cultura (consapevolezza) finanziaria e assicurativa[2]. È fenomeno

[1] GATT L., CAGGIANO I.A., MONTANARI R., (eds), *Privacy and Consent. A legal and UX&HMI approach for data protection*, Napoli, Università degli Studi Suor Orsola Benincasa, 2021; precisa descrizione dell'impianto metodologico è alle pagine 13-16, il questionario (in italiano) alle pagine 159-170.

[2] Utile riferimento, per valutazioni comparative è l'indagine (promossa dall'Ivass, pubblicata a maggio 2021) su "Conoscenze e comportamenti assicurativi degli italiani". Oltreché definire «un sistema di misurazione del livello di conoscenze», l'indagine aveva la finalità di «fornire la base per l'individuazione delle strategie più efficaci per promuovere la cultura assicurativa». Ha utilizzato un questionario di 54 domande (raggruppate in «aree tematiche»); ha raccolto risposte da più di duemila intervistati.
Anche qui si rilevano "incoerenze" da indagare. Caso emblematico il disallineamento tra "percezione del rischio" e "sottoscrizione di polizze": «coloro che sottoscrivono una Polizza Malattie sono solo il 10.6% del

attribuito alle "anomalie nel comportamento"; non facile è l'identificazione delle cause (specifiche), né il ruolo delle loro concorrenze.

A commento dell'analisi proposta si può segnalare che l'incoerenza non necessariamente è attribuibile a incompetenza tecnica. Sebbene in altro ambito e per diversa finalità d'indagine, utile può risultare il riferimento al caso (famoso) del colloquio sulle "Applicazioni della teoria del rischio all'economia", che si tenne in Parigi nel 1952. Nel rispondere a un questionario proposto da Maurice Allais si colsero incoerenze nelle risposte di grandi scienziati: Arrow, Boiteux, Bruno de Finetti, Friedman, Frisch, Marschak, Massé, Morlat, Samuelson, van Dantzing, Jimmie Savage, Ville. In quel caso non ci fu certo carenza di conoscenze tecniche; dichiarati furono gli effetti di impulsività e emotività (de Finetti disse di «stime grossolane e fallaci», dovute a contingenze; analoga posizione fu tenuta da Savage)[3].

Dunque, l'esito del «questionario di profilazione» stimola approfondimenti. Sarebbe un bell'esercizio indagare motivazioni di risposta con qualcuno degli intervistati.

Va anche considerato che l'impostazione – peraltro vastamente diffusa – di alcuni quesiti (quelli con scala da 1 a 5, o comunque con 5 alternative: del tipo quesito 37, e quesito 34) induce ambiguità nell'analisi dei risultati, essendo i livelli della scala lasciati alla libera interpretazione (e definizione). Verifiche sull'interpretazione della scala (da parte dei rispondenti) potrebbe arricchire l'esercizio di indagine.

2. Il «plusvalore documediale».

La prima delle domande al punto 46 del «questionario di profilazione» – «sarebbe disposto a pagare […] 20 euro [per] evitare che i suoi dati venissero venduti […] per finalità commerciali?» – evoca il fenomeno denominato del «plusvalore documediale» (indotto dalla cessione di informazioni, gratuita spesso involontaria da parte degli utenti alle piattaforme informatiche).

Il fenomeno richiede attenzioni, ma anch'esso non è, per tipologia, fenomeno nuovo. Da sempre la sottoscrizione di un contratto – si riprende il riferimento al settore assicurativo – produce "fornitura", da parte del contraente, di informazioni extra-contrattuali (registrate nel periodo di copertura della polizza) anche di tipo "comportamentale", preziose per l'impresa. Riguardano, a esempio, – per le assicurazioni sulla vita – l'effettiva durata in vita dell'assicurato, il momento dell'eventuale "riscatto", la riduzione o aumento del premio (nel caso di "premi ricorrenti"). Innovativa – nei rami danni – è la raccolta dei dati con la "scatola nera", che sostiene nuove forme di assicurazione dell'RC Auto. Sono tutte rilevazioni che arricchiscono la base informativa aziendale (le cosiddette "basi tecnico-attuariali", le caratteristiche

totale degli intervistati, percentuale che sale per la Polizza Infortuni al 20.2%, ma che comunque rimane molto bassa, rispetto al fatto che ben il 76,7% del campione indichi la salute (malattia/infortuni) come principale fonte di preoccupazione.».

[3] ALLAIS M., *Le Comportement de l'Homme Rationnel devant le Risque: Critique des Postulats et Axiomes de l'Ecole Americaine*, Econometrica, 21(1953), 4; in particolare pagine 504-505 (*english summary*) e pagine 525-526 (note 31 e 32); DE FINETTI B., Sulla preferibilità, Giornale degli economisti e Annali di economia, XI (1952), pagina 699; SAVAGE L.J., *The Foundation of Statistics*, NewYork, Dover, (1954)1972, pagina 102.

del "policyholder behaviour"), da utilizzare nei processi di pricing delle polizze, per la definizione delle strategie commerciali, per la valutazione di grandezze ("riserve", capitali a copertura dei rischi "inattesi") vincolate ai principî della normativa.

Anche questo è un «lavoro implicito»? è «lavoro non retribuito»? ciascun assicurato l'ha sempre svolto «gratuitamente a favore del capitale documentale»[4]. Se è così perché il problema si pone soltanto adesso? C'è una nuova fisionomia da indagare?

3. Il "cyber risk".

Del cyber risk si accenna a pagina 104 e se ne tratta più estesamente a pagina 113. Sappiamo essere tema di formidabile rilevanza ed estensione. Riguarda la protezione di dati e funzionalità informatiche di individui, imprese, degli Stati.

La scarsa attenzione al problema da parte degli individui non è fenomeno specifico. Alle diagnosi sugli individui, va aggiunta più rilevante la situazione delle imprese. L'ultima Relazione dell'Ivass (quella relativa al 2021) documenta «il fenomeno della sottoassicurazione […] particolarmente intenso per le coperture sui rischi cyber», le imprese con meno di 50 addetti essendo molto meno assicurate rispetto alle imprese con più di 200 addetti[5]. Anche qui c'è bisogno di approfondire e di sensibilizzare[6].

L'Osservatorio di Accredia, realizzato in collaborazione col Consorzio Interuniversitario Nazionale per l'Informatica – su "Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata" (pubblicato nel 2022) –, può fornire qualche utile spunto. Accelerata è l'evoluzione della problematica: nei dettagli tecnici, nella normativa, per le risposte che si dovranno dare a livello istituzionale.

Recente è il documento sull'"Adozione della Guida nazionale TIBER-IT", di Banca d'Italia, Consob e Ivass. Si pone cruciale motivo di riflessione e definizione di ruolo: se e come coordinare le azioni (e le modalità di test sulla verifica di qualità di apparati e processi) con la "guida" delle autorità di vigilanza; se e come partecipare al «dialogo continuo tra autorità e industria […] alle principali sedi cooperative pubblico-private nazionali»[7], prospettiva

---

[4] Tutte le citazioni tra caporali sono da FERRARIS M., *Documanità. Filosofia del mondo nuovo*, Roma-Bari, Laterza, 2021; pagine 290, 311, 293, nell'ordine.

[5] Ivass, *Relazione sull'attività svolta dall'Istituto nell'anno 2021*, Roma, 28 giugno 2022, pagina 91.

[6] Sono dati da decrittare: documentano scarsa sensibilità delle imprese a uno dei rischi emergenti del comparto informatico? C'è bisogno di più attenta e diffusa informazione sugli effetti potenziali del *cyber risk*? O segnala il giudizio sull'eccessiva onerosità del premio d'assicurazione, rispetto alla probabilità che l'impresa attribuisce alla possibilità di sinistro? E una certificazione di qualità su apparati e processi protettivi potrebbe essere considerata fattrice di riduzione del premio (entrare mitigante nell'algoritmo di *pricing*)? Forse per un *pricing* adeguato c'è carenza di informazione?
Sono domande che sollecitano – per rispondere con finalità operativa – indagini e valutazioni approfondite. Anche sulla rilevazione e sull'analisi dei dati di "incidente informatico" sarà utile condividere schemi operativi (per arrivare alla disponibilità di basi informative espressive ed efficienti per calibrare strategie d'azione): recente sul tema è il documento del Financial Stability Board (su *Achieving Greater Convergence in Cyber Incident Reporting. (Consultative Document*), 17 October 2022).

[7] Banca d'Italia, Consob, Ivass, *Guida nazionale TIBER-IT. Threat Intelligence Based Ethical Red-Teaming – Italia, Agosto 2022 – versione 1.0*; la citazione è dalla pagina 7. Il TIBER-IT simula potenziali attacchi reali riproducendo tattiche, tecniche e procedure (TTP) di attori della minaccia reali, verificando così le capacità di rilevamento, protezione e risposta. Le Autorità forniscono sostegno metodologico. Le informazioni e le

che in quella "guida" si sottolinea.

4. Anticipare i problemi, l'esigenza "anti-disciplinare".

Nel libro si richiama (a pagina 100) l'esigenza di «*interdisciplinary effort*» («*in order to understand privacy's place in society*») e di «*interdisciplinary approach*» («*by conveying legal prescription in a new form*»). È l'impostazione che al *Massachusetts Institute of Technology* qualificano "anti-disciplinare": l'avere alte le competenze di settore (legali, tecnologiche, statistiche, nella teoria delle probabilità), ma conquistare la capacità di lavoro audace negli "spazi di confine tra discipline"[8].

C'è forte accelerazione nello sviluppo delle tecnologie, che porta opportunità e rischi. Le norme sono all'inseguimento dei fenomeni; delicata è l'intersezione tra regole norme e processi decisionali[9]. Necessario e urgente è un piano di anticipazione.

I problemi che si porranno sono ben individuati: vengono dalle sempre nuove applicazioni della cosiddetta "intelligenza artificiale", del *machine learning*; nelle imprese dalle cosiddette "*corporate technologies"* (su cui si va sviluppando ampio dibattito che sollecita «*fundamental changes in the law* »[10]).

Per definire regolamenti efficienti, la collaborazione tra tecnologi, esperti di

---

indicazioni espresse in questa Guida sono fornite a scopo informativo (ai soggetti che intendono sottoporsi ai test); non intendono costituire un'interpretazione legale o di altro tipo. I test TIBER-IT sono condotti sui sistemi che sostengono le funzioni critiche di un'entità in ambiente di produzione, tenendo conto della superficie di attacco reale e delle effettive debolezze dell'entità. Il TIBER-IT non è da intendersi come strumento obbligatorio di supervisione o sorveglianza.

[8] Il ricorso alla storia – all'origine delle ricerche sui robot moderni e sulla cibernetica – aiuta a chiarire il senso dell'«anti-disciplinare». Si guardava all'organizzazione dei piani di ricerca: «Vi sono campi di lavoro scientifico che […] sono stati esplorati dai differenti punti di vista [disciplinari]; nei quali […] una rilevante quantità di lavoro viene triplicata o quadruplicata, mentre altro considerevole lavoro è ritardato dalla mancanza, in un campo, di risultati che possono già essere diventati classici nel campo vicino. Sono queste regioni di confine della scienza che offrono le più ricche opportunità al ricercatore qualificato. Esse sono al tempo stesso le più refrattarie alle correnti tecniche di attacco in massa e alla divisione del lavoro». Si esemplificava il senso dell'interazione (considerando il rapporto tra matematici e fisiologi): «[n]on occorre che il matematico sia capace di condurre un esperimento fisiologico, ma deve essere in grado di comprenderlo, di criticarlo, di suggerirlo. Né occorre che il fisiologo sia capace di dimostrare un certo teorema matematico, ma deve saperne afferrare il significato fisiologico e deve saper dire al matematico che cosa cercare» [Wiener N., *Cybernetics, or control and communication in the animal and the machine*, Cambridge, The MIT Press, 1948; edizione italiana: Wiener N., *La cibernetica. Controllo e comunicazione nell'animale e nella macchina*, Milano, il Saggiatore, 1968, pagina 25].

[9] Da perseguire con determinazione – perché prodigo di prospettive altre – il colloquio con i giuristi (negli "spazi di confine") sulle architetture del decidere. Alcuni itinerari sono stati tracciati nei «Seminari Leibniz per la teoria e la logica del diritto», voluti da Natalino Irti. L'anti-disciplinare è già nelle denominazioni dei temi che si proposero, e che hanno dato il titolo ai volumi che di quei seminari scandiscono la rete delle interrelazioni tra culture: *Calcolabilità giuridica; Il vincolo giudiziale del passato. I precedenti; Decisione robotica* (volumi tutti editi da il Mulino – nel 2017, 2018, 2019 –, a cura di Alessandra Carleo). Fascinoso fu il prepararsi per quella che Irti definì «aperta e prodiga adesione, d[e]gli studiosi di matematica finanziaria»: scoprire impensate convergenze problematiche: sul ruolo dell'astrazione, della probabilità, dell'algoritmica; su "nodi linguistici" e «cancelli delle parole»; sul ruolo di norme e regole, e della *razionalità*; sul *calculemus* di Leibniz e sulla «macchina di carta» di Alan Turing. (Qualche segno è recuperato in De Felice M., *La macchina della decisione. Colloquio con i giuristi*, Torino, Aragno, 2021.)

[10] Enriques L., Zetzsche D.A., *Corporate Technologies and the Tech Nirvana Fallacy*, Hastings Law Journal, vol. 72:55, November 2020, pagine 55, 59. Considerazioni sul ruolo innovativo che possono avere i regolamenti sono in De Felice M., Moriconi F., Mottura C., *Sulle CorpTech. Spunti dalla governance dell'impresa di assicurazione*, Sapienza Università di Roma, Rapporto tecnico 1, 2023 (ci si riferisce agli schemi di governance definiti dalla Direttiva europea "Solvency II").

processi organizzativi e giuristi è sempre più auspicabile e essenziale.

Ma sarebbe utile scendere dal dibattito sui principi alla considerazione di casi concreti, cimentarsi sui fatti, per poi tornare a astrarre – così, efficacemente – verso le fattispecie.

5. Il «*legal design*», l' "anti-disciplinare", la formazione.

Collegato all'approccio di lavoro anti-disciplinare si trova il problema complesso della comunicazione.

Nel libro si richiama il «*legal design* […] *that aims to achieving a correct and effective visualization of a legal content, favoring communication and understanding*»; e si sottolinea che «l*egal design combines law, technology, ethics, philosophy, semiotics and communication*». L'anti-disciplinare si può leggere quindi nella dichiarata necessaria «*hybridization of knowledge*», dove è auspicabile che l'*hybridization* sia intesa e realizzata nei modi della *Cybernetics* di Norbert Wiener: come fu – esemplificando – nel modo di rapporto "operativo" tra medici e matematici[11].

Resta da chiarire come impostare la forma della comunicazione, la cui efficacia potenziale non è giudicabile "in linea di principio", ma dipende – ovviamente – dal livello culturale del destinatario.

Un caso – ancora colto nel settore assicurativo – aiuta a chiarire. Gli "scenari probabilistici", richiesti dai regolamenti tra gli schemi di informazione sulla qualità dei "prodotti d'investimento *insurance-based*" (i"KID for PRIIPs")[12], possono fornire all'"investitore" buon e elegante mezzo per la valutazione e il controllo della rischiosità (e del *trade-off* rischio-rendimento), ma richiedono capacità di lettura ancora non diffusamente disponibile, richiamano – all'estremo positivo – la figura del "consumatore calcolante".

Assumono perciò rilevanza i piani di "formazione diffusa", anche di lungo periodo. Varrebbe la lungimiranza: iniziare dalla scuola, ai diversi livelli; e meglio calibrare le culture universitarie. Le esperienze della Banca d'Italia sulla formazione in economia e finanza sarebbero da estendere[13].

A proposito del «*legal design*» si richiamano (in "*Privacy and Consent*") anche le argomentazioni di Kahneman sulla «cognitive fluidity». Per completare l'armamentario comportamentale si potrebbe valutare – su casi specifici – ruolo e forme di «spinta gentile» (il *nudge*) e di «divulgazione intelligente», per contribuire alla correzione degli errori sistematici (quello che Kahneman definisce il «*de-biasing*»), a evitare o limitare l'indolenza intellettuale, ad alleviare il «lato oscuro [dello] *sludge*» (il *pantano*, «la sgradevole sostanza che rende più difficile fare scelte sensate»). A proposito del "Consent" va considerato che «alcuni architetti delle scelte creano intenzionalmente il

[11] Si rinvia alla nota n.8.

[12] Il Regolamento 41 dell'Ivass impone il Key Information Document per i cosiddetti packaged retail investment and insurance-based investments *products* (i "KID for PRIIPs").

[13] Interessanti considerazioni sugli «effetti della digitalizzazione nell'educazione finanziaria e nell'inclusione», col richiamo al tema complesso della «Science of Science Communication», sono in SIGNORINI L.F., *The impact of digitalization on financial education and inclusion, relazione al Tenth Annual Meeting of International Federation of Finance Museums*, Roma, 4 ottobre 2022.

pantano, generando attriti in un determinato processo per raggiungere i loro scopi»[14].

[14] Stringenti e eleganti sono le argomentazioni su termini concetti strategie in THALER R.H., SUNSTEIN C.R., *Nudge. La spinta gentile. L'edizione definitiva*, Milano, Feltrinelli, 2022; sullo «*sludge*» a pagina 9, nel capitolo 8.

SECTION III

FOCUS PAPERS

Marino R, Kashani SMM, 'The Mechanism of Smart Contract Conclusion in the Italy's and Iran's Legal System (2022) 2 EJPLT, 273-292.
DOI: https://doi.org/10.57230/EJPLT222RMSMMK

EJPLT
ISSN 2704-8012



The mechanism of smart contract conclusion in the Italian and Iranian legal systems.

ROBERTA MARINO
Associate Professor of Private Law, Università degli Studi di Napoli Federico II
SEYED MILAD MAHMOOD KASHANI
Ph.D. (c) Università degli Studi di Napoli Federico II

Abstract

The conclusion of smart contracts is placed on the blockchain platform due to the special features of this platform, including the two features of transparency and decriminalization. After being completed on the blockchain network, these contracts' transparency feature enables the public to observe and offer them. In this case, all the people who have access to this platform have the possibility of knowing what was transferred by whom to whom, and this not only prevents the occurrence of many related lawsuits but also many crimes related to property.

La conclusione degli smart contract avviene sulla piattaforma blockchain la quale è connotata da peculiari caratteristiche di trasparenza e depenalizzazione. Tali aspetti rendono senza dubbio lo smart contract uno strumento utile ai fini di una sicura esecuzione del contratto, ma contemporaneamente, espongono le parti al rischio di una non modificabilità di quanto pattuito anche in caso di accordo tra le stesse.

© The author(s) 2022, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: smart contract; international laws; blockchain; Secure development; technologies.

Summary: Introduction – 1. The civil law debate on smart contracts. – 2. The regulation of smart contracts in the European context and in the Italian legal system. – 3. The debate in Italy around the nature of the smart contract and the problems related to the use of smart contracts. – 4. Iranian law's implementation of smart contracts. – 5. The standards for the legality of smart contracts under Iranian law. – Conclusions.

Introduction[1]

In order to modify the mechanism of smart contracts' conclusion to the rules governing transactions in the legal systems of Iran, Italy, and the European Union, and to express the challenges facing this system in the implementation of these policies, the main question that this research seeks to address is how to make policies for the conclusion of smart contracts.

An advanced type of electronic contract is a smart contract. The primary difference between these contracts and non-electronic ones is how they are concluded. Otherwise, they are identical to non-electronic contracts. These contracts have protocols that describe the commitments made by each contracting party due to the mechanism used in them.[2] These contracts are self-executing and enforceable agreements that, despite the fact that they sometimes call for an operator to oversee the proper execution of the contract, they are executed by a computer and are made enforceable by following the rules established by the laws underlying the applicable legal system.[3]

1. The civil law debate on smart contracts.

In Italy, there is a particularly heated debate on the usefulness of using smart contracts and the 'blockchain' system, which are considered new technologies destined to change our reality in consideration of the growing importance that they assume following the diffusion of digitization processes and the networking of public and private activities and goods. Their widespread use is linked to the growing need for automation in the market.

The Italian civil law doctrine is committed to analysing these new figures in the light of contract law by posing the problem of the regulation of smart contracts, which are functional contracts for the circulation of wealth and which can be implemented, for example, through the use of blockchain technology.[4]

[1] Par. 1-2-3 belongs to Roberta Marino, Associate Professor of Private Law- University of Naples Federico II; Par. 4-5 belongs to Seyed Milad Mahmood Kashani, Ph.D. student - University of Naples Federico II.

[2] S H Safaie, *Preliminary Course of Civil Rights, Tehra*n (2nd edn, Mizan Publications 2012), 135.

[3] R O'Shields, *Smart contracts: Legal agreements for the blockcha*in (NC Banking Inst 2017), 177.

[4] He considered that these modalities give rise to real exchange operations without an agreement N. Irti, 'Scambi senza accordo' (1998) 1, Riv. trim. Proc. civ.,347 ss. On the other hand, do you believe that these are cases in which the dialogic dimension of the agreement is still present, but conveyed by means other than

The 'smart contracts' formula indicates programmable applications aimed at carrying out online exchanges, whose automaticity, speed, and security are guaranteed by the use of blockchain technology.[5] suitable to safeguard the correctness of the contract and to eliminate the risk of default, given the automation of the execution of the performance or services deduced in the contract, thus ensuring, in relation to the context in which they are called to operate and their functioning mechanisms, on the one hand, greater speed, safety, and efficiency of and in traffic, and on the other, fulfilling a deflationary purpose of the dispute.

The smart contracts are distinguished by the fact that they constitute scripts (i.e. codes), which dictate rules and commands, which the parties must compulsorily observe at the time of an exchange so that the transaction is carried out in an automated manner. The main feature of these contracts is that the operation can be carried out peer-to-peer, i.e., directly between two users, without the intermediation of a central control and verification entity, which, for example, establishes the exchange rates.[6]

All this is made possible thanks to the use of 'blockchain' technology (literally, 'a chain of blocks'), by means of which the inputs and outputs deriving from the contract become blocks of encrypted language, stored in a public register (the so-called ledger), which exploits the characteristics of a computer network of 'nodes' (the various participating subjects), whose data are managed and updated in a unique and secure way and cannot be distorted or modified.[7]

---

verbal language G. Oppo, *'Disumanizzazione del contratto?'* (1998) 1 Riv Dir civ., 525. He believes that the agreement is in any case present due to the behaviour of the parties, CM Bianca, Diritto civile, Vol 3. *Il contratto* (III ED Giuffré 2019), 43.

[5] The first definition is due to N. Szabo, 'Formalizing and Securing Relationships on Public Networks' (1997) 2 First Monday, 9; which states: «The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.

[6] Among the various contributions on the subject, cf. MR Maugeri, *Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law* (Il Mulino, 2021); ID, Autonomia e costruzione dello spazio digitale, in P. Perlingieri, S. Giova, I. Prisco (eds), *Il trattamento algoritmico dei dati tra etica, diritto ed economia* (ESI, 2020), 162 ss.; E. Battelli, 'Le nuove frontiere dell'automatizzazione contrattuale tra codici algoritmici e big data: gli smart contract in ambito assicurativo, bancario e finanziario' (2020) 4 Giust. civ., 681 ss.; G. Finocchiaro, Il contratto nell'era dell'intelligenza artificiale (2018) 2 Riv. trim. dir. proc. civ., 441 s.; A. M. Gambino, *Buona fede e rapporti telematici, Principi, clausole generali, argomentazione e fonti del diritto*, a cura di F. Ricci (Giuffré, 2018), 615-616; I. A. Caggiano, Il contratto nel mondo digitale, in L Gatt (ed) *Il contratto del terzo millennio. Dialogando con Guido Alpa* (Editoriale Scientifica 2018), 55 ss.; P. Cuccurru, 'Blockchain ed automazione contrattuale. Riflessioni sugli smart contracts' (2017) 1 Nuova giur. civ. comm., 107; D Di Maio EG Rinaldi, 'Blockchain e la rivoluzione legale degli Smart Contracts', [2016] www.dirittobancario.it; M.Bellini, 'Smart Contracts: che cosa sono, come funzionano, quali sono gli ambiti applicativi' [2018] in www.blockchain-innovation.it.

[7] The Blockchain platform is a distributed, shared, decentralized and encrypted database that acts as a huge public register on which a list of information is recorded. Part of the Distributed Ledger Technology (DLT), the Blockchain ensures the shared management of an archive (ledger or ledger) between different users of a network (so-called nodes). The data recorded in the ledger can be read and written by all users, but they are stored in such a way that the modification of the register is possible only after the acquisition of consent to the operation by all the other nodes in the network. This guarantees considerable resistance to external attacks, since in order to be able to modify a single part of the chain, it is necessary to obtain the 'consent' of all the other nodes. Among the main advantages of Blockchain technology is first of all the reliability of the archive, which, being managed by several nodes of a network in a decentralized manner, is less exposed to cyber-attacks. In fact, to compromise the database it would be necessary to hit all the network nodes that manage it at the same time. It follows, therefore, that the information, once registered, is irrevocable and

The non-modifiability of the data in the blockchain allows for the creation of a relationship of trust in a totally disintermediated environment between parties who, while not knowing each other at all, want to carry out financial transactions and operations.

Thus, it happens that two or more subjects who identify a common interest put in place a smart contract, providing within it clauses containing the desired conditions and effects.

Subsequently, the parties insert the smart contract into the chosen blockchain, which, in turn, becomes the guarantor of the contract and ensures that the instructions given to it are no longer modifiable.

At this point, the smart contract becomes part of a block (identified by a hash code), which is validated by the nodes, i.e., by the participants in the blockchain, who are called to give their consent. Once the latter is obtained, the block is added to the chain, immutable, and certified.

In this way, the contract acquires the ability to enforce its clauses and to have prompt and immediate execution as soon as the agreed conditions occur, without, however, the parties having to carry out checks or activate paper or manual procedures.

The smart contract, therefore, is mainly characterized by the following characteristics:

i) Irretractability, as once inserted in the blockchain, it can no longer be cancelled unless the parties have expressly provided for the kill function;

ii) Unchangeability, as once inserted in the blockchain, the smart contract can no longer be changed;

iii) Unstoppability: following its implementation, the operation of the smart contract cannot be blocked or cancelled.

Such aspects undoubtedly make the smart contract a useful tool for the purpose of ensuring the safe execution of the contract, but at the same time, as the other side of the coin, they expose the parties to the risk of the non-modifiability of what was agreed, even in the event of an agreement between them.

2. Regulation of smart contracts in the European context and in the Italian legal system.

For some time now, the European legislator has shown that it carefully monitors the developments of new technologies in an attempt to arrive at an appropriate regulation. In this direction, the Resolution of the European Parliament of October 3, 2018 on distributed ledger and blockchain technologies Within the European Union, extensive reflections and insights have been dedicated to the application implications of the blockchain and smart contracts. On this point, the work carried out by the European Parliamentary Research Service deserves mention, which highlights the need

is also completely traceable. Blockchain technology then guarantees the convenience and speed of transactions, which, being completely digitized, are performed directly between the parties without the need for third party intervention.

to start a work of integration and harmonization of contract law regulations with the new tool represented by smart contracts.

Other interesting initiatives are the establishment, by the European Commission, of the Blockchain Observatory and Forum, the 'Blockchain4EU' project, and, finally, the establishment of the European Blockchain Partnership (EBP) for the creation of blockchain-based infrastructures aimed at the provision of cross-border public services within the framework of the European Union.

Furthermore, the resolution of the European Parliament of October 3, 2018, entitled 'Distributed ledger technologies and blockchain: creating trust through disintermediation' in which, in addition to highlighting the benefits of DLT technologies in terms of strengthening trust, transparency, and security of transactions, with particular reference to smart contracts, it is underlined that 'smart contracts are an important element enabled by DLTs and can act as key drivers of decentralized applications' and, at the same time, the European Commission is invited to promote the development of technical standards at the level of relevant international organizations, such as ISO, ITU, and CEN-CELE, and to conduct an in-depth analysis of the existing legal framework in the various Member States in relation to the app In view of the digital single market, Parliament also notes that 'legal certainty can be strengthened through legal coordination or mutual recognition between Member States in the field of smart contracts'.

Finally, it is worth recalling the Ministerial Declaration of the Southern European Countries on Technologies Based on Distributed Ledgers, of 4 December 2018, signed in Brussels by the Southern European Countries belonging to the EuroMed 7 (France, Italy, Spain, Portugal, Greece, Cyprus, and Malta), which highlights the need to undertake greater close technological collaboration in order to promote the shared development of DLT technologies, in compliance with the fundamental European principles and neutrality. The declaration also reads that: 'smart contracts represent a potential turning point, capable of transforming the methods of providing services in areas such as 'the certification of the origin of products, education, transport, mobility, maritime navigation, cadastral registers, customs, company registers, and health care'.

The Italian legislator was among the very first in Europe to intervene to regulate the notions of technologies based on distributed registers and Smart Contracts by the Decree Law of 14 December 2018, n. 135, containing 'Urgent provisions on support and simplification for businesses and the public administration',[8] converted with amendments by Law 11 February 2019, n. 12.[9]

This is a particularly significant intervention since the homeland legislator was among the first at European level to regulate the two phenomena.[10]

More precisely, art. 8-ter, paragraph 1, of Legislative Decree No. 135/2018, provides a definition of technologies based on distributed registers, qualifying

[8] Published in the Official Gazette n. 290 of 14 December 2018.

[9] Published in the Official Gazette n. 36, of 12 February 2019.

[10] *See* the contributions of D. Belloni – F. Vasoli, 'Blockchain, smart contract e decreto semplificazioni, in Cammino e diritto', 15 April 2020, 8.; A. Davola, 'Blockchain and Smart Contract as a Service: market perspectives to regulatory criticalities of BaaS and SCaaS performance in the light of an uncertain legal qualification' (2020) 6 Dir. ind, 155.

them as technologies and IT protocols that use a shared, distributed, replicable, simultaneously accessible, architecturally decentralized register on a cryptographic basis, such as to allow the registration, validation, updating, and archiving of data both unencrypted and further protected by encryption verifiable by each participant, non-alterable, and non-modifiable. Art. 8-ter, paragraph 2, of Legislative Decree No. 135/2018, on the other hand, defines smart contracts as 'a computer program that operates on technologies based on distributed registers and whose execution automatically binds two or more parties on the basis of the effects predefined by them'.

Furthermore, in paragraph 3 of the same article, it is established that the memorization of an IT document through the use of the blockchain produces the legal effects of the electronic time stamp pursuant to Regulation (EU) 910/2014 (eIDAS Regulation).

The legislative intervention for the regulation and definition of the smart contract implicitly recognizes the existence of these new technologies and the operations that can take place through them, and therefore the transactions that take place through DLT and/or with the use of a smart contract are recognized by law and can acquire a certain date and probative value of private writing.

The law has mainly dealt with the definitional aspect, meagre but essential, and with the formal aspect of the blockchain and the smart contract, for which the theme specifically addressed is that of the value, precisely from a formal point of view, of the IT document stored on a blockchain.

The definition provided by the legislator in art. 18-ter, paragraph 2, of Legislative Decree No. 135/2018, seems to attribute to the smart contract the legal qualification of contract: the law indicates, in fact, that the smart contract is the source of a legal bond between the parties, taking care to define the criteria for identifying the parties to the transaction.

It is established that, following the execution of a smart contract, an automatic bond is generated between the parties ('on the basis of the effects predefined by them'). This provision, in particular, referring to 'effects predefined by the parties', suggests that there must necessarily exist a moment of formation of the agreement and, therefore, a contractual obligation, prior to the smart contract.

For these reasons, it is not entirely clear whether, in the intentions of the legislator, a smart contract is, or can be considered, a contract - understood in its classical legal meaning referred to in Art. 1321 of the Civil Code.[11]

The legislative definition has raised doubts in the part in which it refers to the smart contract as a program whose execution binds the parties, meaning that the bond arises from the execution of the program. Instead, in accordance with the consensual principle in force, it can only originate from the meeting of wills, which is the basis of the intelligent contract.

Of course, it should be noted that the execution of the contract, which derives from the previously assumed contractual obligation, has the peculiar characteristic of taking place independently of the will of the parties, but it is not the execution of the program that binds the parties; rather, the parties, in

[11] G Finocchiaro, C Bomprezzi, 'A legal analysis of the use of blockchain technology for the formation of smart legal contracts' (2020) 2, mediaLaws – Riv. di diritto dei media, 117.

exercising their private autonomy, accept that the constraint assumed by them is performed automatically and cannot be modified by the program itself.

The smart contract is a computer program that is 'executed' by processing the instructions contained within it; this automatic execution will be imposed on the parties, who will be unable to intervene. In this sense, the smart contract is understood as a way of managing a contractual agreement reached between the parties 'before and elsewhere'. In fact, in computer language, 'execution' means launching the program on the computer, which does not necessarily coincide with the complete execution of the operations envisaged in the program itself.

It is reasonable to believe that when the legislator defines the smart contract as a 'computer program (...) the execution of which automatically binds two or more parties', he uses the term 'execution' in a technical and non-juridical sense, referring to the program and not to the contract. It is, therefore, execution in the computer sense, i.e., a process by which the program is started and, therefore, executed by the device (usually a computer). In other words, once the parties have transfused the negotiating will into the algorithmic code and added the smart contract in a permanent and unchangeable manner to the Blockchain platform, the IT execution of the code will start the program, with consequent reading of the instructions uploaded by the parties for the self-execution of the services.

In the second part of Art. 8-ter of Legislative Decree No. 135/2018, the legal and probative value of a contract in written form is attributed to the IT protocol. More specifically, the rule specifies that the smart contract satisfies the requirement of the written form, provided that it proceeds to the prior IT identification of the parties through a process whose requirements are delegated to the AgId with guidelines to be adopted within ninety days from the date of entry into force of the law converting the decree. The regulation, however, does not expressly refer to national and European legislation on the formation of the electronic document—in particular, Regulation (EU) No. 919/2014, known as eIDAS, and Legislative Decree 82/2005 establishing the Digital Administration Code (CAD)—and this inevitably poses coordination problems. In the opinion of the writer, however, a reminder would have been necessary in order to avoid, especially in the application dimension of the phenomenon, the onset of interpretative doubts and application uncertainties.[12]

Indeed, it is undeniable that smart contracts fall within the concept of 'electronic document', defined by art. 3, point 35, of EU Regulation 910/2014 (the eIDAS Regulation), as 'any content stored in electronic form, in particular text, sound, visual, or audio-visual recording', whose legal validity is recognized by article 46 of the eIDAS Regulation.

In the case of DLTs, it has been observed that the legislator, by requiring their unmodifiability and immutability for the sole purpose of configurability, creates confusion between distributed registers in general and blockchains in particular, the latter's peculiar inalterability and immutability being the main and distinguishing feature of the latter and not of all DLTs. Precisely because

[12] M Giaccaglia, 'Considerazioni su Blockchain e smart contracts (oltre le criptovalute)' (2019) 3 Contratto e impresa, 956.

of these characteristics, it has been argued that, at times, intervening on the chain may be necessary to ensure the rights of the participants, such as, as we will see, the right to confidentiality, for which the definition appears excessive in its rigidity and absoluteness. Therefore, the interpreters have read the law, not in the sense of claiming the absolute inalterability and unchangeability of the chain, which is, at present, as mentioned, neither possible nor desirable, but in the sense of imposing that, for the purposes of the legal qualification of the DLTs, it must not be an identifiable (single) subject holding the power to alter or modify the register, which must be and remain a 'distributed' register.[13] This must be guaranteed not only in public and permissionless blockchains but also in private and permissioned ones.[14]

3. The debate in Italy around the nature of the smart contract and the problems related to the use of smart contracts.

Precisely in consideration of the aforementioned characteristics of modifiability and self-execution, scholars wonder whether smart contracts can be qualified as real contracts.

According to some scholars, smart contracts have the legal nature of a contract, since the computer code underlying the process would represent the transposition of the will of the parties into the language of the machine, with the consequent completion of the contract, which will therefore have the force of law between the parties (ex. art. 1372 of the Italian Civil Code) and the ability to be executed automatically.[15]

This approach would be confirmed by the definition provided by art. 18-ter, paragraph 2, of Legislative Decree No. 135/2018, since the smart contract is indicated as the source of a legal bond between the parties, to which the value of a written document is attributed, elements that would end up bringing the case in question closer to an actual contract.

Others, on the other hand, believe that smart contracts cannot be classified as contracts since they are not real agreements in themselves but, at most, 'tools' for the management of pre-existing agreements, logically prior to the smart contract. In support of the aforesaid interpretative option, the reference in the regulation to 'effects predefined by the parties', which would at least suggest the existence of a pre-existing contractual bond between the parties that the smart contract will allow to execute automatically, would serve. To believe that the computer code underlying the process has the force of law between the parties would be equivalent to stating that any error, illegal clause, or non-compliance with mandatory rules would become part of the contract. In this way, it would be an instrument that could not be controlled by the third judge.

This is also supported by the aforementioned definition, which underlines that it is the execution of the smart contract that binds the parties. According to this doctrine, the term 'execution' used in the formulation of the standard

[13] G Passagnoli, 'Ragionamento giuridico e tutele nell'intelligenza artificiale' (2019) 3 Persona e Mercato.
[14] G Finocchiaro, C Bomprezzi, (n. 11), 119.
[15] Mr Maugeri, (n 6), 162; E. Battelli, (n 6), 688.

suggests the existence of an agreement reached upstream between the parties, thus positioning the smart contract in the merely executive phase of the contractual relationship.[16]

In an intermediate position, another doctrine has observed that the qualification or not of smart contracts as contracts cannot be given in a general and abstract way but depends to a large extent on the specific characteristics assumed from time to time, without prejudice to the attitude of the smart contracts to pass the assessment of merit pursuant to art. 1322, paragraph 2, of the Italian Civil Code.[17]

One of the limitations of smart contracts is the difficulty in modifying them if the need arises, because an agreement between the parties is insufficient, and the intervention of a computer programmer who was responsible for initially preparing the 'code' of the smart contract is required.

There may also be cases of impossibility of performance for reasons not attributable to the debtor. Accordingly, the contract can only be performed in partial terms with respect to what was agreed, without a real breach occurring and without there being a concrete possibility for the parties to discuss this partial breach, in order to overcome it.

Therefore, the need arises to increase the degree of detail of smart contracts, but this would end up increasing their initial negotiation costs, with the risk of eliminating the savings obtained during the execution of the smart contract.

Therefore, it has become necessary to distinguish between 'weak' and 'strong' smart contracts to affirm that smart contracts will be able to find diffusion only with reference to less complex types of agreements.

Another problem is the possibility of non-performance and contract defects, which can happen with any sort of agreement.

Deemed necessary to facilitate as many dispute resolution mechanisms as possible by inserting clauses in the contract that leave the first attempt at resolving any dispute to the figures of mediators or allow the weaker party to withdraw from the contract when the mediator considers the weaker party's request to be founded.[18]

However, this would involve the risk of choices being made by unpredictable groups of decision-makers who lack responsibility and would not be able to lead to the correct resolution of the dispute.

To overcome the problem, it was proposed to set up a panel of mediators from which to extract the single decision-maker of the concrete case, developing the so-called 'online dispute resolution' (ODR).[19]

As regards the judicial settlement of disputes, the use of smart contracts and their diffusion, especially in contracts involving final consumers, could have a significantly deflationary effect on the work of the courts.

The trend that is establishing itself globally provides for the introduction of an arbitration clause in smart contracts. If the arbitration were robotic, the issue would be whether the arbitration process should also be managed by the

[16] IA Caggiano, 'Il contratto nel mondo digitale' (2018) 7-8 La nuova giurisprudenza civile commentata, 1154.
[17] M Giaccaglia, (n 12) 956.
[18] The problem was immediately highlighted by N. Szabo, (n 5) 12.
[19] Aj Schmitz, C. Rule, Online dispute resolutions for smart contracts [2019] J. disp. res

blockchain or whether the decisions are made by a mechanism outside the blockchain. In this regard, in Italy, a problem that arises for robotic arbitration is that relating to the validity of the award.

Italian law provides that the award must be signed by all the arbitrators. Indeed, according to art. 823 cpc the award is approved by majority vote with the participation of all the arbitrators and is therefore drawn up in writing. The provision opens with the indication of a fundamental requirement for the validity of the ruling, i.e., the presence of all the arbitrators at the deliberative moment. On this point, it should be noted that it is permissible for the arbitrators to operate separately in relation to the drafting of the justification or the written formation and signing of the award, but separate votes or votes cast outside the arbitration panel are not permitted.

A further requirement for the validity of the award pursuant to art. 823 CPC is the written form ad substantial. However, the robot arbitrator will not be able to sign, as he has no legal personality. It is also true that, given that formally the arbitrator is the manager of the program, the question could be easily resolved by having the legal representative of the manager of the robotized arbitration service sign it.[20]

4. Iranian law's implementation of smart contracts.

The procedure for establishing smart contracts in the context of a blockchain is based on factors relating to the intention and satisfaction of the participants, including the two parameters of these contracts' self-execution and their accuracy. Smart contracts' self-execution results in the conclusion of contract provisions under the direction of artificial intelligence from the start of contract negotiations to their final approval. This is accessible if the parties engaged in the signing of these contracts are identified. Ensuring the intention or eligibility of the parties can be included in the accuracy of these contracts and the accessibility of Oracle information systems during contract negotiations.[21] Contracts that are executed through the blockchain technology are known as smart contracts. This system is a distributed digital ledger that uses a computer network. Transactions concluded on this platform are recorded between the parties to be executed in a completely safe manner, and after they are finished, they are made available electronically in the blockchain area.

In smart contracts, the contract substitutes in acquisition transactions are smart assets or cryptocurrencies. The government recognizes the ownership of 'smart properties', which are assets with information stored in the form of cryptographic codes on the blockchain network.[22]

Due to the fact that Iran's legal system has not yet adopted blockchain technology, it may be stated that these contracts are concluded in the

[20] G Bonato, '*La natura e gli effetti del lodo arbitrale. Studio di diritto italiano e comparato*' [2012] , Naples.
[21] M Sadeghi – M. Nasser, 'Smart contract technology, a tool in the development of e-commerce' [2018] Requirements and policies, Tehran university, 143-167.
[22] A Wright, P De Filippi,. Decentralized blockchain technology and the rise of lex cryptographia. Available at SSRN 2580664 (2015).

electronic domain using computer instructions, and once they have been accepted, they are registered in the blockchain technology. The blockchain technology itself then serves as the final record of these contracts. Document registration in this context is regarded as document registration in the register office system since it is a centralized information system that is utilized by other systems, such as the document and real estate registration systems. Although countries are sensitive to the value of property in terms of people's property and its political nature in terms of each government's regional territory, and as a result, its transfers are subject to registration in the government real estate office, it is necessary to register these transactions in the notary office and to recognize the legitimacy of the parties involved.

The introduction of smart contracts into any country's legal system can introduce a new surface of technology into that system. A technology that can prevent many law suits and commercial real estate stability, resulting in the development of the economic system and other systems. Smart contracts are a viable alternative to traditional contracts due to their security, speed, high accuracy, and low cost. Using them helps to relieve people of the time-consuming process of registering documents with registration authorities and forms the basis for the best possible development of the registration system.

In some cases, the parties mention conditions in the contract that, despite being enforceable under their will, are in conflict with social norms and cannot be implemented. Such conditions are not possible with smart contracts, which means that these contracts are also transparent between parties given that they are governed by a system designed in accordance with specific instructions that has the ability to reread the contract or attract attention to any uncertain or invalid clauses. It is not possible for either party, or both, to intentionally or unintentionally make any clauses of the contract in this sort of contract null and void. Due to the conflict between the enforceability of these contracts and the fact that unclear, invalid, or null-and-void acts are sufficient circumstances for the impossibility of implementing the contract.

Since smart contracts and paper contracts are the same under the assimilation approach, no separate legal system is established for smart contracts, and the substantive and formal rules that govern other contracts also govern these types of contracts. The working group on electronic commerce of the United Nations Commission on International Trade Laws examined some legal concepts of electronic commerce as well as the issue of concluding a smart contract and concluded that the United Nations Convention on International Sales can be cited as the substantive law governing smart contracts.

However, in Iranian law, it is possible to demonstrate the legality and validity of smart contracts by pointing to a few civil code laws, such as articles 219[23] and 223.[24] Iran's e-commerce law, which was passed as a result of numerous changes in the nation, legalized transactions made over the Internet and

[23] Article 219 - Contracts made according to the law between the parties and their representatives are binding unless they are terminated by the consent of the parties or due to legal reasons.
[24] Article 223: 'Every transaction that has taken place is predicated on authenticity unless its corruption is known'.

through new communication technologies as well as regulated the electronic business process.

By recognizing and validating the legal status of electronic message data, Iran's e-commerce law has also accepted the principle of functional equality of message data and writing. A contract may be created and assembled virtually, but it does not need necessarily be signed there as well. The smart contract actually conforms to the general principles of the law of contracts and obligations in terms of the fundamental assumptions guiding the contract and the justification of the result.

Solving these challenges on an international level can lay the foundation for these contracts in general legal systems, and the policy-making process of concluding these contracts in accordance with the general rules for validating contracts concluded in the Iranian legal system can be adapted to the conditions of Article 190[25] of Iran's Civil Code. According to Article 190 of the Iranian Civil Code, the intention and satisfaction of the parties, their eligibility, the certainty of the transaction, and its legitimacy are the fundamental requirements for transactions. The parties to the contract, both legal and natural persons, must be eligible to conduct transactions. Therefore, bankrupt or mentally disabled people are considered ineligible. Lack of eligibility can be considered one of the defects of intention. In smart contracts, it is possible to verify the existence of eligibility and, in other words, the full intention of parties in concluding a contract by predicting the procedures for assigning digital signatures and allowing the possibility of acquiring virtual currencies. In Iran's legal system, according to Article 183 of the Civil Code, a 'contract' means that one or more persons make a commitment to one or more other persons, and it is accepted by them.

The nature of smart contracts in relation to the validity of their form and their conformity with the general rules and regulations of civil law regarding contracts is one of the new topics; knowledge and examination of the legal relations and works resulting from them are dependent on the formal structure of the electronic environment and the communication technology concepts known in this field.[26]

Smart contracts are similar to traditional contracts in many ways, but the formal structure of the electronic environment has given these contracts new features and concepts. In terms of the basic conditions of the contract and the regulation of its effects, smart contracts are subject to the general rules and regulations of the law of contracts and obligations; however, in terms of technical characteristics, methods of conclusion, and methods of protecting legal works, it necessitates their recognition and strict adherence to the general principles and rules governing contracts.

Smart contracts, in fact, do not have a different nature from conventional contracts in terms of the accuracy of the case or the subject matter, but are

[25] Article 190: The following conditions are essential for the validity of any transaction:
1) The intention of the parties and their consent
2) Eligibility of the parties
3) The specific subject to be traded
4) Legitimacy of the transaction.

[26] M Megaki Nia, 'How to conclude electronic contracts and its features' (2012) 1 Scientific and research biannual knowledge of civil rights, 85-98.

considered a new description of the contract formation environment, for which the legislator has not provided special regulations.

According to some legal experts, a smart contract is 'an agreement in which the parties' offer and acceptance are exchanged through the open international network of remote communication with audio and video tools'.[27]

Smart contracts cover a wide range of aspects of electronic transactions, including commercial or non-commercial practices as well as electronic offer and acceptance. Each of these may be a demonstration of the will and its effects in the electronic environment, such as the supply of goods and services to invite parties to conclude a contract, electronic purchase orders, electronic bank statements, and electronic payment orders.

In general, the formation of a legal relationship in the internet environment, particularly the conclusion of contracts in accordance with the principle of autonomy of the will and freedom of contracts, is not subject to special forms or formalities, as long as there is no explicit provision to the contrary in the law or the will of the parties; that is, the conclusion of contracts is based on the principle of consent. Individuals can also enter into any type of contract they want within the limitations of the law.[28]

In terms of the electronic nature of the contract conclusion environment, the subject of the contract has no distinguishing features when compared to traditional contracts. As a result, the parties to the contract have no restrictions in choosing the subject of the smart contract within the framework of the law, based on the principles of autonomy and freedom of will.

In principle, any type of property can be the main topic of a smart contract as the subject of a purchase and sale contract or the provision of services, but three items cannot be considered the subject of a smart contract, according to the implication of Article 6 of the Electronic Commerce Law. These include:

A: Real estate ownership documents

B: Sale of pharmaceuticals to final consumers

C: Announcing warnings or similar phrases that issue special orders for the use of goods or forbid the use of certain methods in the form of verbs or refraining from verbs.

According to the Iranian e-commerce law, in order to conclude a legal relationship in the electronic environment, the existence of the originator and the recipient and the exchange of message data between them are necessary. However, the term 'parties' does not include any person who acts as an intermediary in connection with the data of the message, according to clauses B and C of Article 2 of the Electronic Commerce Law.

As mentioned in the above discussions, the data of the message implies the expression of the will; it can be cited in lawsuits like other reasons, and its invalidity can also be proven through other evidence. According to Article 12 of the Electronic Commerce Law, the documents and evidence to prove the claim may be in the form of message data and may be presented in any court or government office. Based on the existing evidence rules, the probative value

[27] MM Ahmed, 'Obligations arising from the contract of subscription to the network connection services' (2020) (9(3) Academic Journal of Nawroz University, 74-93.

[28] SM Qasimzadeh, Civil Laws, Principles of Contracts and Obligations, Dadgostar Publishing House, Tehran, (2ND EDN,2005).

of the message data, one of the basic elements for the validity of the contract, cannot be simply rejected because of its shape and form.[29]

In these instances, the legislator incorporated the message data into the written ruling because, according to the cited article, whenever the existence of a writing is required by law, the message data is written in the ruling.

According to Article 190 of the Civil Code, the parties' intention is the most basic condition of contract validity and accuracy.[30] In addition to this condition, the validity of the contract requires the provision of other conditions, such as the eligibility of the parties, the determination of the subject of the contract, and the legitimacy of its purpose.

Contracts concluded by means of electronic tools, in their structural essence, are among the forms of contracts that the parties can conclude in this way with a prior agreement, but this is not legally required in any way. It is worth noting that according to Article 6 of the Electronic Commerce Law, whenever the existence of a writing is required by law, the data of the message, which according to the legal conditions is the expression of the will to be sent or received through electronic means, is written in the order.

Despite the fact that different laws generally tend to eliminate the formalities of concluding a smart contract, because the transaction is virtual and requires legal security, minimum formal conditions, such as the consumer's consent, are frequently required for the contract's conclusion in an electronic process. The provision of preliminary information and the ability to store the conditions of the contract have been imposed, and it is necessary to comply with them to conclude the contract. Based on this, the supplier must take steps to ensure that the consumer can complete the smart contract without hesitation.

There will therefore be no chance for a private agreement with the consumer to choose a different law than Iranian law as the ruling law if the chosen legislation offers less protection for the consumer than Iranian law. As a result, the destination country principle of protective jurisdiction has been approved by Iran's e-commerce law as a principle of conflict of laws in smart contracts. By reinforcing the rule of will and accepting the requirement of choosing the governing law in international smart contracts, this approach expresses the further limitation of the subjective factor of determining jurisdiction in determining the governing law in Iranian law, which is contrary to the policy of predictability of the governing law.

As a consequence, unless the parties to the contract have agreed otherwise and the chosen legislation has not offered less protection for the consumer than Iran's law, the rule is that smart consumer contracts are governed by Iranian law.

[29] Iran's e-commerce law approved in 2002. (https://dotic.ir/news/5144/)
[30] N Katouzian, *General principles of contract* Majd Publication (1996) 102-103.

5. The standards for the legality of smart contracts under Iranian law.

From the point of view of the legislator, the law of smart contracts is generally considered to apply to written contracts, except for the cases mentioned in the law, and when the contract is subject to the written form due to the law, its conclusion through electronic data will be sufficient. Of course, the signature is an important point in written contracts because it represents the parties' final will. With the creation of an electronic signature and its legal validity in smart contracts, an important flaw in the validity of electronic contracts has been removed.

In the meanwhile, using digital signatures to sign smart contracts is one of the requirements for doing so; otherwise, these contracts cannot be completed. The use of digital signatures might, of course, be considered in this context as one of the special requirements for concluding smart contracts, which need the approval of special laws to enforce their conclusion in individuals' transactions. A challenge like this is one that the Legislative Assembly in Iran's legal system should deal with. Although two simple and secure types of electronic signatures have been made public under Iran's e-commerce law, none of its provisions have mandated the usage of this kind of information.

In Iran's e-commerce law, electronic message data is recognized as a valid expression of will.[31] According to Article 2 of the Electronic Commerce Law, message data is any symbol of an event, information, or concept that is produced, sent, received, stored, or processed by electronic, optical, and new information technology devices. Therefore, electronic requests in the form of message data are created or sent according to the creator's will through the Internet or new information technologies.

In the e-commerce law of Iran, according to clause B of article 2, in the concept of electronic technologies, the term ‘originator’ is required. According to this law, the originator is the principal cause of the message data that he generates and sends, but this does not include the person who acts as an intermediary for the message data.

Acceptance in the course of concluding a contract is an expression of will that is declared in accordance with the other party's will. Acceptance, in other words, is the unconditional acceptance of the given offer to conclude a contract. Declaring consent to the requirements in the electronic environment is called ‘electronic acceptance’.

Electronic or non-electronic declaration of acceptance does not affect the nature of the will or how it implies the creation of legal relations. Electronic acceptance does not have a special status compared to traditional acceptance in the nature of the expression of will in contracts, but in terms of the form and manner of the declaration of will, a different situation can be observed in electronic acceptance. Electronic acceptance is usually achieved exclusively by clicking on the electronic expression of agreement to the terms of the electronic request provided in the Internet environment.

[31] Article 12 of Iran's e-commerce law states that documents and evidence to prove a claim may be in the form of message data, and the message data is valid for the purpose of litigation or defence.

The transmission of message data is valid, according to Article 26 of Iran's e-commerce law, when it is entered into an information system that is not under the control of the originator or his deputy. According to the provisions of this article, the message data is valid for the purpose of determining the recipient's willingness to accept when it is entered from the computer information system in a way that is out of the control of the acceptor and into the requesting information system. Some authors consider the sending and receiving of the electronic consent as concluding the electronic contract.

As long as the offeror has not stipulated a certain method of electronic notification, the electronic acceptance can be announced by any electronic method, such as by email, by filling out the form on the website page, or in the form of electronic payment of the sale price. If, despite the agreement of the parties to declare acceptance electronically, the recipient declares his acceptance through traditional mail, fax, or telephone communication, this acceptance is not considered electronic acceptance, and the declared acceptance will not be valid.

The validity of the time of conclusion of smart contracts is subject to the general rules governing contracts in civil law and usual procedures, but according to the methods of electronic communication and the special regulations that the legislator has explicitly provided in the law of electronic commerce, the time of conclusion of electronic contracts is considered upon submission. Despite the fact that the 2002 e-commerce law did not explicitly mention the time of contract conclusion, the e-commerce law requires that the validity of sending message data is dependent on the fact that this data is entered into an information system outside the control of the originator or his deputy. In terms of validity and the ability to refer to the message's data, it is important to note that the electronic commerce law considers the message's data to be a written ruling, as stated in Article 6.

According to Article 29 of the mentioned law, the Iranian legislator has determined the location of demand realization and acceptance in the smart contract. According to this article, if the location of the data transmission information system is the same as the location of the information system for receiving the same data, then the data transmission location and the data reception location are the same location, but if these two locations are different from each other, in this case, the legislator has provided three options:

A: If the parties have not agreed otherwise, the first option is that the location of the message data is the originator's business or commercial place, and the location of the message data receiving is also considered a business or commercial place.

B: The second option is that, if the originator has multiple business or commercial locations, the location closest to the original transaction is given credit for shipping; otherwise, the company's main location is considered to be the same business and commercial location.

C: The third option is that their legal residence will be the criterion if they do not have a place of business or commercial.

In drafting and approving the e-commerce law, the Iranian legislator is claimed to have paid special attention to the international aspect of smart

contracts in the field of e-commerce law. In this way, the provisions of the Electronic Commerce Law have been formulated and stipulated in accordance with the UNCITRAL Model Law's basic provisions and concepts. Of course, this is one of the rules that are expected to be established in international practice of various legal issues related to international electronic transactions, because local and domestic laws governing electronic transactions are insufficient in their international dimensions to address legal consequences arising from international law relations in this field.

The legal conditions desired by the legislator exist in Iran's e-commerce law for smart contracts, and these contracts qualify for authenticity due to the presence of reliable methods of verifying intent, because the legislator defined a secure electronic record in articles 10 and 11 of the e-commerce law of 2009.

According to Article 10, the secure electronic signature must have the following conditions:

A: Be unique to the signatory.

B: Find out the identity of the message data signer.

C: Issued by the signatory or under his exclusive will.

D: Connect to message data in such a way that any change in that message data can be recognized and discovered.

Also, according to Article 11 of the secure electronic record, 'data' is a message that is stored in accordance with the conditions of a secure information system and is accessible and understandable when necessary.

Digital signatures are a more advanced type of electronic signature, also known as encrypted electronic signatures. In terms of the security factor, it is ranked higher than other signatures and has three unique features as follows:

1. License or permit
2. Confirmation; and
3. Fraud protection.

According to Article 16 of the Electronic Commerce Law, any message data that is recorded and stored by third parties in accordance with Article 11 of this law is reliable. In addition, the existence of decentralized, independent systems can be considered the reason for the intention of their creators to conclude a transaction.

Though since Iran's e-commerce law appears to lack specific provisions for determining the governing law in smart contracts, the rules of conflict of laws contained in civil law should be applied in this regard. Some detailed safeguards have been established in articles 33 to 49 of the e-commerce law to protect consumer rights in the electronic environment. The principle is that smart consumer contracts are governed by Iranian law unless the parties to the contract agree otherwise and the chosen law does not provide less protection to the consumer than Iranian law. In the case of other smart contracts, the objective communication factor used to determine the governing law is the contract's location. As a result, determining the place of conclusion of electronic contracts is critical in determining the governing law as well as the rights and obligations of the contract's parties.

According to Article 27 of Iran's Electronic Commerce Law, the time of receiving the message data is the time when the data of the acceptance

message is entered into his information system, regardless of whether the addressee has determined the information system or not.

According to Article 28 of Iran's Electronic Commerce Law, the location of the information system should not be considered when determining the time and place of receiving message data. As a result, the location of information systems, according to Iran's e-commerce convention and law, is ineffective in determining the location and, as a result, the time of sending or receiving message data.

Accepting the electronic signature in cases where a signature is required also accepts the validity of the electronic signature, as does the fact that the documents and proofs of the lawsuit may be in the form of data messages. It compelled courts and government agencies to accept the evidentiary value of message data, and thus accepted the principle of the equality of validity of electronic evidence with other evidence in litigation.

Therefore, the data of the messages that have been created and stored in a secure way, in terms of the content and signature included in them, is considered the source of the obligations of the parties or the committed party and their legal representative, and as a result, in terms of execution and other effects, they are valid documents and can be cited in judicial and legal authorities.

Conclusions.

The adoption of smart contracts into any country's legal system can demonstrate new technological developments in legal systems, including a technology that can reduce the probability of numerous legal claims and improve transaction stability, both of which will advance the economy. However, the establishment of such structures in legal systems necessitates the supply of significant infrastructure to ensure that, once this system is put into place, it can successfully complete the specified aims. All individuals must be classified by a comprehensive system and given authorization to use one under law in order to construct this system.

Technology advancement over time has resulted in the introduction of new exchange system tools. By abandoning the traditional procedure of concluding paper contracts, these tools have led to the creation of a new space for concluding electronic contracts based on binary information, data-oriented contracts, and finally smart contracts. The newest kind of digital contracts, known as ‘smart contracts’, are made on the blockchain platform and are managed by artificial intelligence.

In order to conclude smart contracts, the parties need to obtain a license. In addition to the parties' final approval, the contracts also need the approval of artificial intelligence. Despite the similarity of smart contracts and traditional contracts in most of the governing rules, the emergence and expansion of electronic commerce have caused a new challenge in current contract law. Aside from the general ambiguity of electronic relations, the contracts made in this setting also include some legal questions and uncertainties.

The introduction of new financial instruments into the legal system of any country requires the approval of new laws in order to identify and recognize the different aspects of these instruments in the legal system. With the development of technology, developed countries have always tried to adapt their legal systems to new technologies, and in this way, they try to create new mechanisms in the legal relations of individuals in order to stabilize their property rights and their properties.

Smart contracts are viewed as a very acceptable replacement for traditional contracts because of their security, speed, high accuracy, and low cost. Due to their self-executing capabilities, transparency, and correctness, smart contracts are effective in lowering legal claims. Smart contracts prevent the occurrence of many legal and criminal lawsuits, as well as the occurrence of crimes such as financial frauds, the sale of other people's property, and the conclusion of fraudulent transactions.

These contracts reduce the costs of concluding transactions, avoid wasting time, and prevent the occurrence of some legal claims, such as the necessity of preparing official documents, enforcement of ownership, etc., because they are self-executing in relation to the implementation of the provisions of the contracts. Additionally, it stops numerous financial abuses by providing transparency features.

However, due to the unique characteristics of the electronic environment and in order to be able to assign legal actions, some minimal form requirements have been established. Smart contracts are not specifically foreseen in terms of the form of contracts, accepting the principle of the freedom of the parties to choose the form of the contract as the basis of legislation in this regard‹.

The replacement of traditional contracts with smart contracts not only saves money by reducing the costs of concluding and registering transactions but also leads to more supervision by the competent authorities over the financial transactions of individuals. The result of this is an increase in exchange security and, in other words, the stabilization of the property rights of individuals, which leads to an increase in foreign investment and the entry of countries onto the global stage in terms of transactions.

According to the materials mentioned, it was found that popularizing such contracts has many advantages and greatly increases the security and strength of transactions. This will reduce lawsuits, increase speed and accuracy in the markets, and, in general, lead to security and economic growth.

It is possible to justify the various aspects of these contracts, but in any case, the foundation of a new process in any legal system requires the approval of laws to formalize the validity of these contracts in that system and create a general obligation to oblige individuals to conclude their contracts in the form of these contracts.

The findings indicate that in the context of substantive rules, the principles of technical neutrality and functional equality are the basis for establishing laws governing smart contracts so that a person can understand that changing the constituent elements of the contract does not change the legal regime governing it, and smart contracts also have the same protections as traditional contracts. When addressing formal conditions in smart contracts, the response taken by countries and international organizations demonstrates the

acceptability of the method of removing formal restrictions. However, some formal regulations, such as the need to provide relevant information before closing a contract and the requirement of having a stable history, are still in force due to the necessity of identifying in the virtual world and establishing confidence.

Due to the special characteristics of smart contracts, developed countries have made efforts in recent years to validate these contracts. However, with the introduction of smart contracts, legal systems have decided to replace these contracts with traditional contracts.

The use of smart contracts depends on overcoming obstacles like educating the general public, defining the contract-closing procedure, resolving conflicts between national and international laws, harmonizing national and international laws to avoid conflicts, ensuring that third parties do not have access to the parties' private commercial and non-commercial information, and improving information security.

The issue of trust is the biggest concern for organizations requesting to use ‘electronic’ or ‘smart’ contracts. A person must have enough trust in the smart contract and transaction for them to be willing to send items, transfer money, or enter into binding contracts in real time. Securing that the smart contract conforms with legal standards is one challenge.

According to the mentioned materials, it was found that smart contracts have special qualities that contribute significantly to the growth of the exchange system and also popularizing such contracts has many advantages and greatly increases the security and strength of transactions. This will reduce lawsuits, increase speed and accuracy in the markets, and, in general, lead to security and economic growth.

Di Cerbo A, 'L'inquadramento giuridico dei dati perdsonali ceduti per la fruizione dei servizi digitali' (2022) 2 EJPLT, 293-304.
DOI: https://doi.org/10.57230/EJPLT222ADC

EJPLT
ISSN 2704-8012



L'inquadramento giuridico dei dati personali ceduti per la fruizione dei servizi digitali.

The legal framework of personal data transferred for the use of digital services.

ANTONELLA DI CERBO
Ph.D (c) in Private Law
Università degli Studi del Sannio

Abstract

Il contributo analizza le riflessioni dottrinali che hanno preceduto il riconoscimento della commerciabilità dei dati personali, con specifico riferimento all'individuazione della base giuridica del trattamento dei dati forniti quale controprestazione non monetaria. In particolare, nel lavoro vengono indicate le ragioni per cui è escluso che l'esecuzione di un contratto possa rappresentare una valida legal basis per legittimare il trattamento dei dati personali in oggetto, individuando nel consenso la condizione di liceità più idonea.
Le conclusioni tentano di far ordine tra le norme e gli orientamenti giurisprudenziali analizzati, riepilogando le deduzioni più significative a cui si è giunti.

The contribution analyses the doctrinal reflections that preceded the recognition of the merchantability of personal data, with specific reference on identifying the legal basis for the processing of personal data provided as nonmonetary performance. Specifically, the paper outlines the reasons why it is ruled out that the execution of a contract can not be a valid legal basis for the lawful processing of the personal data, identifying the consent as the most appropriate condition of lawfulness.
The conclusions attempt to bring order to the rules and judicial decisions analysed, summarising the most significant deductions reached.

© The author(s) 2022, 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: GDPR; Direttiva 770/2019; social network; profilazione; marketing

Summary: Introduzione. – 1. Approccio tradizionale vs Approccio negoziale. - 1.1 Approccio tradizionale. – 1.2 Approccio negoziale. – 2. La base giuridica del surplus di dati forniti dall'interessato come controprestazione non monetaria e trattati dal titolare per finalità di marketing. – 2.1. Il contratto. – 2.2. Il consenso. – 3. Consenso al trattamento dei dati personali e consenso negoziale. - Conclusioni.

Introduzione.

Le nuove tecnologie e la data driven economy, in particolare i modelli di business che si fondano sulla raccolta e sull'analisi delle attività degli utenti in rete, hanno richiesto più di un intervento comunitario che favorisse la libera circolazione dei dati personali ed al contempo assicurasse un'adeguata tutela degli interessati che si trovino nell'Unione Europea.

In tal senso, la legislazione comunitaria, attraverso il GDPR[1], il Digital Service Act [2] e il Digital Market Act [3], persegue l'obiettivo di facilitare la libera circolazione dei dati personali all'interno dell'Unione ed il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati.

Negli ultimi anni, il confronto dottrinale e giurisprudenziale in merito al contemperamento di questi interessi, almeno apparentemente contrapposti, è avvenuto mantenendo sullo sfondo il tema della commercializzazione dei dati personali e le questioni ad esso correlate.

Originariamente il trattamento dei dati si configurava come un'attività ancillare rispetto all'oggetto ed alla causa del contratto, mentre negli ultimi anni si sono diffusi a macchia d'olio schemi negoziali che prevedono la cessione dei dati personali dell'interessato a titolo di corrispettivo per la fruizione di un contenuto o di un servizio digitale.

Il merito di aver intuito le potenzialità dei dati raccolti nel contesto della fornitura dei servizi è attribuito dalla professoressa Zubuff [4] al giovane ingegnere di Alphabet Amit Patel, che per primo ha estratto valore dalle attività degli utenti registrate da Google, comprendendo come le stesse fossero un potente rilevatore del comportamento umano.

1Regolamento 2016/679/UE (GDPR) .

2 P Regolamento (UE) del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (DSA) e che modifica la Direttiva 2000/31/CE. Lobiettivo del DSA è contrastare la diffusione di contenuti illeciti e disinformativi, nonché di altri contenuti potenzialmente rischiosi, potenziando l'azione di moderazione da parte dei prestatori di servizi intermediari (social media, marketplace, ecc.). In linea generale, il Digital Services Act e il Digital Markets Act puntano complessivamente ad affermare la supremazia digitale europea ed a creare un ambiente digitale caratterizzato dal raggiungimento di una più ampia tutela dei diritti fondamentali degli utenti e dalla creazione di un 'level playing field' per le imprese.

3 Regolamento (UE) del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (DMA)

4 S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019, par.2.. Si veda anche J. BRIDLE, *The Age of Surveillance Capitalism by Shoshana Zuboff review – we are the pawns,* in The Guardian, 2019. Consultabile al sito: www.theguardian.com

Negli schemi economici che caratterizzano l'odierna economia digitale i dati hanno assunto un nuovo ruolo di mercato, divenendo un indispensabile *asset* strategico in grado di studiare le tendenze dei singoli consumatori.

Il mercato è costellato da servizi digitali per la cui attivazione è richiesta la fornitura di dati ulteriori rispetto a quelli strettamente necessari per l'esecuzione della prestazione oggetto del contratto. Si tratta di un surplus informativo, utilizzato per l'esercizio di attività correlate principalmente al marketing, da cui il titolare ricava utili e profitti.

Lo schema descritto palesa l'importante ruolo assunto dai dati personali nell'ambito degli accordi negoziali conclusi nel contesto digitale.

Queste considerazioni, unitamente alle premesse sopra accennate in merito alla tutela dei diritti fondamentali della persona ed alla necessità di prevedere una disciplina giuridica che favorisca la libera circolazione delle informazioni, hanno condotto gli studiosi della materia ad interrogarsi circa l'attitudine commerciale dei dati personali.

1. Approccio tradizionale vs Approccio negoziale.

1.1. Approccio tradizionale.

La necessità di avviare una riflessione sul tema ha portato la dottrina a dividersi tra chi sostiene che ammettere in modo chiaro la commerciabilità del dato personale significhi rendere l'interessato-consumatore maggiormente consapevole del valore dei propri dati, e chi sostiene, invece, che i dati personali rappresentino un valore assoluto intrasmissibile ed indisponibile.

Di seguito si tenterà di indicare gli argomenti a sostegno dell'approccio tradizionale che più convincono.

La dottrina che esclude l'attitudine patrimoniale dei dati personali si fonda sull'assunto secondo cui il modello europeo, in particolare l'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea, sia incompatibile con una visione proprietaria del diritto alla protezione dei dati personali. Più precipuamente, la collocazione di tale diritto all'interno della Carta di Nizza lo sottrae alla disponibilità dell'avente diritto, determinandone l'inidoneità ad essere sia oggetto di negoziazione sia di trasmissione dal titolare a un altro soggetto.

Secondo tale impostazione, l'indisponibilità del diritto alla protezione dei dati personali è disposta dal legislatore per evitare che la decisione circa la cessione dei dati sia rimessa all'interessato, in quanto questi non sarebbe in grado di comprendere, sempre e pienamente, i pregiudizi a cui si espone cedendo pezzi della propria identità digitale. A titolo esemplificativo, si rappresenta che il trattamento di dati apparentemente privi di una connotazione dettagliata della propria persona, come la quantità di km percorsi in bici su base giornaliera, potrebbe essere gravosamente pregiudizievole per l'interessato, in quanto tali attività di trattamento potrebbero essere utilizzate ai fini del calcolo di un premio assicurativo.

Considerata le implicazioni sulla sfera personale dell'individuo derivanti da un *trade – off* tra informazioni e servizi, ammettere l'utilizzo, mediante cessione, dei dati quale moneta di scambio potrebbe sminuirne l'effettivo valore, esponendo gli interessati a gravi pregiudizi.

È stato osservato[5] che, seppur non si rintracci nel GDPR un espresso divieto di monetizzazione dei dati personali, sia possibile ricavarlo da un'attenta lettura dei principi generali di cui all'articolo 5 del regolamento.

Ammettere la cessione dei dati personali significherebbe accettare una perdita di controllo sugli stessi da parte degli interessati, a detrimento della libertà di autodeterminazione informativa che la normativa in materia mira a valorizzare.

Vi è di più. Posto che, a seguito della cessione dei dati, sia difficile che l'interessato conosca le successive attività di trattamento che li abbiano ad oggetto, tale trasmissione sarebbe verosimilmente foriera di violazioni rispetto ai principi di finalità, della minimizzazione e della trasparenza del trattamento.

Inoltre, equiparare i dati personali ad un corrispettivo contrattuale comporterebbe una discrepanza fra coloro che godono di una migliore condizione economica[6] e che quindi si trovino nella possibilità di adottare scelte pienamente libere, e coloro che, riversando in condizioni economiche disagiate, siano invece portati, per necessità, a cedere i propri dati al fine di ottenere un guadagno o di fruire di un servizio.

La privacy, a questo punto, diventerebbe un diritto dei soli ricchi.

Anche le Linee Guida dello European Data Protection Board (d'ora innazi Board o Comitato) sul trattamento dei dati personali nel contesto della fornitura dei servizi online[7], registrano il medesimo approccio ove si legge: "*considerando che la protezione dei dati è un diritto fondamentale garantito dall'articolo 8 della Carta dei diritti fondamentali, e che una delle finalità principali del GDPR è quella di fornire agli interessati il controllo sulle informazioni che li riguardano, i dati personali non possono essere considerati un bene commerciabile. Anche se l'interessato può acconsentire al trattamento di dati personali, non può cedere i propri diritti fondamentali attraverso tale accordo[8]. E, ancora, nella nota[9] (posta alla fine del periodo sopra riportato) si legge: oltre al fatto che l'uso dei dati personali sia disciplinato dal GDPR, vi sono altri motivi per cui il trattamento dei dati personali si distingue concettualmente dai pagamenti*

5 A. SPATUZZI, *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali,* in Notariato, 4, 2021, 371 – 378.

6 Si veda il comunicato stampa dell'Autorità garante per la protezione dei dati personali *Si può fare commercio di dati personali? Scorza: "Consiglio di Stato boccia ricorso Facebook, ecco le questioni aperte" - Intervento di Guido Scorza* sul sito dell'Autorità, 2021
Consultabile al sito https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9569905

7 Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del GDPR nel contesto della fornitura di servizi online agli interessati - Versione 2.0 - 8 Ottobre 2019. Consultabili al sito: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_it

8 Cfr Considerando 54 della Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del GDPR nel contesto della fornitura di servizi online agli interessati - Versione 2.0 - 8 Ottobre 2019.

9 Cfr nota 30 delle Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del GDPR nel contesto della fornitura di servizi online agli interessati - Versione 2.0 - 8 Ottobre 2019.

monetari. Ad esempio, il denaro può essere contato, il che significa che è possibile confrontare i prezzi in un mercato concorrenziale e di norma i pagamenti in denaro possono essere effettuati soltanto con la partecipazione dell'interessato. Inoltre i dati personali possono essere sfruttati da più servizi contemporaneamente. Una volta perduto il controllo sui propri dati personali, non è detto che tale controllo possa essere ripristinato."

Il Board evidenzia come l'equiparazione dei dati personali ad una moneta di scambio si scontri con l'assenza di un criterio comune e condiviso di valutazione economica dei dati che consenta all'interessato di conoscere il valore che con gli stessi sarà creato.

Ancora il Comitato, nella Dichiarazione relativa all'atto sulla *governance* dei dati, adottata il 19 maggio del2021[10], afferma che "*Da un lato l'atto sulla governance dei dati dovrebbe contenere le definizioni di «dati personali», «interessato», «consenso» e «trattamento» facenti riferimento alle definizioni del regolamento generale sulla protezione dei dati; dall'altro, le definizioni dell'atto sulla governance dei dati dei termini «metadati», «titolare dei dati», «utente dei dati», «condivisione dei dati» e «altruismo dei dati» dovrebbero essere modificate per evitare incongruenze e incertezza del diritto ed essere in linea con la «natura dei diritti in questione», ossia il carattere individuale del diritto alla protezione dei dati personali come diritto di ciascuna persona e come diritto inalienabile, «al quale non è possibile rinunciare» e che non può essere reso oggetto di diritti di proprietà. A tale riguardo, il comitato si rammarica del riferimento allo «scambio, alla messa in comune o al commercio di dati» aggiunto nel testo di compromesso del Consiglio per quanto riguarda la definizione di «fornitore di servizi di condivisione dei dati», dato che, per quanto concerne i dati personali, suggerisce l'idea di legittimarne il commercio e ciò è pertanto incompatibile con il carattere personale del diritto alla protezione dei dati personali. In effetti, considerando che la protezione dei dati è un diritto fondamentale garantito dall'articolo 8 della Carta e tenendo conto del fatto che una delle finalità principali del regolamento generale sulla protezione dei dati è quella di fornire agli interessati il controllo sui dati personali che li riguardano, il comitato ribadisce che i dati personali non possono essere considerati una «merce commerciabile». Una conseguenza importante è data dal fatto che, anche se l'interessato può acconsentire al trattamento dei propri dati personali, non può rinunciare ai propri diritti fondamentali. Di conseguenza, il titolare del trattamento al quale l'interessato ha prestato il consenso al trattamento dei propri dati personali non ha diritto a «scambiare» o «commerciare» i dati personali (come una cosiddetta «merce») in un modo che determinerebbe una non conformità rispetto a tutti i principi e a tutte le norme applicabili in materia di protezione dei dati*"[11].

1.2. Approccio negoziale.

L'approccio negoziale parte dal presupposto che non esista nel GDPR una disposizione che escluda la monetizzazione del dato e che, anzi, tale normativa, pur collocandosi nel solco della Direttiva 95/46, si spinga oltre affermando in

10 Dichiarazione 05/2021 relativa all'atto sulla *governance* dei dati Consultabile al sito: https://edpb.europa.eu/system/files/2021-08/edpb_statementondga_19052021_it.pdf
11 Dichiarazione 5/2021, 51

più parti che il diritto alla protezione dei dati personali non sia una prerogativa assoluta, ma vada considerato alla luce della sua funzione sociale e contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Ciò anche sulla base della storia del processo di integrazione eurounitaria, che nasce e si sviluppa attorno al fenomeno economico. Ne risulta che qualsiasi diritto, con la sola esclusione del diritto alla vita, può essere declinato lungo la coordinata del bilanciamento di interessi[12].

Mantenere una posizione rigida che non riconosca il ruolo economico dei dati rischierebbe di tradursi in una privazione di tutela a discapito degli interessati-consumatori, in quanto escluderebbe l'operatività delle discipline consumeristica e civilistica alla cessione dei dati.

Diversamente, l'inserimento della cessione dei dati in schemi negoziali disciplinati dai codici civile e del consumo consentirebbe di sottrarre la loro regolamentazione all'arbitrio dei titolari e, al contempo, di accrescere la consapevolezza dell'utente ed il controllo che questi ha dei suoi dati, valorizzando il principio di autodeterminazione informativa.

A sostegno di una lettura in termini patrimoniali dei dati personali si colloca la Direttiva 2019/770/CE[13] recepita ad opera del d.Lgs. numero 173/21, ove l'articolo 3 paragrafo 2 recita "*La presente direttiva si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire un contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previst*i."

La Direttiva 2019/770/CE è portatrice di un approccio negoziale innovativo rispetto al trattamento dei dati personali[14].

Particolarmente utile a declinare il fenomeno in argomento è la sentenza n.2631/2021 [15] del Consiglio di Stato ha riformato parzialmente il provvedimento numero 27432[16] dell'Autorità Garante della Concorrenza e del Mercato in materia di raccolta, utilizzo e cessione a terzi, a fini commerciali, dei dati degli utenti del social network Facebook.

L'Autorità preposta alla tutela dei consumatori, partendo dall'assunto secondo cui il *business model* del gruppo di Meta si fondi sulla raccolta e sullo sfruttamento dei dati degli utenti a fini remunerativi e che tali attività

12 A. RICCI S*ulla funzione sociale del diritto alla protezione dei dati personali*, in *Contratto e impresa,* 2017, 2, 591 - 595; 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*, 2019, 108 - 111. La stessa Corte di Giustizia ha stabilito che il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale (CGUE, 9 .11.2010, cause riunite C92/09 e C-93/09, in www.curia.europa.eu) e il legislatore europeo ne ha tenuto conto per formulare il considerando n. 4 GDPR (v. Relazione alla Proposta di GDPR.

13 Direttiva 2019/770/UE. In tale contesto assume rilevanza anche la Direttiva 2019/771/UE, recepita con il D.lgs. n. 170/2021.

14 G. RESTA, Z. ZENCOVICH, V*olontà e consenso nella fruizione dei dati personali,* in *Rivista trimestrale di diritto e procedura civile*, 2018, 440-441. Consultabile al sito: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213551*

15 Cons. St., 29.03.2021., n.2631, in Italgiure Web

16 Provvedimento AGCM, 29.11.2018, n. 27432

consentano il 98% del fatturato di Facebook Inc., aveva qualificato apertamente tali dati come contro-prestazione del servizio offerto [17] e contestato le seguenti violazioni:

a) il mancato rispetto degli articoli 21 e 22 del codice del consumo, per aver tratto in inganno gli utenti attraverso pratiche commerciali scorrette che consistevano nell'aver offerto il prodotto come gratuito, senza informare gli interessati che i loro dati sarebbero stati utilizzati a fini commerciali ed impedendo loro di assumere una decisione commerciale pienamente libera;
b) il mancato rispetto degli articoli 24 e 25 del codice del consumo, che disciplinano le pratiche commerciali aggressive, mediante l'acquisizione del consenso degli utenti alla cessione dei dati a terzi. La volontà dell'utente, secondo l'Authority, sarebbe stata indebitamente condizionata in quanto preimpostata sul consenso all'integrazione tecnica tra Facebook e i siti web. Pertanto, per impedire il trattamento, l'utente avrebbe dovuto compiere un'azione positiva de-selezionando la scelta, attraverso un meccanismo di *opt-out*. Attraverso tale pratica l'utente sarebbe stato indotto a mantenere attivo il trasferimento e l'uso dei propri dati a terzi operatori, per evitare di subire limitazioni nell'utilizzo del servizio conseguenti alla de-selezione.

La contestazione di cui alla lettera a) ha trovato conferma da parte del Tar[18], che, però, ha annullato la sanzione emessa con riferimento alla pratica b) in quanto ha ritenuto non sussistenti gli elementi idonei a dimostrare la natura aggressiva della pratica commerciale.

A fronte della contestazione di cui al primo punto, sopravvissuta al vaglio del Tar, Facebook si è difesa argomentando che il provvedimento dell'Autorità parta da un assunto errato: i dati personali degli utenti, stante la loro insita indisponibilità, non possono fungere da corrispettivo della prestazione contrattuale.

Con l'intervento del Consiglio di Stato la tesi sostenuta da Facebook secondo cui la non patrimonialità del dato renderebbe inapplicabile il diritto consumeristico è stata definitivamente smontata. Secondo i giudici di Palazzo Spada *"riconoscere la assoluta specialità del settore riferibile alla tutela dei dati personali condurrebbe, inevitabilmente, ad escludere in radice, l'applicabilità di ogni altra disciplina giuridica[19],* giacché ogni comportamento umano implica il coinvolgimento dei dati personali. Ad avviso del Collegio, le disposizioni normative vanno interpretate non *"nel senso della creazione di compartimenti stagni di tutela ma della esigenza di garantire tutele multilivello che possano amplificare il livello di garanzia dei diritti delle persone fisiche, anche quando un diritto personalissimo sia sfruttato a fini commerciali, indipendentemente dalla volontà dell'interessato-utente-consumatore. È dunque imprescindibile una lettura anche in termini patrimoniali dei dati senza ignorare i rischi connessi ad una sostanziale mercificazione della persona.*

17 Provvedimento AGCM, 29.11.2018, n. 27432, punto 18
18 Tar Lazio, 10.01.2020, n.260, in Italgiure Web.
19 Cons. St., 29.03.2021., n.2631,23, in Italgiure Web.

Il Consiglio ha poi confermato la pronuncia del Tar, riconoscendo la sussistenza della violazione degli articoli 21 e 22 del codice del consumo contestata al punto a) relativa all'esercizio di pratiche commerciali scorrette da parte del social ed escludendo la configurabilità della violazione degli articoli 24 e 25 del codice del consumo di cui al punto b) del provvedimento dell'Antitrust, in quanto *la pratica per essere aggressiva necessita di un quid pluris che provochi una sorta di manipolazione concreta o anestetizzi abilmente la volontà dell'utente, non incidendo meramente e semplicemente sul suo diritto a conoscere le informazioni necessarie ad effettuare una libera e consapevole scelta, ma che si concretizzi in una condotta che sia addirittura capace di coartare il comportamento (e quindi la libertà di scelta) dell'utente*[20].

2. La base giuridica del surplus di dati forniti dall'interessato come controprestazione non monetaria e trattati dal titolare per finalità di marketing.

Posto che i modelli fondati sulla monetizzazione dei dati costituiscano una realtà nei mercati dei servizi digitali, la dottrina più attenta si sta interrogando su quale sia la base giuridica, ai sensi dell'articolo 6 del GDPR, che giustifichi il loro trattamento. In particolare i dubbi sono sorti con riferimento alla individuazione delle condizioni di liceità relative alle attività di trattamento che coinvolgono dati diversi da quelli necessari per la prestazione del servizio. È il caso, ad esempio, dei dati relativi alle esperienze di navigazione degli utenti raccolti da piattaforme social ed utilizzati per finalità di pubblicità comportamentale e personalizzazione dei contenuti.

2.1. Il contratto.

Dato il ruolo che la pubblicità comportamentale online (anche detta OBA) riveste nei principali modelli di business dei più importanti players del settore si è scelto di analizzare le policy privacy di quest'ultimi in riferimento alla legal basis individuata per tali attività di trattamento

Ne è risultato che i principali fornitori di servizi online basino le attività di OBA sull'art. 6, par.1, lett.b) del GDPR, vale a dire sulla c.d. esenzione contrattuale.

Il trattamento sarebbe qualificato dal titolare come necessario all'esecuzione del contratto di cui sia parte l'interessato o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Del resto, come ha sostenuto autorevole dottrina, la forza dirompente del nuovo regolamento è consistita nell'aver sottratto al consenso la valenza prioritaria di prima e nell'aver autorizzato la circolazione dei dati anche a prescindere da una manifestazione di volontà.[21]

20 Cons. St., 29.03.2021., n.2631, 38, in Italgiure Web.

21 D. POLETTI, Le condizioni di liceità del trattamento dei dati personali, in *Giur.it*, 2019, 12, 2785 - 2789. Al riguardo si segnala anche l'articolo di M. SENOR *La reticenza italiana sul legittimo interesse del titolare quale base giuridica del trattamento di dati personali,* in *MediaLaw*, 2018, par.1. Consultabile al sito https://www.medialaws.eu/12333-2/ in cui l'autrice sostiene che le condizioni di liceità del consenso già fossero già equivalenti ed alternative ai sensi della precedente normativa europea ma che il legislatore

Tuttavia, a ben vedere, in tale contesto l'esenzione di cui alla lett.b) dell'articolo 6 GDPR su cui poggiano la raccolta e l'analisi dei dati finalizzate alla pubblicità comportamentale è destinata ad operare in virtù di condizioni contrattuali unilateralmente imposte dal titolare.

Vista la considerevole asimmetria negoziale, l'interessato, pur di accedere ad un servizio, è verosimilemnte condizionato ad accettare che i suoi dati vengano sottoposti ad attività di profilazione ovvero ceduti in modo indiscriminato,

Né tanto meno è possibile argomentare che la necessità del trattamento riguardi genericamente l'esecuzione di un contratto in cui l'interessato si impegni ad adempiere mediante la cessione dei propri dati per attività di profilazione. Una tale lettura finirebbe per consentire un utilizzo indebito della condizione di liceità in argomento.

Come è stato opportunamente rilevato[22], tale interpretazione si pone in contrasto con quanto disposto dall'articolo 7, par.4 del GDPR secondo cui "*Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.*"

In riferimento all'individuazione della base giuridica idonea a rendere le attività di trattamento per finalità di OBA conformi all'*acquis* comunitario rileva la domanda di pronuncia pregiudiziale proposta ex articolo 267[23] del TFUE dalla Corte suprema austriaca relativamente al trattamento dei dati personali coinvolti nelle attività di pubblicità comportamentale e personalizzazione dei contenuti da parte di Facebook.

La difesa del social ha sostenuto l'applicabilità del fondamento di liceità di cui all'articolo 6 paragrafo 1, lettera b) del GDPR, per cui il trattamento sarebbe necessario per l'esecuzione del contratto, in quanto la profilazione a fini pubblicitari costituisce un pilastro fondamentale dell'accordo concluso dalle parti in causa.

Di contro, il giudice del rinvio, richiamando le Linee guida 2/2019 del Comitato europeo per la protezione dei dati personali (EDPB)[24], ha dichiarato che l'articolo 6 paragrafo 1, lettera b) del GDPR non sia una base giuridica adeguata per tracciare i profili attinenti ai gusti ed alle scelte di stile di vita degli utenti, in quanto rappresenta un trattamento che va al di là sia di quanto oggettivamente necessario per l'esecuzione di un contratto e sia di quanto l'interessato possa legittimamente aspettarsi.

La Corte austriaca ritiene che la ratio dell'articolo 6, par.1, lett.b) sia fornire una base giuridica per le attività di trattamento "*necessarie all'esecuzione del contratto*" ovvero "*all'esecuzione di misure precontrattuali"* e non per quei casi

nazionale avesse attuato in maniera piuttosto peculiare il dettato comunitario, riservando al consenso un ruolo preponderante rispetto alle altre basi giuridiche.

22 F. BRAVO, I*l commercio elettronico dei dati personali,* in T. Pasquino-A. Rizzo-M. Tescaro (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, ESI, 2020, 83-130.

23 CGUE, 24.09.2019, Causa C-446/21, in Italgiure Web.

24 EDPB - Linee guida 2/2019 sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo1, lettera b), del GDPR nel contesto della fornitura dei servizi online agli interessati.

in cui i dati personali siano l'oggetto stesso del contratto, come nei modelli di business fondati sulla monetizzazione.

Lo stesso ragionamento pare soggiacere al provvedimento emesso nel luglio del 2021 dalla Commissione nazionale lussemburghese per la protezione dei dati (CNPD) contro il gigante Amazon[25]. L'Authority, che ha comminato una multa di 746 milioni di euro, ha statuito che le attività di online behavioural advertising siano conformi alla normativa solo in presenza di un libero consenso degli utenti alla profilazione per fini pubblicitari.

Il provvedimento della Commissione è stato impugnato, si è dunque in attesa della pronuncia definitiva.

2.2 Il consenso.

Alla luce delle considerazioni appena espresse sembrerebbe che per le attività di raccolta e analisi delle informazioni comportamentali degli utenti per fini pubblicitari andrebbe preferita la base giuridica del consenso di cui all'articolo 6 paragrafo 1, della lettera a) del GDPR, come disciplinato dall'articolo 7 del Regolamento generale e dalle linee guida in materia di consenso al trattamento dei dati personali numero 5 del 2020[26] adottate dall'*European Data Protection Board.*

Il principio di *accountability*, che permea l'intero impianto della disciplina europea in materia di protezione dei dati personali, pone *l'onus probandi* in merito all'acquisizione del consenso sul titolare del trattamento, a cui è chiesto anche di dimostrare il consenso raccolto sia informato, quindi di aver messo a disposizione dell'interessato tutte le informazioni idonee a permettergli di comprendere la portata del trattamento dei suoi dati. A tal proposito, l'articolo 13 del GDPR dispone che l'interessato dovrebbe essere almeno edotto dell'identità del titolare, delle finalità a cui sono destinati i dati personali trattati, della tipologia dei dati raccolti e del diritto di revocare il consenso. Si tratta di un nucleo informativo minimo che, in linea con il principio di autodeterminazione informativa, si ritiene consenta all'interessato di esercitare un effettivo controllo sulle attività di trattamento che abbiano ad oggetto i propri dati.

Appurato che il consenso ricopra un ruolo ineludibile nelle dinamiche negoziali appena descritte, bisognerebbe verificarne la genuinità nei casi in cui lo stesso rappresenti lo strumento di pagamento dei servizi digitali.

---

25 Al momento il provvedimento della CNPD non è stato ancora reso pubblico. Invero, la comunicazione della sanzione è stata data dalla stessa Amazon in quanto la normativa nazionale sulla protezione dei dati vincola il CNPD al segreto professionale e gli impedisce di commentare casi individuali. Inoltre, la piena e chiara pubblicazione delle decisioni del CNPD è considerata sanzione supplementare. Pertanto, non può pubblicare alcuna decisione prima della scadenza dei termini per i ricorsi. La CNPD si è limitata a confermare che il 15 luglio 2021 il suo Collegio ha emesso una decisione in merito ad Amazon Europe Core S.à rl nell'ambito del meccanismo di cooperazione e coerenza europeo previsto dall'articolo 60 del GDPR. Quest'ultima dichiarazione è Consultabile al sito: https://cnpd.public.lu/en/actualites/international/2021/08/decision-amazon-2.html

26 Linee guida 5/2020 sul consenso ai sensi del Regolamento 2016/679/UE (GDPR)

Al riguardo risulta dirimente la sentenza numero 17278/2018[27] della Prima sezione della Corte di Cassazione relativa all'invio di e-mail pubblicitarie ove si legge che "i*n tema di consenso al trattamento dei dati personali, l'articolo 23 del codice della privacy[28], nello stabilire che il consenso sia validamente prestato solo se espresso liberamente e specificatamente in riferimento ad un trattamento chiaramente individuato, consente al gestore di un sito internet, il quale somministri un servizio fungibile, cui l'utente possa rinunciare senza gravoso sacrificio, di condizionare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie, sempre che il consenso sia singolarmente ed inequivocabilmente prestato in riferimento a tale effetto, il che comporta altresì la necessità, almeno, dell'indicazione dei settori merceologici dei servizi i cui messaggi saranno riferiti*". E ancora, "*Nulla impedisce al gestore del sito - beninteso, si ripete, in un caso come quello in questione, concernente un servizio né infungibile, né irrinunciabile - di negare il servizio offerto a chi non si presti a ricevere messaggi promozionali, mentre ciò che gli è interdetto è di utilizzare i dati personali per somministrare informazioni pubblicitarie a colui che non abbia effettivamente manifestato la volontà di riceverli. Insomma, l'ordinamento non vieta lo scambio di dati personali, ma esige tuttavia che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato*".

La Corte pone particolare enfasi sulla fungibilità del servizio offerto. Secondo l'interpretazione dei giudici della cassazione, l'ordinamento non vieta tout court lo scambio di dati personali ma esige che tale scambio sia frutto di un consenso pieno ed in nessun modo forzato, la qual cosa accadrebbe se il servizio fosse infungibile ed irrinunciabile per l'interessato.

Nella stessa sentenza, la Corte afferma che "*non v'è dubbio, allora, che, nel suo complesso la previsione di un consenso in tal modo «rafforzato» sia dettato dall'esigenza di rimediare alla intrinseca situazione di debolezza dell'interessato, sia sotto il profilo della evidente «asimmetria informativa», sia dal versante della tutela contro possibili tecniche commerciali aggressive o suggestive. La normativa in questione, dunque, sorge dall'esigenza di affrontare i rischi per la persona posti dal trattamento in massa dei dati personali, così come reso possibile dall'evoluzione tecnologica. Può dunque dirsi che il consenso in questione debba essere ricondotto alla nozione di "consenso informato", nozione ampiamente impiegata in taluni settori — basti menzionare il campo delle prestazioni sanitarie — in cui è particolarmente avvertita l'esigenza di tutelare la pienezza del consenso, in vista dell'esplicazione del diritto di autodeterminazione dell'interessato, attraverso la previsione di obblighi di informazione contemplati in favore della parte ritenuta più debole*".

3. Consenso al trattamento dei dati personali e consenso negoziale.

Il consenso al trattamento dei dati personali va tenuto distinto dal consenso negoziale disciplinato dalle norme del codice civile, ancorchè entrambi siano

27 Cass. Civ.,11.05.2018, n. 17278, in Italgiure Web.
28 Articolo abrogato dall' art. 27, comma 1, lett. a), n. 2), D.Lgs. 10 agosto 2018, n. 101, che ha abrogato l'intero Titolo III.

funzionali a plasmare un assetto idoneo a tutelare i piani d'interesse di entrambe le parti[29].

Una lettura minimale che sovrapponga i due consensi non offre motivi sufficienti per spiegare la stessa ragion d'essere delle norme europee in materia di consenso al trattamento dei dati personali, in particolare dell'articolo 7 del GDPR rubricato condizioni per il consenso.

Inoltre, si fa notare che il legislatore comune in riferimento al consenso al trattamento dei dati personali non discorre di un generico consenso ma di un consenso libero e granulare, espresso dall'interessato dopo che siano state offerte le informazioni elencate negli articoli 12 e 13 del GDPR ovvero nell'articolo 14 del GDPR, qualora i dati non siano stati raccolti presso l'interessato.

A tali argomenti, si aggiunga la circostanza per cui il consenso privacy non risulti idoneo a giustificare un negozio viziato ai sensi dell'articolo 1321 del codice civile, configurandosi il primo esclusivamente come un'autorizzazione integrativa che, in quanto tale, non giustifica comportamenti illegittimi ma si limita a rendere concretamente esercitabili attività lecite, interdette da limiti posti a protezione dell'interessato[30]. Per tali ragioni qualora l'interessato revochi il consenso e quindi priviil trattamento della condizione di liceità su cui si regge, il negozio giuridico sarebbe valido ma inefficace.

Conclusioni.

Dai provvedimenti amministrativi e giurisprudenziali riportati si ricava una visione pressoché unanime circa la necessità di riconoscere ed inquadrare giuridicamente le attività di monetizzazione dei dati personali.

Gli attuali schemi negoziali necessitano di una regolamentazione dall'alto, espressamente disciplinata da norme codicistiche e sottratta all'autoregolamentazione dei titolari del trattamento, che, forti di un potere contrattuale squilibrato a loro favore, impongano condizioni particolarmente sfavorevoli per l'interessato e da questo, spesso, non comprese.

Il breve excurs relativo al tema in argomento porta altresì ad escludere che le attività di trattamento di OBA mediante profilazione possano prescindere dal ricorso ad una condizione di liceità del trattamento diversa dal consenso libero, specifico, informato e sempre revocabile, dell'interessato. La validità di quest'ultimo dovrebbe essere valutata caso per caso, tenendo in considerazione il dettato della Suprema Corte in tema di fungibilità e rinunciabilità del servizio ricevuto dall'utente in cambio dei suoi dati personali. Invero, i criteri elaborati dalla Corte, ad oggi, sono l'unico strumento ermeneutico utile ad armonizzare il dettato del regolamento generale, in particolare il paragrafo 4 dell'articolo 7, con la cessione dei dati a titolo di controprestazione contrattuale.

29 A. SPATUZZI, *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali,* in *Notariato*, 4, 2021, 375 - 376.

30 A. SPATUZZI, *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali*, cit. 375 - 376.

Ribezzo F, 'Le nuove vie della giuridificazione del corpo' (2022) 2 EJPLT, 305-312.
DOI: https://doi.org/10.57230/EJPLT222FR

EJPLT
ISSN 2704-8012



Le nuove vie della giuridificazione del corpo.

The new ways of body juridification.

FRANCESCO RIBEZZO
Ph.D. (c) Università degli Studi di Bari Aldo Moro

Abstract

This paper aims to analyze the relationship between the law and the body from a legal and philosophical perspective. The presupposition of the following remarks is that the technological development is the defining feature of the modern societies. This phenomenon has relevant implications on the languages describing the body and its disposability. The enigma of the body, which has always concerned the philosophical thought, is nowadays of great importance, since it is a privileged position from which to look at the modernity.
The law, that has always taken the corporeity into account, is concerned with the emersion of the digital persona, which now more than ever calls for appropriate protection. The investigated matter recalls the distinction between personality rights and property rights. The existential situations can be subject of agreements that entail a non-contractual nature. Yet, market-alienability and non-patrimonial interest get to be strictly entangled in the case of contracts regulating aspects of one's identity, in which case existential components remain.

Questo elaborato intende analizzare la relazione tra diritto e corpo da una prospettiva giuridico-filosofica. Premessa delle seguenti riflessioni è che lo sviluppo tecnologico sia il carattere precipuo delle società moderne. Questo fenomeno ha implicazioni rilevanti sui linguaggi descrittivi del corpo e sugli atti di disposizione del corpo. L'enigma della corporeità, che ha da sempre interessato la riflessione filosofica, ha oggi importanza primaria, rappresentando un punto prospettivo privilegiato dal quale analizzare la modernità.
Il diritto, che ha sempre disciplinato il corpo, è posto dinanzi all'emersione della digital persona, la quale richiede oggi l'approntamento di un adeguato sistema di tutele. La materia in esame richiama la distinzione tradizionale tra diritti della personalità e diritti di proprietà. Le situazioni esistenziali possono formare oggetto di accordi di natura non contrattuale. Purtuttavia logiche di mercato e interessi non patrimoniali convivono nel caso dei contratti aventi ad oggetto l'utilizzo di segni distintivi, nei quali permane una componente esistenziale.

© The author(s) 2022, 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/

Parole-chiave: corpo; corporeità; digital persona; sviluppo tecnologico; situazioni esistenziali.

Sommario: Introduzione: il progresso tecnologico come carattere della società moderna. – 1. L'enigma della corporeità. – 2. L'antica relazione tra diritto e corpo. L'avvento della *digital persona*. – 3. Corpo, diritti soggettivi e situazioni esistenziali. – Conclusioni: Il corpo e il mercato.

Introduzione: Il progresso tecnologico come carattere della società moderna.

Il progredire delle tecnologie è un fenomeno descrittivo della società del nuovo millennio, fattore determinante dello stato della condizione umana[1]. Esso è divenuto in breve tempo il «campo semantico in cui si incrociano e si intrecciano le diverse discipline»[2], il che rende ancor più complesso fornirne una definizione esaustiva. Tale condizione si riverbera sui linguaggi che costituiscono il corpo. Non esiste, difatti, perfetta sovrapponibilità tra il corpo della medicina e il corpo giuridificato, né tra il corpo oggetto degli studi biologici e quello della filosofia[3].

È oggi possibile operare una costruzione personale del corpo, per renderlo «oggetto transitorio e manipolabile, suscettibile di molteplici metamorfosi secondo i desideri individuali»[4]. Un tempo si reputava che l'istituto proprietario avrebbe rappresentato l'ambito di distinzione privilegiato tra gli individui[5]. Oggi, invece, le nuove tecnologie hanno conferito centralità alla relazione tra l'uomo e il proprio corpo, tanto che «la descrizione dell'epoca odierna può essere configurata alla stregua di un campo di battaglia avente ad oggetto il corpo umano, con le sue innumerevoli applicazioni tecniche e scientifiche»[6].

Le possibilità della sperimentazione investono in maniera totale l'ambito della disponibilità corporea[7] e sollevano sempre nuovi interrogativi di carattere

[1] M. G. SALARIS, *Corpo umano e diritto civile*, Milano, 2007, 1.
[2] S. ROSSI, *Corpo (atti di disposizione sul)*, in *Digesto delle discipline privatistiche* (*Sez. Civ.*), Torino, 2012, 221.
[3] «Il che rende tale concetto irriducibile ad una dimensione unitaria e monologante», S. ROSSI, *Corpo*, cit., pag. 221; E. RESTA, *Diritto vivente*, Roma-Bari, 2008, 45 ss.: «il corpo rimane campo semantico largo e incoercibile forse perché vive di con-fini e non sopporta tanto facilmente definizioni; è investito da con-notazioni piuttosto che da de-notazioni». Ancora, M. TALLACHINI, *Bodyright. Corpo biotecnologico e diritto*, in *Biblioteca della libertà*, 1998, XXXIII, pag. 21, afferma che «il corpo umano è ormai la pagina su cui più profondamente è incisa la parabola di una modernità che, muovendo dalla tecnologia come strumento per plasmare il mondo, approda alla tecnologia per l'automutazione». A dimostrazione della molteplicità degli interrogativi si rinvia a S. RODOTÀ, *Ipotesi sul corpo giuridifcato*, in Aa. Vv., *Tecnologie e diritti*, Bologna, 1995, 191.
[4] D. LE BRETON, *Signes d'identité: tatouages, piercing et autres marques corporelles*, Paris, 2002, 7. Di «automutazione» discorre M. TALLACHINI, *Bodyright. Corpo biotecnologico e diritto*, cit., 21.
[5] S. RODOTÀ, *Ipotesi sul corpo giuridifcato*, cit., pag. 125.
[6] M. G. SALARIS, *Corpo umano e diritto civile*, cit., pagg. 1 e 2; A. SANTOSUSSO, *Corpo e libertà. Una storia tra scienza e diritto*, Milano, 2001, 9.
[7] Così M. G. SALARIS, *Corpo umano e diritto civile*, cit., 2: «le novità dei trapianti provenienti da organi non umani geneticamente modificati, gli interventi sulle cellule staminali, i procedimenti di fecondazione artificiale, la clonazione – tanto per riferirci ad esempi limitati – prospettano problematiche differenti tra loro, ma tutte accomunate da una emergente esigenza: la conservazione dell'identità individuale»; P. D'ADDINO SERRAVALLE, *Atti di disposizione del corpo e tutela della persona umana*, Napoli, 1983, *passim*. Per R. ESPOSITO, *Bìos. Biopolitica e filosofia*, Torino, 2004, 4 – 5, «il corpo umano appare sempre più sfidato, e anche letteralmente attraversato, dalla tecnica», tanto che «il rapporto a due tra *bìos* e *zoé* deve ormai, o forse da sempre, includere, come terzo termine correlato, la *téchne* […]». Utili riferimenti nella raccolta di CH. GEYER, *Biopolitik: Die Positionen*, Frankfurt am Main, 2001.

bioetico[8]. L'evoluzione (*rectius*, rivoluzione) scientifica ha investito «le basi elementari della natura vivente, i confini dell'individualità biologica umana (nascita e morte) e il loro stesso significato»[9]. Gli avanzamenti della biomedicina e delle biotecnologie, le ampie possibilità di azione sul corpo umano e su parti, prodotti e funzioni del medesimo, «sottratti al limite dell'unità della struttura corporea[10] e dell'inalterabilità dei processi naturali»[11], hanno condotto a una diversa considerazione del corpo umano e del potere dei privati di disporne. Si fa strada, anche in ambito giuridico, l'idea per la quale il corpo non è più (e soltanto) incarnazione dell'Io[12], ben potendo costituire fonte di nuove utilità, anche di natura economica[13].

L'esperienza giuridica risulta investita da cambiamenti repentini, tant'è che categorie tradizionali, come il concetto di persona, di autonomia individuale, il rapporto delle azioni umani nel tempo e nello spazio, risultano interessate da un «effetto di spiazzamento e di riformulazione», che sembra quasi richiedere un nuovo diritto[14]. La presenza nello spazio e nel tempo dell'umano appare completamente rinnovata nel senso dell'«eccedenza del campo della vita»[15].

Il corpo «potenziato» viene proiettato in spazi temporali al confine con l'immortalità[16]. Esso è interessato da un processo di scomposizione nella dimensione spaziale e nel tempo, con la diffusione di banche ove sono depositate parti ovvero prodotti del corpo (gameti, sangue, cellule, tessuti) per una possibile futura utilizzazione[17]. La smaterializzazione del corpo preannuncia una dimensione sempre più *cyborg*. In sintesi, lo statuto del corpo

---

[8] «Nella letteratura angloamericana è ormai molto diffusa l'espressione "*enhancement*", traducibile con "potenziamento" o "miglioramento". Un termine che ancora non è entrato nel linguaggio abituale della bioetica, ma che sta aprendo un nuovo articolato capitolo dell'etica applicata. L'*enhancement* include svariate modalità di intervento sull'uomo, il cui minimo comune denominatore è l'alterazione – moderata o estrema – del corpo e della mente, finalizzata al perfezionamento della salute e della vita», L. PALAZZINI, *Il potenziamento umano. Tecnoscienza, etica e diritto*, Torino, 2015, IX.

[9] A. D'ALOIA, *Norme, giustizia, diritti nel tempo delle bio-tecnologie: note introduttive*, in ID., *Bio-tecnologie e valori costituzionali. Il contributo della giustizia costituzionale*, Atti del Seminario di Parma svoltosi il 19 marzo 2004, Torino, 2005, XII.

[10] Per F. MACIOCE, *Il corpo. Prospettive di filosofia del diritto*, Roma, 2002, la corporeità si presenta oggi soprattutto «come problema, per la stessa difficoltà di inquadrarla in un concetto unitario ed univoco»; cfr. altresì S. RODOTÀ, *Ipotesi sul corpo giuridificato*, cit., 191.

[11] P. D'ADDINO SERRAVALLE, *Biotecnologie e disposizione delle c.dd. parti staccate del corpo*, in Aa. Vv., *Il diritto civile oggi. Compiti scientifici e didattici del civilista. Atti SISDiC*, Napoli, 2006, 397.

[12] H. KUHSE, *Il corpo come proprietà. Ragioni di scambio e valori etici*, in S. RODOTÀ, *Questioni di bioetica*, Roma-Bari, 1997, 70: «se il mio corpo è l'incarnazione del mio Io, la continuità fisica è necessaria all'identità individuale». L'Autrice (*ibid.*, pag. 66) sottolinea che «la novità oggi non consiste nel fatto che il corpo umano o parti di esso sia apprezzato dagli altri (e talvolta abbia un prezzo), quanto piuttosto nel fatto che abbia molti nuovi impieghi: il rene, ad esempio, poteva avere valore in alcuni rituali religiosi dell'antichità; ora invece ha un valore diverso e decisamente più concreto: è mezzo per migliorare la qualità della vita del sofferente o addirittura per garantirgli la sopravvivenza. Le parti del corpo, inoltre, non sono preziose solamente nella medicina clinica, ma nella ricerca e nella sperimentazione e spesso nella produzione di prodotti farmaceutici e per molti altri scopi».

[13] «Tanto nella sua totalità ed in relazione ad alcune funzioni [funzione procreativa e gestazione per conto altrui] divenute "alienabili", quanto nelle singole parti e nei prodotti dei processi naturali, isolabili ed utilizzabili per il conseguimento di scopi pratici del soggetto o di terzi», P. D'ADDINO SERRAVALLE, *Biotecnologie*, cit., 397.

[14] A. D'ALOIA, *Norme, giustizia, diritti*, cit., XII.

[15] S. ROSSI, *Corpo*, cit., pag. 222.

[16] S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 318.

[17] Di «corpo permanentemente incompiuto» discorre S. RODOTÀ, *Il corpo giuridificato*, in S. Rodotà, P. Zatti (diretto da), *Trattato di Biodiritto*, I, *Il governo del corpo*, Milano, 63 ss.

appare dunque oggi un *limen*, la soglia della differenza (e dell'indifferenza) tra volontà e identità.

1. L'enigma della corporeità.

Il corpo è l'enigma che ognuno reca con sé[18]. Ogni uomo vive il paradosso della propria relazione con esso[19]. Siamo un corpo «ma non siamo solo un corpo»[20]. Si spiega allora come la conoscenza della corporeità abbia da sempre interessato il pensiero filosofico. Visioni della corporeità e concezioni sul rapporto esistente tra anima e corpo da sempre si susseguono nella storia del pensiero occidentale.

Ciò emerge in maniera evidente, ad esempio, in alcune discorsi connessi all'*eros*. È, questo, il caso di Hegel, il quale sottolinea che il fenomeno del pudore nasce nei riguardi di un corpo che si presenta *per sé*[21], come diversità che resta a sé stante. L'uomo sa di essere un corpo ma al contempo è consapevole di non poter essere ridotto a quest'unica dimensione.

Le plurime categorizzazioni prodotte dalla riflessione filosofica, pur con il rischio di una eccessiva semplificazione, possono essere ricondotte a due impostazioni fondamentali: un modello di tipo monista ed un modello dualista[22].

Al secondo insieme si ascrivono, tradizionalmente, la concezione platonica e cartesiana della corporeità, assertive di una radicale separazione tra anima e corpo[23]. Il modello monista risulta maggiormente differenziato al suo interno, potendo condurre ai due opposti esiti del materialismo e del riduzionismo psichico[24]. A prescindere dalle diverse elaborazioni, parrebbe qui ferma la negazione di una differenza ontologica tra anima e corpo.

---

[18] F. D'AGOSTINO, *Bioetica*, Torino, 1998, 124; U. GALIMBERTI, F. BOSIO, G. M. TOTOLONE, G. CUCINATO, R. CRISTIAN, *Del corpo*, in *Il pensiero rivista di filosofia*, diretta da L. LUGARINI, II, 1996, *passim*.; E. SGRECCIA, *Manuale di bioetica*, I, Milano, 1988, 123 ss.; M. SALES, *Il mistero del corpo*, in *Communio*, LIV,1980, 29.

[19] «In effetti, che il corpo sia un che di enigmatico può sembrare strano: niente è più *mio* del mio corpo, e di nulla siamo abituati a considerarci "signori per natura" più che del corpo, anzi esso è ciò con cui immediatamente ci identifichiamo e attraverso cui identifichiamo gli altri […]. Ed è tanto stretto questo legame identitario, questo nesso di identificazione, che spesso può essere fonte di disagio e sofferenza» e «l'ordinamento, nel ridurre la nostra inconfondibile identità a ciò che viene attestato sulla base di elementi formali ed empirici (fotografia, impronte digitali, DNA), non fa che confermare quanto appena detto: per il diritto siamo, almeno in una certa misura, il nostro corpo», F. MACIOCE, *Il corpo. Prospettive di filosofia del diritto*, Roma, 2002, 15.

[20] F. MACIOCE, *Il corpo*, cit., pag. 16. F. D'AGOSTINO, *Introduzione ad una bioetica del corpo umano*, in Id., *Bioetica nella prospettiva della filosofia del diritto*, Torino, 1996, 109 ss.

[21] G. W. F. HEGEL, *Scritti teologici giovanili*, Napoli, 1972, *passim*. «Il pudore nasce quando l'altro che mi sta di fronte prende l'esteriorità del mio io come se questa esaurisse tutto me stesso, come se io non fossi altro che ciò che può essere preso e osservato, nasce da uno sguardo che riducendo il mio essere al mio essere-corporeo mi rende oggetto tra gli oggetti, mi priva della dimensione che mi caratterizza nel modo più vero», F. MACIOCE, *Il corpo*, cit., pagg. 16 – 17, il quale cita, a sua volta, V. MELCHIORRE, *Corpo e persona*, Genova, 1987, 46.

[22] E. SGRECCIA, *Manuale di bioetica*, Milano, 1988, 85; E. RUNGGALDIER, *Leib – Seele Verhältnis*, in *Lexicon der Bioethik*, Gütersloh, 1998, 577 ss.

[23] Per gli esponenti di questa linea interpretativa «il problema è – almeno da Cartesio in poi – quello di stabilire il fondamento e le condizioni della corrispondenza tra i processi mentali e quelli fisici», F. MACIOCE, *Il corpo*, cit., pag. 19; N. ABBAGNANO, *Corpo*, in *Dizionario di Filosofia*, Torino, 1964, 172.

[24] «Si pensi, solo per fare un esempio, alle dottrine – quali quella di Berkeley – che pur non negando la realtà e la materia negano che essa abbia una consistenza ontologica a prescindere dalla percezione, dall'idea e dal pensiero. Non solo, ma si pensi anche alla posizione leibniziana, che riduce la sostanza corporea a quella

L'importanza di questa ulteriore considerazione si comprende già solo rammentando come i punti prospettici privilegiati da cui guardare al XX secolo sono stati la tecnologia e il corpo[25]. L'ampiezza della questione inevitabilmente impone una limitazione della prospettiva d'analisi, la quale condiziona il metodo adottato. Difatti, è sempre possibile discutere per o contro il corpo, ma con il rischio di smarrire l'«uomo»[26].

2. L'antica relazione tra diritto e corpo. L'avvento della digital persona.

L'attenzione del diritto per il corpo è antica. È lecito affermare che la disciplina giuridica del corpo e delle sue parti è precedente all'instaurazione di un fitto legame tra scienza e diritto. Il riferimento alla persona implica necessariamente la sua considerazione in termini di soggetto e oggetto della disciplina giuridica[27]. Mutato risulta, tuttavia, lo scenario nel quale ha avuto luogo il passaggio «dall'individuo alla persona» [28], rendendo difficoltosa l'individuazione di un unico concetto di corpo[29].

Le attuali relazioni sociali non sono più vincolate alla «fisicità» mentre il corpo «elettronico» ritaglia per sé sempre maggiore spazio nelle pratiche quotidiane. Per tale ragione, come è stato acutamente osservato, il riconoscimento della rilevanza della persona sarebbe incompleto allorché si trascurasse la dimensione del «corpo elettronico» [30], espressione con cui è possibile intendere, al contempo, l'insieme di dati ed il sistema informativo in cui si colloca la persona. La *digital person* necessita vieppiù di adeguata tutela, giacché chiama in causa il nesso che astringe identità, integrità e dignità umana[31].

I dati elettronici costituiscono la base di tutti i sistemi economici, sono oggetto di scambio, rendono talora impossibile distinguere dimensione

---

spirituale, vedendo nel corpo un insieme di monadi, un aggregato di sostanze – e quindi non sostanza in sé – riunite intorno ad un'entelechia dominante, l'anima; o a quella bergsoniana, che nega realtà propria al corpo riducendolo a uno strumento della percezione, rispetto al quale la coscienza è indipendente. Si può parlare di concezione monistica, tuttavia, in un senso ancora differente, e con riguardo all'elaborazione spinoziana, nella quale corpo e anima sono de-sostanzializzati perché intesi come attributi di un'unica sostanza, o ancora, ma in modo molto impreciso e vago, a proposito del pensiero fenomenologico e tipicamente husserliano, con la nota distinzione […] tra *Leib* (corpo-che-sono) e *Körper* (corpo-che-ho)», F. MACIOCE, *Il corpo*, cit., pag. 21.

[25] S. SPINSANTI, *Il corpo nella cultura contemporanea*, Brescia, 1983, 5. Per F. MACIOCE, cit., 18, il culto del corpo rappresenta «l'ideologia ecumenica della modernità».

[26] F. CHIRPAZ, *Le corps*, Paris, 1963, 2: «*on peut, en effet, discuter pour ou contre le corps, pour ou contre la valeur qu'on lui reconnaîtra. Et pourtant, qu'en est-il de l'*homme*?*».

[27] S. RODOTÀ, *Il corpo giuridificato*, cit., 51: «qualsiasi insieme di norme volto a regolare l'organizzazione sociale si occupa variamente del corpo. E l'ovvietà deriva dal fatto che il riferimento alla persona, soggetto e oggetto della disciplina giuridica, inevitabilmente porta con sé la considerazione della sua corporeità». L'Autore fa presente che «il corpo, dunque, entra nella dimensione giuridica in modo drammatico, la sua giuridificazione racconta storie di punizione, subordinazione, discriminazione» (pag. 52). La disciplina giuridica del corpo nasce in un tempo in cui il legame tra diritto e scienza era ben differente. Si rinvia, senza pretesa di esaustività, a G. CRICENTI, *I diritti sul corpo*, Napoli, 2008, pag. 16; M. M. MARZANO PARISOLI, *Il corpo tra diritto e diritti*, in *Materiali per una storia della cultura giuridica europea*, II, 1999, *passim*.

[28] A. MUSTO, *Sul trattato di biodiritto a cura di Stefano Rodotà e Paolo Zatti*, in *Persona e Mercato*, 235.

[29] S. RODOTÀ, *La vita e le regole, tra diritto e non diritto*, Milano, 2006, 72.

[30] La notazione è di S. RODOTÀ, *Dal soggetto alla persona*, Napoli, 2007, 35.

[31] P. ZATTI, *Principi e forme del "governo del corpo"*, in *Il governo del corpo*, cit., 63.

personale, sociale e consumeristica[32]. Il richiamato fenomeno ha rilevanti ripercussioni sulla possibilità di esteriorizzazione dell'identità personale[33], astretta in un processo di moltiplicazione infinita[34], con il rischio che la persona fisica venga a coincidere con la mera sintesi dei propri dati[35].

V'è chi auspica la nascita di una «nuova antropologia»[36], capace di scomporre (e ri-comporre) la persona in un complesso di dati, nella quale la *natural person* diviene una *digital person*. Ma è evidente, per quanto sinora detto, che non si tratta soltanto di un mutamento culturale. È in gioco una radicale trasformazione del paradigma della naturalità[37], la cui antica immodificabilità non richiedeva in passato un'apposita disciplina legislativa.

A fronte del superamento delle leggi naturali si pone oggi un dilemma: è sufficiente la regola scientifica o è comunque necessaria la norma giuridica[38]? L'opinione pressoché concorde in dottrina propende per un diritto strutturato in termini di *soft law*, come diritto "mite", ritenuto strumento più efficace nel contrasto al dominio della tecnica[39].

3. Corpo, diritti soggettivi e situazioni esistenziali.

La possibilità di considerare il corpo umano alla stregua di oggetto di diritti soggettivi ha tradizionalmente interessato la teoria dei diritti della personalità[40]. Ai sensi dell'art. 810 c.c. si definiscono beni «le cose che possono formare oggetto di diritti». Per quanto i termini «cose» e «diritti» non si esauriscano, rispettivamente, nelle cose corporali[41] e nel diritto esclusivo di proprietà, la citata definizione «sembra mal conciliarsi con la possibilità di

---

[32] A. ALPINI, *La trasformazione digitale nella formazione del civilista*, 7.

[33] «Alla locuzione "identità personale" possono essere attribuiti vari significati, che ruotano tutti attorno ad un unico denominatore: l'identità personale è la formula che riassume ciò che rende una persona ciò che essa è», G. PINO, *L'identità personale*, in S. RODOTÀ, P. ZATTI (diretto da), *Trattato di Biodiritto*, cit., III, *Ambito e fonti del biodiritto*, 297; L. LONARDO, *Identità personale, metodi, diritti della personalità*, 1077.

[34] S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. critica dir. priv.*, 1997, 583.

[35] La persona digitale è definita da R. CLARK, *The digital persona and its Application to Data Surveillance*, in *Inf. Soc.*, 1994, 77 – 92, nei termini di un costrutto «destinato ad essere utilizzato come *proxy* dell'individuo»; G. ALPA, *L'identità digitale e la tutela della persona*, 727. Tratteggiano il rischio che l'uomo della società algoritmica possa diventare una «categoria merceologica» A. QUARTA, U. MATTEI, *Punto di svolta. Ecologia, tecnologia e diritto privato. Dal capitale ai beni comuni*, Sansepolcro, 2018, 15.

[36] S. RODOTÀ, *La vita e le regole. Tra diritto e non diritto*, Milano, 2012, 99.

[37] S. ROSSI, *Corpo*, cit., 221.

[38] S. RODOTÀ, *Il corpo tra norma giuridica e norma sociale*, in *Nuove geometrie della mente. Psicoanalisi e bioetica*, in L. PRETA, Roma-Bari, 1999, 91 ss.

[39] P. PERLINGIERI, *Riflessioni sull'inseminazione artificiale e sulla manipolazione genetica*, in *Justitia*, 1988, 100.

[40] «Nella dottrina prevalente si identifica la personalità con la capacità giuridica generale e la si definisce come attitudine ad essere titolare di diritti e di doveri. In conseguenza, se la personalità è come un guscio bisognoso di contenere diritti e a tal uopo destinato, tutti i diritti, in quanto destinati a dar contenuto alla personalità, potrebbero dirsi diritti della personalità. Se non che il comune linguaggio giuridico riserva tale denominazione ai cosiddetti diritti essenziali, senza dei quali la personalità rimarrebbe un'attitudine completamente insoddisfatta, priva di ogni concreto valore […] La tutela della personalità concernerebbe l'individualità e l'inviolabilità fisica e morale della persona […] Poiché giuridicamente parlando si dispone di diritti e non già di beni, ci si è domandato: si può disporre del corpo umano, nel senso che esistono diritti sul corpo umano e dei quali si possa disporre? Il problema da risolvere è, allora, quello dell'oggetto dei diritti della personalità», M. PESANTE, *Corpo umano (atti di disposizione)*, in *Enciclopedia del diritto*, Milano, Giuffrè, pag. 653; A. DE CUPIS, *I diritti della personalità*, Milano, Giuffrè, 1950, pag. 19.

[41] C. MAIORCA, *La cosa in senso giuridico. Contributo alla critica di un dogma* (1937), rist., Camerino-Napoli, 1981, 29 ss.

assimilare le situazioni esistenziali, che fanno capo alla persona umana, ai beni suscettibili di appropriazione, godimento e disposizione»[42].

Gli attributi della persona non si piegano, sotto diversi profili, alla logica del diritto soggettivo. Il concetto di diritto, anche se riferibile a categorie diverse dalla proprietà, evoca inevitabilmente la logica dominicale di appartenenza. Essa attribuisce al soggetto che ne è titolare un potere di utilizzo, di disposizione [43] ed esclusione di altri, sino alla possibilità di dismissione e distruzione nei limiti del contenuto del diritto attribuito. Nessuno di questi predicati può dirsi conferente con le situazioni giuridiche che fanno capo alla persona in quanto tale[44].

Dalla lettura dell'art. 5 c.c., paradigma normativo fondamentale per la teorica dei negozi giuridici a contenuto non patrimoniale, emerge l'assenza di un principio di assoluta indisponibilità del corpo[45]. La nozione medesima di «disposizione»[46], inoltre, è suscettibile di un'interpretazione restrittiva ovvero estensiva, tanto che la sua concreta portata applicativa si comprende solo all'esito del confronto con le discipline di settore. Le discipline settoriali contemplano atti dispositivi che importano la diminuzione permanente dell'integrità fisica. Ciò consente di sostenere che, più che il rispetto del limite esterno della liceità, esse esaltano la dimensione della meritevolezza sottesa allo specifico atto[47]. In questi termini si spiega la tesi già espressa in dottrina, secondo la quale un'interpretazione lata dell'art. 5 c.c. finirebbe oggi per divenire incostituzionale, in quanto lesiva della libertà di autodeterminazione[48]. La regola codicistica appare in ogni caso insufficiente a disciplinare le possibili forme di coinvolgimento di interessi attinenti alla persona[49].

---

[42] S. POLIDORI, *Situazioni esistenziali, beni e diritti: dal negozio a contenuto non patrimoniale al mercato dei segni distintivi della personalità*, in *Annali SISDiC*, V, 2020, 1 – 2, il quale rileva (*ibid.*, nota 3) che «l'approccio al tema delle situazioni esistenziali rischia di condurre a risultati fuorvianti laddove condotto sulla scorta delle categorie giuridiche forgiate sulla tutela del patrimonio, *in primis* quella del diritto soggettivo»; si veda altresì P. PERLINGIERI, *Il diritto alla salute quale diritto della personalità*, in *Rass. dir. civ.*, 1982, 1020 ss.

[43] F. SANTORO-PASSARELLI, *Dottrine generali del diritto civile*, Napoli, 1954, 186 ss., e 196 ss.

[44] Lo rileva lucidamente S. POLIDORI, *Situazioni esistenziali*, cit., pag. 2, il quale suggerisce a tal scopo di utilizzare la più evocativa espressione «situazioni esistenziali»; M. A URCIOLI, *Autonomia negoziale e diritto all'immagine*, Napoli, 2000, 52 ss.

[45] V. RIZZO, *Atti di «disposizione» del corpo e tecniche legislative*, in *Rass. dir. civ.*, 1989, 625; C. M. D'ARRIGO, *Il contratto e il corpo: meritevolezza e liceità degli atti di disposizione dell'integrità fisica*, in *Familia*, 2005, 777 ss.

[46] «Quando degli atti di disposizione si vuol parlare con riferimento al corpo umano e si vuole usare la preposizione "sul", più lata della preposizione "del", si vengono ad indicare tutti quegli atti di attribuzione obbligatori, di disposizione attributivi e di disposizione in senso stretto, onerosi e gratuiti, costitutivi o modificativi o estintivi, il cui indice di riferimento oggettivo sia dato dal corpo umano, dalle sue parti o anche dalle attività psico-fisiche sia dei soggetti medesimi dell'atto giuridico, sia ancora di terzi», M. PESANTE, *Corpo umano (atti di disposizione)*, cit., pag. 653.

[47] Così S. POLIDORI, *Situazioni esistenziali*, cit., pag. 3, ove ancora si legge: «ragioni solidaristiche, se si vuole altruistiche e, al tempo stesso, legate al pieno sviluppo della personalità del disponente» (*ibid.*); ID., *Il controllo di meritevolezza sugli atti di autonomia negoziale*, in G. Perlingieri, M. D'Ambrosio, *Fonti, metodo e interpretazione. Primo incontro di studio dell'associazione dei dottorati di diritto privato*, Napoli, 2017, 391 ss.; C. M. D'ARRIGO, *Il contratto e il corpo: meritevolezza e liceità degli atti di disposizione dell'integrità fisica*, in *Familia*, 2005, 777 ss.

[48] G. ANZANI, *Gli «atti di disposizione della persona» nel prisma dell'identità personale (tra regole e principi)*, in *La nuova giurisprudenza civile commentata*, I, 2009, 1: «l'art. 5 c.c. può essere interpretato restrittivamente, così da regolare la sua portata applicativa agli atti di disposizione giuridica del corpo, oppure estensivamente, così da ricomprendere gli atti di disposizione materiale; ma un'interpretazione lata finirebbe oggigiorno con l'essere incostituzionale, in quanto lesiva della libertà di autodeterminazione, specialmente qualora l'esercizio di quest'ultima sia protesa verso una piena realizzazione della personalità».

[49] «"Attengono", ma non "appartengono", perché in tema di attributi personalissimi è impossibile individuare una demarcazione fra soggetto titolare e oggetto del diritto: la persona è al tempo stesso il

Conclusioni: Il corpo e il mercato.

Le regole giuridiche mirano a garantire il soddisfacimento ordinato dei bisogni dell'uomo, consentendo lo sviluppo armonico della personalità umana nel contesto sociale. Tra questi precetti è da annoverare quanto rientra nell'ampio concetto di proprietà, in quanto le relative regole trovano fondamento in una delle innate esigenze dell'uomo [50]. La prospettiva dominicale potrebbe tuttavia suggerire un utilizzo spregiudicato del corpo con l'obiettivo di conseguire un'utilità economica.

Ebbene, alla dinamica corpo-mercato sembra corrispondere la dialettica tra essenza ed attinenza. Il trattamento giuridico degli atti di disposizione del corpo suggerisce l'estensione della categoria del negozio giuridico all'ambito della disposizione di situazioni giuridiche non patrimoniali, sebbene sia netta la demarcazione con la disciplina del contratto[51].

Se, difatti, resta salva la rilevanza del consenso, si registra una sensibile attenuazione della forza di legge [52]. La non assimilabilità della situazione esistenziale alla *res* comporta la possibilità di revocare il consenso in ogni momento. La definitività delle statuizioni del diritto patrimoniale (art. 1372 c.c.) lascia il posto alla regola *rebus sic stantibus*[53], fermo restando un esercizio improntato a lealtà, correttezza e solidarietà, anche delle situazioni esistenziali.

In alcuni settori di mercato la prassi commerciale è sempre più interessata ad aspetti della personalità[54]. È il caso, ad esempio, dell'immagine e dei segni distintivi della persona[55] e di alcune note figure contrattuali, come il *testimonial* pubblicitario, la sponsorizzazione e, più in generale, vari esempi di *personality merchandising*. Anche in questo caso sarebbe limitante una prospettiva ancorata alla sola dimensione contrattuale, giacché è evidente la presenza di una componente esistenziale nella capacità evocativa della personalità del soggetto rappresentato. Si porrebbe in contrasto con la gerarchia assiologica del sistema l'atteggiamento teso ad ignorare la componente personalissima nell'individuazione di una disciplina del concreto rapporto oggetto di analisi.

---

titolare della situazione giuridica e l'oggetto della tutela, che non a caso è offerta dall'ordinamento anche nei confronti di atti lesivi provenienti dal medesimo titolare», S. POLIDORI, *Situazioni esistenziali*, cit., pagg. 2 – 3; L. LONARDO, *Informazione e persona. Conflitti di interessi e concorso di valori*, Napoli, 1999, 166 ss.

[50] G. GIAIMO, *Il corpo umano tra proprietà e autodeterminazione*, II, 2020, 49.

[51] S. POLIDORI, *Situazioni esistenziali*, cit., 4; P. PERLINGIERI, *Mercato, solidarietà, diritti umani*, in *Rass. dir. civ.*, 1995, 84 ss.; C. MIGNONE, *Identità della persona e potere di disposizione*, Camerino-Napoli, 2014, 287 ss.

[52] A. NICOLUSSI, *Autonomia contrattuale e diritti della persona*, in S. Mazzamuto, in L. NIVARRA, *Giurisprudenza per principi e autonomia privata*, Torino, 2016, 119 ss.

[53] L. DI BONA, *I negozi giuridici a contenuto non patrimoniale*, Napoli, 2000, 138 ss.

[54] S. POLIDORI, *Situazioni esistenziali*, cit., 7.

[55] V. ZENO-ZENCOVICH, *Profili negoziali degli attributi della personalità*, in *Dir. inf.*, 1993, 555 ss.

Guida S, 'Golem vs. transhuman: l'uomo del futuro tra biologia, nuove tecnologie, etica e sostenibilità ' (2022) 2 EJPLT, 313-346.
DOI : https://doi.org/10.57230/EJPLT222SG

EJPLT
ISSN 2704-8012



Golem vs. Transhuman: l'uomo del futuro tra biologia, nuove tecnologie, etica e sostenibilità.

Golem vs. Transhuman: the man of the future between biology, new technology, ethic and sustainability.

SERGIO GUIDA
Independent Scholar, Founder & Team Leader
Sustaihuble Impact LAB

Abstract

In tema di uomo del futuro, spaziare tra diverse discipline fa pensare a come le scoperte e le innovazioni scientifiche, supportate e potenziate dalle nuove tecnologie, abbiano importanti ricadute etiche e interrogativi sui vantaggi concreti e sul benessere che l'essere umano potrebbe derivare dall'uso consapevole e responsabile di strumenti inediti e straordinari come CRISPR Cas9, un sistema di editing genomico Premio Nobel per la Chimica nel 2020. Come evidenziato anche da EGE e OMS, le terapie cellulari varcano un confine, trasformando le persone in una 'nuova somma di nuove parti', sicché consultazioni pubbliche le più ampie possibili sono essenziali per garantire che la piena sostenibilità scientifica e tecnologica sia valutata dagli stakeholder globali, magari integrati fra loro.

About the man of the future, ranging between different disciplines suggests how scientific discoveries and innovations, supported and enhanced by new technologies, pose important ethical implications and questions on the concrete advantages and well-being that human beings could derive from conscious and responsible use of unprecedented and extraordinary tools, such as CRISPR Cas9, a genomic editing system Nobel Prize in Chemistry in 2020. As also highlighted by EGE and WHO, cell therapies cross a border, so that the broadest public consultations are essential to ensure that full scientific and technological sustainability is evaluated by global stakeholders, even integrated with each other.

© The author(s) 2022, 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: editing genomico; crispr/cas9; life design; innovazione sostenibile

Summary: Introduzione. – 1. Vita, complessità, naturale, artificiale. – 2. Ab ordine chaos... Golem vs. Transhuman. – 3. Disegno intelligente e intelligenza del disegno. – 4. Techne, Hybris, Ethos. – 5. Senso del limite e rischi percepiti. – 6. Etica dell'editing genomico (UE). – 7. Raccomandazioni e quadro per la governance (OMS). – 7.1. Ricerca sull'editing del genoma umano attuale, potenziale e speculativa (OMS). – 7.2. Ammissibilità editing genoma ereditabile (x riproduzione) per regione OMS. – 8. (New) life design. L'uomo come fulcro di un impatto sostenibile. – 9. Innovazione sostenibile. Bridging the sustainability gap. – Conclusioni.

Introduzione.

L'ascesa della scienza e della tecnologia moderne ha trasformato radicalmente il rapporto tra gli esseri umani e la natura. La natura, che per millenni era sembrata onnipotente e immutabile, è improvvisamente diventata un oggetto di controllo e manipolazione, qualcosa che può essere sistematicamente modellato per fini umani. Tuttavia, durante i drammatici sconvolgimenti dell'era moderna, le costanti fondamentali della natura umana - la mortalità umana, un repertorio condiviso di emozioni e stati d'animo, una gamma di capacità percettive e intellettuali di base - sono rimaste un punto di riferimento relativamente fisso che poteva colmare le differenze culturali e ideologiche. Ma negli ultimi decenni, i progressi radicali della genetica e delle neuroscienze, dell'informatica e di altre forme di tecnologia, hanno aumentato la possibilità che siamo sull'orlo di un'ulteriore rivoluzione, questa volta non nella nostra relazione con il mondo naturale, ma nella nostra relazione con noi stessi (fig.1).

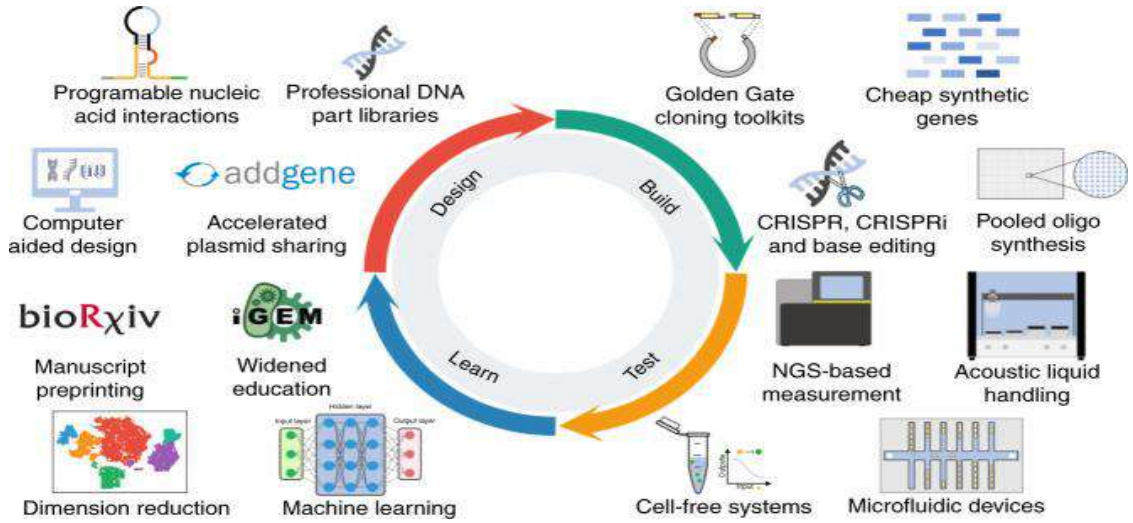


Fig. 1: Nuove tecnologie abilitanti e modalità di lavoro che hanno accelerato il ciclo progettazione-costruzione-test-apprendimento della biologia sintetica nell'ultimo decennio. Il diagramma mostra il ciclo ingegneristico utilizzato nella biologia sintetica (al centro) con icone

che illustrano alcune delle tecnologie chiave e dei metodi di lavoro che ora aiutano ad accelerare ogni fase del ciclo[1].

Anche i nostri corpi, persino i nostri sentimenti, pensieri e capacità intellettuali, stanno gradualmente entrando nella sfera del controllo e della manipolazione scientifica. Sembra che presto saremo in grado di potenziare radicalmente le capacità umane ben oltre il normale range. In alcuni ambienti si parla addirittura di un'era post-umana che si avvicina, una prospettiva che fa orrore a molti, ma alletta altri. Ad es., l'uso di pillole per «rallegrare» l'umore e la diagnosi di nuove condizioni psichiatriche controverse e curabili farmacologicamente come il disturbo da deficit di attenzione, stanno mettendo in discussione la tradizionale concezione della medicina come interessata solo al trattamento e alla cura della malattia.

Le nozioni tradizionali di natura umana, normalità e prosperità sembrano sempre più inadeguate. I fautori del potenziamento li vedono come sviluppi positivi. Sostengono che è giunto il momento di utilizzare la scienza biomedica, non solo per combattere le malattie, ma anche per migliorare positivamente le capacità umane e il benessere. Ma gli oppositori del potenziamento vedono questi sviluppi come una grave minaccia a ciò che è più caro nella vita umana. Queste speranze e paure contrastanti hanno già generato intense polemiche[2].

D'altro canto, i cambiamenti significativi delle nuove tecnologie e della globalizzazione hanno messo il mondo di fronte al limite (già Hutton, Giddens e Meyers, On the edge, 2000). Da nessuna parte questo è sperimentato con più vigore che in medicina, dove l'editing genetico, i gene drive, i Big Data, l'intelligenza artificiale, gli organoidi e le chimere offrono possibilità senza precedenti ma anche implicazioni imprevedibili. Quindi, la concezione di essere al limite sembra essere pervasiva e solleva la questione di cosa significhi essere al limite della medicina e quale sia il ruolo delle discipline umanistiche a questo limite[3].

In effetti le nuove tecnologie sfidano le concezioni filosofiche di base come la personalità, la coscienza, l'incarnazione e l'empowerment. Ad esempio, le connessioni computer-cervello e il potenziale per scaricare il contenuto del cervello umano o per generare autocoscienza sui computer, sfidano le concezioni fondamentali della filosofia. Quindi, le nuove tecnologie ai margini della medicina e della scienza mettono la filosofia al limite. Sono in gioco concetti fondamentali tradizionali, come «umanità» e «naturale».

Nuove sfide pongono nuove domande che richiedono nuove prospettive e approcci: le tecnologie emergenti non solo rivitalizzano la domanda «che cos'è un essere umano?» ma pongono anche la domanda cruciale «cosa significa essere un essere umano?» e «cosa dovremmo fare in modo che sia un essere

[1] Immagine e didascalia tratti da F. MENG, T. ELLIS, *The second decade of synthetic biology: 2010-2020*, in *Nature communications*, 2020, 11(1), 5174. Consultabile al sito: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7560693/.

[2] Cfr. J. SAVULESCU, R.T. MEULEN, G. KAHANE, *Enhancing Human Capacities*, 2011, Blackwell Publishing. Consultabile al sito: https://onlinelibrary.wiley.com/doi/10.1002/9781444393552.fmatter, XV.

[3] Cfr. B. HOFMANN, *The role of philosophy and ethics at the edges of medicine*, in *Philos Ethics Humanit Med*, 2021, 16, 14. Consultabile al sito: https://peh-med.biomedcentral.com/articles/10.1186/s13010-021-00114-w.

umano?» Tali domande possono richiedere prospettive nuove e più ampie di quelle finora sviluppate[4].

1. Vita, complessità, naturale, artificiale.

La conoscenza umana sulla «natura delle leggi in natura» si è ampliata negli ultimi 50 anni: i sistemi viventi mostrano essenzialmente una dinamica non lineare caratterizzata da uno sviluppo al limite della criticità.

Tuttavia, molte strutture e funzioni a livello di sistemi si sovrappongono, suggerendo che potrebbero non avere una chiara definizione fisiologica, sicché padroneggiare la modellazione di sistemi biologici complessi è una sfida terribilmente seria (fig.2).

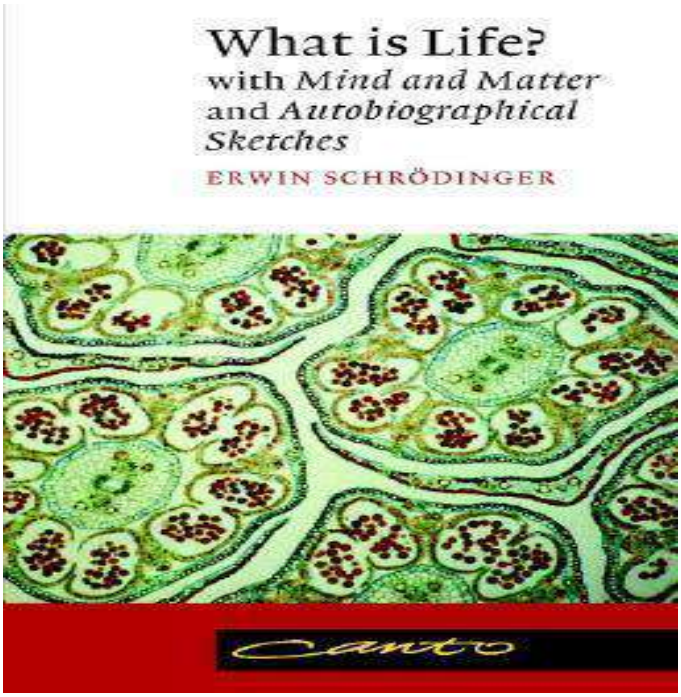


Fig. 2: in Cos'è la vita?, Schrödinger focalizza l'attenzione su: (a) la natura del materiale ereditario e (b) la termodinamica dei sistemi viventi. In una revisione dello stato delle conoscenze della genetica in quel momento, Schrödinger ha considerato una serie di argomenti relativi ai fenomeni genetici.

Ad es. Denis Noble ha fatto appello a modelli pratici e sostenibili che uniscano i diversi livelli di rappresentazione, verso una visione più olistica e «organica» della vita che vada oltre la teoria generale dei sistemi, la biologia dei sistemi e sistemi di insiemi fuzzy nei regni delle interazioni quantistiche: in ogni caso, nei sistemi viventi ci sono flussi di informazioni ed energia estremamente complessi[5].

[4] *Ibidem*.
[5] Cfr. «I rigorosi strumenti computazionali del Progetto Physiome (www.physiomeproject.org) sono pronti con molti dei modelli fisiologici necessari per svolgere il lavoro. Questo è esattamente il modo in cui il

Il concetto di vita artificiale può assumere diversi significati. Nel suo uso attuale, il termine vita artificiale (ALife) è stato coniato da Christopher Langton (1989), che lo definì come «vita fatta dall'uomo piuttosto che dalla natura», poi come «lo studio della vita naturale, in cui la natura è intesa come includere piuttosto che escludere, gli esseri umani e i loro manufatti» (1998). Allora gli esseri umani, e tutto ciò che fanno, fanno parte della natura e, come tale, uno degli obiettivi principali di ALife dovrebbe essere quello di lavorare per rimuovere la «vita artificiale» come una frase che differisce nel significato in modo fondamentale dal termine «biologia»[6].

In realtà ALife è un campo radicalmente interdisciplinare che comprende biologi, informatici, fisici, medici, chimici, ingegneri, robotisti, filosofi, artisti e rappresentanti di molte altre discipline. Esistono diversi approcci per definire la ricerca ALife, ma si può distinguere tra tre declinazioni che esibiscono un comportamento simile alla vita (fig.3)[7]:

- Soft ALife mira a creare simulazioni o altre costruzioni puramente digitali.
- Hard ALife è legato alla robotica e hardware costituito principalmente da silicio, acciaio e plastica.
- Wet ALife utilizza tutti gli approcci di chimica e biochimica per sintetizzare sistemi in laboratorio.

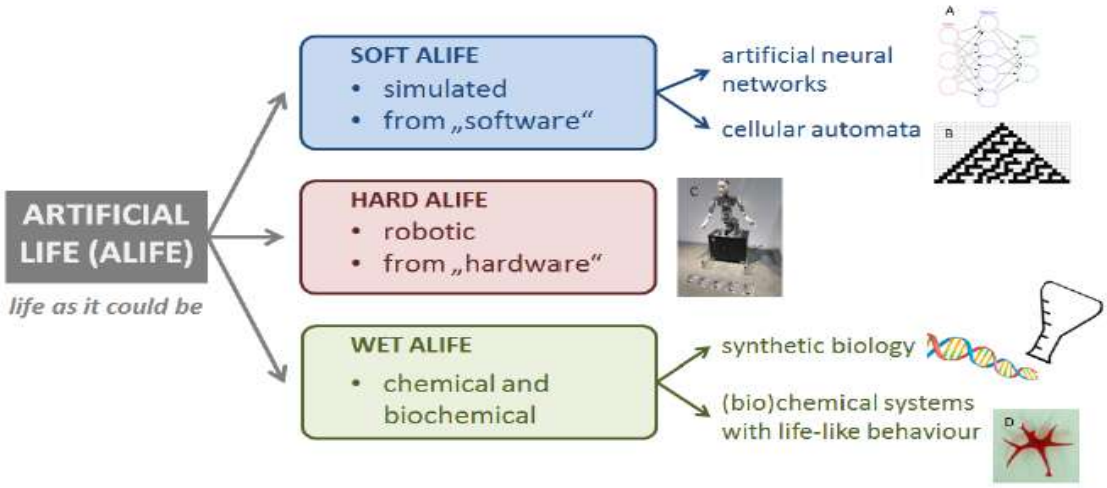


Fig. 3: Ricerca sulla vita artificiale e sue articolazioni (fonte Gershenson, *op.cit.*).

confronto tra associazione genetica e causalità funzionale è stato dimostrato per il pacemaker cardiaco e potrebbe essere dimostrato per molti altri punteggi di associazione gene-fenotipo. La differenza tra associazione e causalità è una misura importante della misura in cui le reti fisiologiche funzionali proteggono l'organismo dalla variazione genomica. Abbiamo bisogno di quella misura per fare progressi, perché è alla base della finalità della vita. La misurazione empirica di tale differenza è anche una forma di prova della finalità negli organismi. La fisiologia è anche la via da seguire per seguire la scomparsa della barriera di Weismann. In effetti lo sta già facendo in un'ampia ricerca nel corso di molti anni sugli effetti materni e paterni trans-generazionali e sui processi molecolari e di altro tipo mediante i quali si verificano» in D. NOBLE, *What Future for Evolutionary Biology? Response to Commentaries on «The Illusions of the Modern Synthesis»*, in *Biosemiotics*, 2021 14. Consultabile al sito: https://www.researchgate.net/publication/355071379_What_Future_for_Evolutionary_Biology_Response_to_Commentaries_on_The_Illusions_of_the_Modern_Synthesis.

[6] Cfr. W. AGUILAR, G. SANTAMARÍA-BONFIL, T. FROESE, C. GERSHENSON, *The past, present, and future of artificial life,* in *Front. Robot. AI, Sec. Computational Intelligence in Robotics*, 2014. Consultabile al sito: https://www.frontiersin.org/articles/10.3389/frobt.2014.00008/full .

[7] Cfr. C. GERSHENSON, J. ČEJKOVÁ, *Artificial life: sustainable self-replicating systems* in *ArXiv*, 2021. Consultabile al sito: https://arxiv.org/abs/2105.13971v2, 3.

2. Ab ordine chaos… Golem vs. Transhuman.

Dietro alla complessità dei dibattiti intorno all'uomo che verrà, una vera e propria «metafisica dell'evoluzione»[8] ha accomunato pensatori in apparenza molto diversi. È la stessa metafisica che ha modellato il transumanesimo contemporaneo, che non è soltanto una collezione di stranezze di eccentrici miliardari libertari con il pallino dell'immortalità, ma una visione che sostiene il dibattito sul domani.

Ad es., l'idea centrale del potenziamento umano è la prospettiva di migliorare le capacità, le prestazioni o il benessere umano con mezzi biomedici o biotecnici (Savulescu & Bostrom, 2009; Bostrom & Roache, 2008). In genere, questo è visto come un'impresa in contrasto con l'utilizzo di mezzi simili per mantenere o ripristinare le capacità, le prestazioni o il benessere umano a livelli considerati in qualche modo normali, sebbene alcuni sostengano che questa dicotomia potrebbe essere problematica (Cwik, 2019; Earp et al., 2014)[9].

Moatti (Aux racines du transhumanisme, 2020) cita come massimo profeta e divulgatore di questa visione lo storico israeliano Yuval Noah Harari, secondo il quale non c'è motivo di pensare che *sapiens* sia l'ultima fase dell'evoluzione. Del resto, sostiene Harari, l'umanità sta acquisendo in fretta qualità che abbiamo storicamente attribuito al divino.

«Creando un antropoide, il maestro ebreo non solo è in grado di manifestare le sue forze creative, ma può raggiungere l'esperienza del momento creativo di Dio, che ha creato anche l'uomo in modo simile a quello che si trova nelle ricette usate dai mistici e maghi. (..) Possiamo descrivere le pratiche del Golem come un tentativo dell'uomo di conoscere Dio mediante l'arte che usa per creare l'uomo» (Idel, 1990).

Originariamente un mito ebraico su una figura antropoide di argilla, il Golem si è reincarnato più e più volte, portando attraverso i secoli un'ansia e un fascino profondamente radicati riguardo alla prospettiva di una tecnologia intelligente e senziente che si spegne del controllo umano. Sebbene progettato per essere una sorta di robot obbediente, efficace e formidabile, il Golem nella maggior parte delle storie diventa indipendente dai suoi padroni e alla fine semina il caos tra i suoi creatori umani. Il Golem ha guadagnato una notevole reputazione nella cultura popolare ed è apparso frequentemente in letteratura - il più famoso in Der Golem di Gustav Meyrink del 1915, fig.4 -, nei fumetti (sia Marvel che DC Comics), film e televisione, dal film muto del 1915 Der Golem a I Simpson e X-Files[10].

[8] Cfr. A. MOATTI, *L'eterna illusione dell'uomo che verrà*, in *Il Foglio*, 7/6/2020. Consultabile al sito: https://www.ilfoglio.it/scienza/2020/06/07/news/leterna-illusione-delluomo-che-verra-320443/ .

[9] Cfr. D. M. LYRESKOG, A. MCKEOWN, *On the (Non-) Rationality of Human Enhancement and Transhumanism,* in *Science and engineering ethics*, 2022, 28(6), 52. Consultabile al sito: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9626409/.

[10] Cfr. A. VUDKA, *The Golem in the age of artificial intelligence*, in *Necsus*, July 6, 2020. Consultabile al sito: https://necsus-ejms.org/the-golem-in-the-age-of-artificial-intelligence/#_edn62.

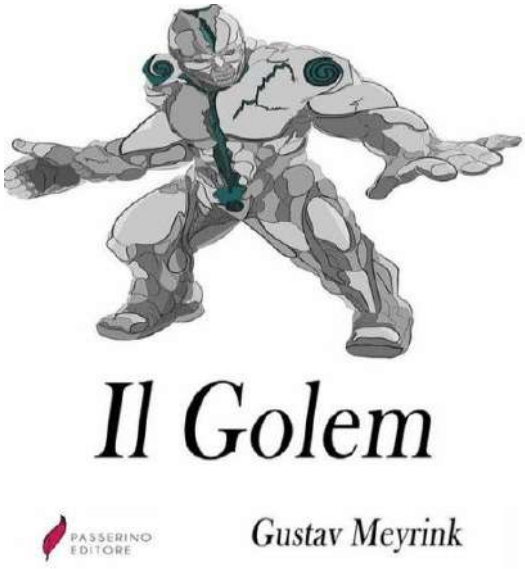


Fig. 4: «il libro è una delle opere di fantasy più avvincenti, atmosferiche e sbalorditive mai stampate» (D. BARNETT, *Meyrink's The Golem*, in *The Guardian*, 30 Jan 2014. Consultabile al sito: https://www.theguardian.com/books/booksblog/2014/jan/30/ the-golem-gustav-meyrink-books).

Guardando avanti, il prossimo trend tecnologico sui mercati potrebbe essere quello dei robot umanoidi, o meglio dei robot che lavoreranno come gli esseri umani (fig.5).

Secondo le stime di Goldman Sachs entro il 2030 i robot umanoidi potrebbero coprire il 4% della carenza di manodopera negli Usa e il 2% della forza lavoro mancante, a livello globale, nell'ambito dell'assistenza agli anziani. La previsione di Goldman Sachs, nel caso in cui gli ostacoli legati alla progettazione del prodotto, ai casi d'uso, alla tecnologia, all'accessibilità economica e all'ampia accettazione da parte del pubblico dovessero essere completamente superati (quindi lo scenario più ottimistico), è di un mercato potenziale da 154 miliardi di dollari entro il 2035 circa[11].

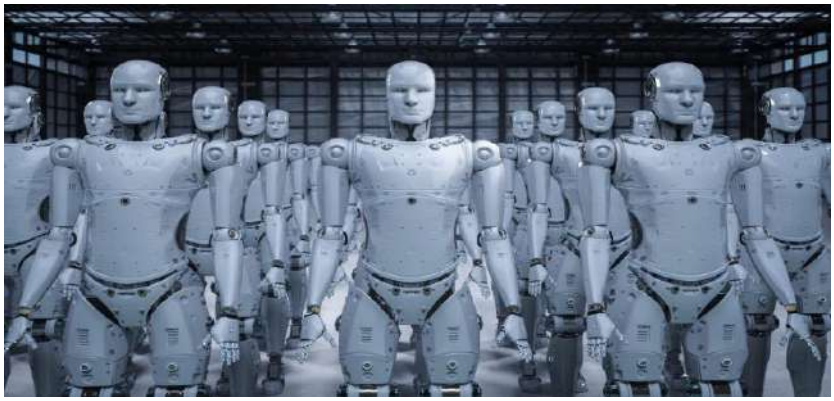


Fig. 5: i nuovi golem, transumani (fonte Cardarelli, *op. cit.*).

[11] Cfr. A. CARDARELLI, *Goldman Sachs scommette sui robot umanoidi*, in *Financial lounge*, 4/11/2022. Consultabile al sito: https://www.financialounge.com/news/2022/11/04/goldman-sachs-scommette-sui-robot-umanoidi/?y=700.

D'altra parte, nel 1543 Andreas Vesalius pubblicò a Basilea il *De humani corporis fabrica*, in cui rifletteva, con abbondanti illustrazioni, le sue conoscenze anatomiche acquisite attraverso l'esecuzione di dissezioni.

L'uso del termine «fabbrica», con connotazioni architettoniche, riflette già la concezione del corpo umano come struttura complessa da cui analizza ogni sua parte. Lo sviluppo della meccanica filosofica da parte di Francis Bacon e Rene Descartes nel XVII secolo mostra un cambiamento nella concezione della realtà che si è conclusa con la differenziazione tra le scienze liberali e le scienze meccaniche[12]. Fino ad arrivare al punto che «i geni potevano essere trasmessi fedelmente con tassi di mutazione (errori) inferiori a uno su un miliardo. Questo straordinario alto grado di fedeltà convinse Schrödinger che le leggi dell'ereditarietà non potevano essere fondate sulle leggi classiche dell'«ordine dal disordine»[13]. Invece, ha proposto che i geni fossero più simili a singoli atomi o molecole in quanto soggetti alle regole non classiche ma stranamente ordinate della scienza che ha contribuito a fondare, la meccanica quantistica»[14].

In realtà si può scorgere un fattore comune tra gli elementi: vi è qualcosa di profondamente legato al vivente umano in concetti come quello di «mostro»[15]. È in definitiva il ruolo che la «funzione senza organo» dell'immaginazione (come già aveva notato Bachelard) riveste nella produzione delle immagini, come peraltro immediatamente evidente anche di fronte alle figure 4 e 5, *supra*.

In fondo l'immaginario è quell'elemento che impedisce in fondo che la scienza finisca per produrre un mondo biecamente positivista, dove tutto cade sotto il dominio delle leggi della natura, ma solo a patto che esso non divenga l'occasione per lo scienziato di perdersi in un «antimondo» dove tutto è possibile, dimenticando che ogni eccezione, ogni mostro, presuppone una legge da infrangere[16].

---

[12] Cfr. A. CASTÁN, *Humans Moving Toward a Cyborg Horizon*, in *Bbbvaopenmind*, 8/9/2017. Consultabile al sito: https://www.bbvaopenmind.com/en/technology/future/humans-moving-toward-a-cyborg-horizon/.

[13] Cfr. «Con l'applicazione della teoria quantistica ai fenomeni biologici, Schrödinger (1944) tentò di chiarire la struttura e la funzione dei geni in termini di un paradigma ibrido. È spesso all'intersezione di due o più discipline che avviene il progresso scientifico innovativo. Heisenberg (1962), scrivendo di fisica e filosofia, aveva affermato in precedenza che "nella storia del pensiero umano gli sviluppi più fruttuosi si verificano spesso in quei punti in cui due diverse linee di pensiero si incontrano". Nuovi rami della scienza nascono da una sintesi di diversi punti di vista, concetti e metodi di diverse discipline, perché porta a un "vigore ibrido" sul piano intellettuale. Ad esempio, le tecniche di diffrazione dei raggi X hanno contribuito alla delucidazione della struttura del DNA (Watson e Crick,1953). Tuttavia, nel caso in esame, il fisico Schrödinger ha indicato un nuovo modo di guardare alla biologia, rinvigorendo e stimolando così il pensiero di una nuova generazione di biologi. L'ascesa della biologia molecolare, il progetto del genoma umano e varie scienze della salute ambientale sono il risultato diretto di una riuscita sintesi tra molteplici discipline scientifiche. Questo processo è stato chiamato "ibridazione intellettuale" (Dronamraju,1989). Non fu tanto una "rivoluzione" discontinua nel senso kuhniano (Kuhn,1962), ma una graduale sintesi (o "evoluzione") di idee, concetti e metodi provenienti da diverse discipline», come si legge in K.R. DRONAMRAJU, *Erwin Schrödinger and the Origins of Molecular Biology*, in *Genetics*, 1999, 153, 3, 1071–1076. Consultabile al sito: https://academic.oup.com/genetics/article/153/3/1071/6050772.

[14] Cfr. J. MCFADDEN, J. AL-KHALILI, *The origins of quantum biology*, in *Proc. R. Soc. A*, 2018, 474, 2220. Consultabile al sito: https://royalsocietypublishing.org/doi/10.1098/rspa.2018.0674.

[15] Come si legge in G. VISSIO, *Georges Canguilhem, La conoscenza della vita. Introduzione all'edizione italiana*, in *S&F*_n. 17_2017, Consultabile al sito: https://www.scienzaefilosofia.com/?portfolio=georges-canguilhem-la-conoscenza-della-vita-tr-it-a-cura-di-franco-bassani-introduzione-alledizione-italiana-di-antonio-santucci-il-mulino-bologna-1976-pp-279.

[16] *Ibidem*.

3. Disegno intelligente e intelligenza del disegno.

Le cellule eucariotiche utilizzano una sofisticata rete di geni ed elementi regolatori genomici per svolgere funzioni relative alla crescita e morte cellulare, formazione e organizzazione di organelli, produzione di metaboliti e rilevamento del microambiente.

La capacità di manipolare con precisione il genoma è essenziale per comprendere processi cellulari complessi e dinamici.

In generale, l'ingegneria del genoma definisce approcci metodologici per alterare la sequenza del DNA genomico (editing genico), modificare i segni epigenetici (editing epigenetico), modulare l'output funzionale (regolazione trascrizionale) e riorganizzare la struttura cromosomica (manipolazione strutturale) (fig.6)[17]. Questi obiettivi richiedono un toolkit di molecole di design che possono essere opportunamente costruite e consegnate nelle cellule per svolgere una delle funzioni di cui sopra.

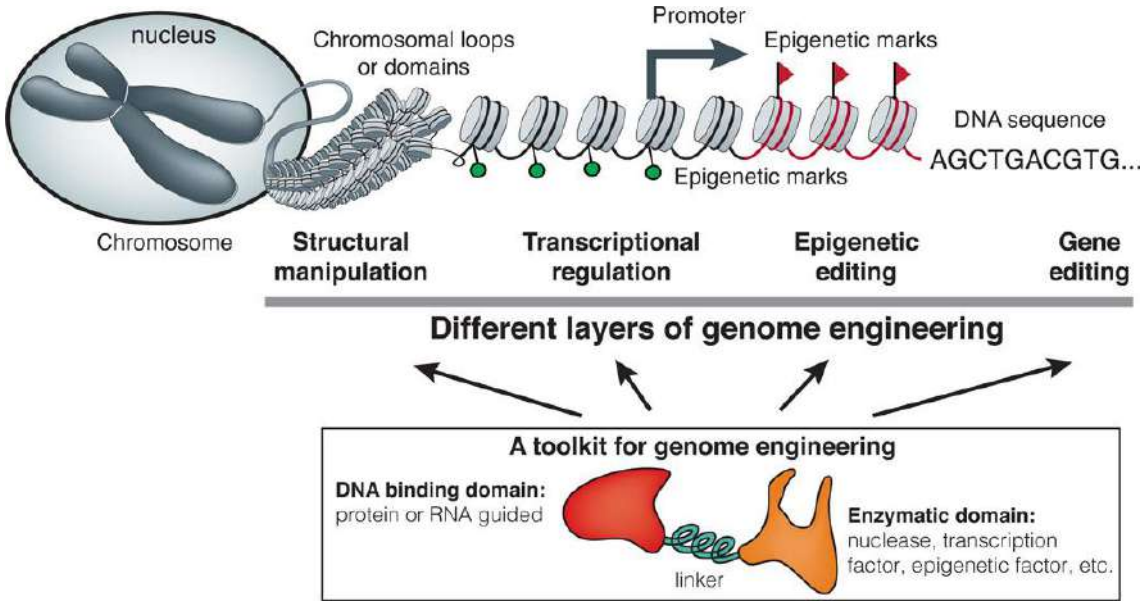


Fig. 6: Una visione schematica dei diversi obiettivi dell'ingegneria del genoma. Essa definisce approcci metodologici per alterare la sequenza del DNA (editing genomico), modificare i segni epigenetici (editing epigenetico), modulare l'output funzionale (regolazione trascrizionale) e riorganizzare la struttura cromosomica (manipolazione strutturale) (fonte Wang, *op.cit.*).

Ora possiamo sfruttare la biologia oltre la selezione artificiale e la riprogrammazione del segnale, che intervengono a un livello molecolare e nucleotidico inferiore, hackerando i macchinari della biologia molecolare e i suoi meccanismi di riparazione del DNA per riprogrammare le cellule con tecniche come CRISPR/CAS9 [18], che diventa così uno script *de facto* di

[17] Cfr. F. WANG, L. S. QI, *Applications of CRISPR Genome Engineering in Cell Biology*, in *Trends in cell biology*, 2016 26(11), 875–888. Consultabile al sito: https://www.ncbi.nlm.nih.gov/pmc/articles/ PMC5077632/.

[18] Cfr. «I ricercatori devono modificare i geni nelle cellule se vogliono scoprire i meccanismi interni della vita. Questo era un lavoro che richiedeva tempo, difficile e talvolta impossibile. Utilizzando le forbici genetiche CRISPR/Cas9, è ora possibile cambiare il codice della vita nel corso di poche settimane. (..) Come spesso

riprogrammazione biologica che hackera un meccanismo di riparazione del DNA per inserire un'istruzione valida sotto forma di un gene in una sequenza di DNA altrimenti naturale[19].

CRISPR/Cas9 (Clustered Regularly Interspaced Short Palindromic Repeats, brevi ripetizioni palindrome raggruppate e separate a intervalli regolari) è una tecnologia di editing genetico che coinvolge due componenti essenziali: un RNA guida per abbinare un gene bersaglio desiderato e Cas9 (proteina 9 associata a CRISPR), un'endonucleasi che provoca una rottura del DNA a doppio filamento, consentendo modifiche al genoma (fig. 7)[20].

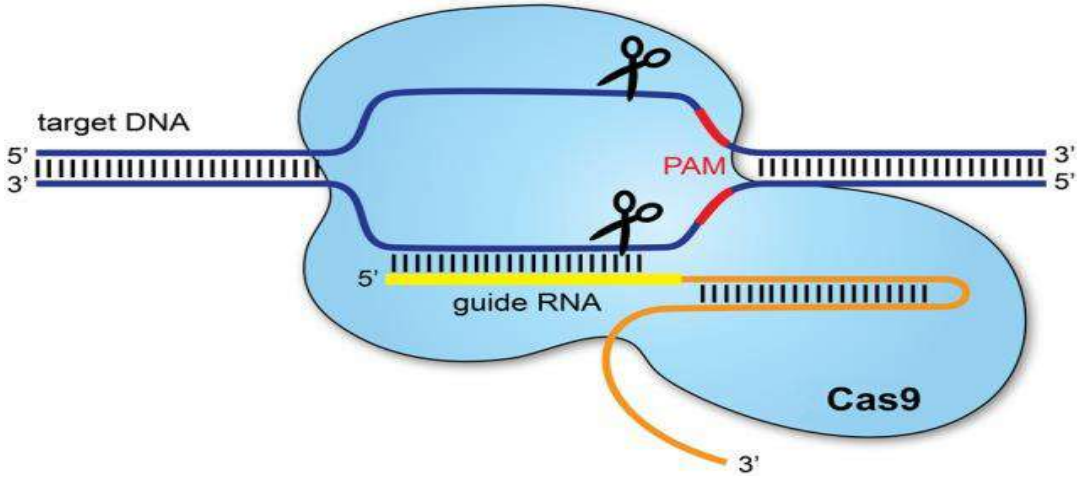


Fig. 7: Il sistema CRISPR/Cas9 (fonte Redman, *op.cit.*).

Le ripetizioni palindrome raggruppate regolarmente interspaziate si riferiscono a sequenze nel genoma batterico. Offrono protezione contro i virus invasori, se combinati con una serie di proteine associate a CRISPR (Cas). Cas9, una delle proteine associate, è un'endonucleasi che taglia entrambi i filamenti di DNA. Cas9 è diretto al suo bersaglio da una sezione di RNA, un singolo filamento chiamato RNA sintetico a guida singola (sgRNA); la sezione di RNA

accade nella scienza, la scoperta di queste forbici genetiche è stata inaspettata. Durante gli studi di Emmanuelle Charpentier sullo Streptococcus pyogenes, uno dei batteri più dannosi per l'umanità, ha scoperto una molecola precedentemente sconosciuta, il tracrRNA. Il suo lavoro ha dimostrato che il tracrRNA fa parte dell'antico sistema immunitario dei batteri, CRISPR/Cas, che disarma i virus scindendo il loro DNA. Charpentier ha pubblicato la sua scoperta nel 2011. Lo stesso anno, ha avviato una collaborazione con Jennifer Doudna, una biochimica esperta con una vasta conoscenza dell'RNA. Insieme sono riuscite a ricreare le forbici genetiche dei batteri in una provetta e a semplificare i componenti molecolari delle forbici in modo che fossero più facili da usare. In un esperimento epocale, hanno poi riprogrammato le forbici genetiche. Nella loro forma naturale, le forbici riconoscono il DNA dei virus, ma Charpentier e Doudna hanno dimostrato che possono essere controllate in modo da poter tagliare qualsiasi molecola di DNA in un punto predeterminato. Dove si taglia il DNA è poi facile riscrivere il codice della vita», come si legge nella *Press release* dell'ACCADEMIA REALE SVEDESE DELLE SCIENZE che il 7 ottobre 2020 ha assegnato il Premio Nobel per la Chimica 2020 a Emmanuelle Charpentier - Unità Max Planck per la scienza degli agenti patogeni, Berlino, Germania e Jennifer A. Doudna - Università della California, Berkeley, USA «per lo sviluppo di un metodo per l'editing del genoma». Consultabile al sito: https://www.nobelprize.org/prizes/chemistry/2020/press-release/.

[19] Cfr. H. ZENIL, *Reprogramming Matter, Life, and Purpose*, in *International Journal of Unconventional Computing*, 2017,13. Consultabile al sito: https://arxiv.org/abs/1704.00725v4, 7.

[20] Cfr. M. REDMAN, A. KING, C. WATSON, D. KING, *What is CRISPR/Cas9?* in *Archives of disease in childhood. Education and practice edition,* 2016, 101(4), 213–215. Consultabile al sito: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4975809/.

che si lega al DNA genomico è di 18-20 nucleotidi. Per tagliare, una specifica sequenza di DNA compresa tra 2 e 5 nucleotidi (la sequenza esatta dipende dai batteri che producono il Cas9) deve trovarsi all'estremità 3' dell'RNA guida: questo è chiamato motivo adiacente protospacer (PAM). La riparazione dopo il taglio del DNA può avvenire attraverso due vie: giunzione dell'estremità non omologa, che in genere porta a un inserimento/ cancellazione casuale del DNA, o riparazione diretta per omologia in cui un pezzo omologo di DNA viene utilizzato come modello di riparazione. È quest'ultimo che consente una precisa modifica del genoma: la sezione omologa del DNA con il cambio di sequenza richiesto può essere fornita con la nucleasi Cas9 e l'sgRNA, consentendo teoricamente cambiamenti precisi[21].

Pertanto, il complesso Cas9 è stato sviluppato come uno strumento straordinariamente utile per l'editing del genoma (fig. 8)[22].

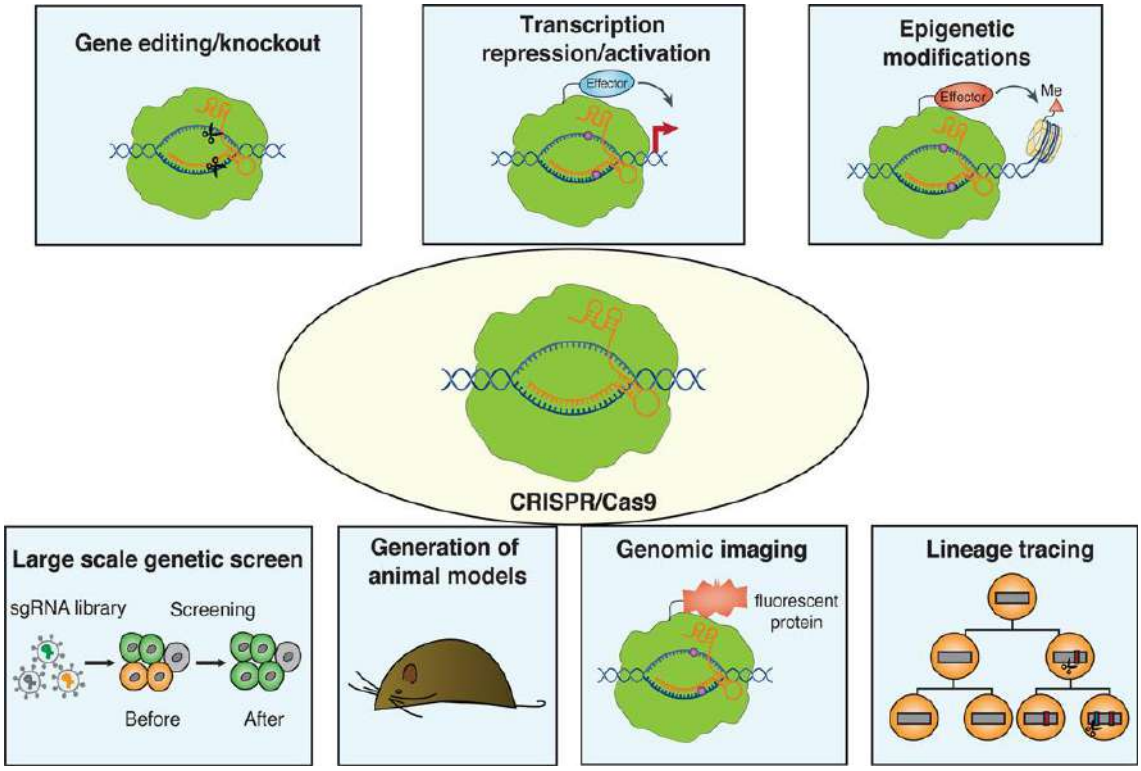


Fig. 8: Applicazioni di CRISPR/Cas9 alla ricerca in biologia cellulare. La tecnologia CRISPR/Cas9 è stata utilizzata per l'editing genetico, la regolazione trascrizionale, la regolazione epigenetica, gli schermi genetici su larga scala, la generazione di modelli animali e l'imaging genomico (fonte Wang, *op.cit.*).

È interessante notare che Cas9 richiede un'ampia omologia tra l'RNA guida e il DNA bersaglio per scindere, ma può rimanere legato in modo semi-transitorio con solo un breve tratto di sequenza complementare tra l'RNA guida e il DNA bersaglio.

Queste osservazioni suggeriscono che Cas9 ha molti siti di legame fuori

[21] *Ibidem.*
[22] Cfr. WANG, *op. cit.*.

bersaglio ma ne scinde solo una piccola frazione (Wu et al., 2014).

Pertanto, le preoccupazioni sull'attività fuori bersaglio potrebbero variare ampiamente data un'applicazione desiderata che sfrutta Cas9 per le sue capacità di legame o scissione del DNA[23].

In fig. 9 vengono sintetizzate le applicazioni di Cas9 come piattaforma di ingegneria del genoma[24]:

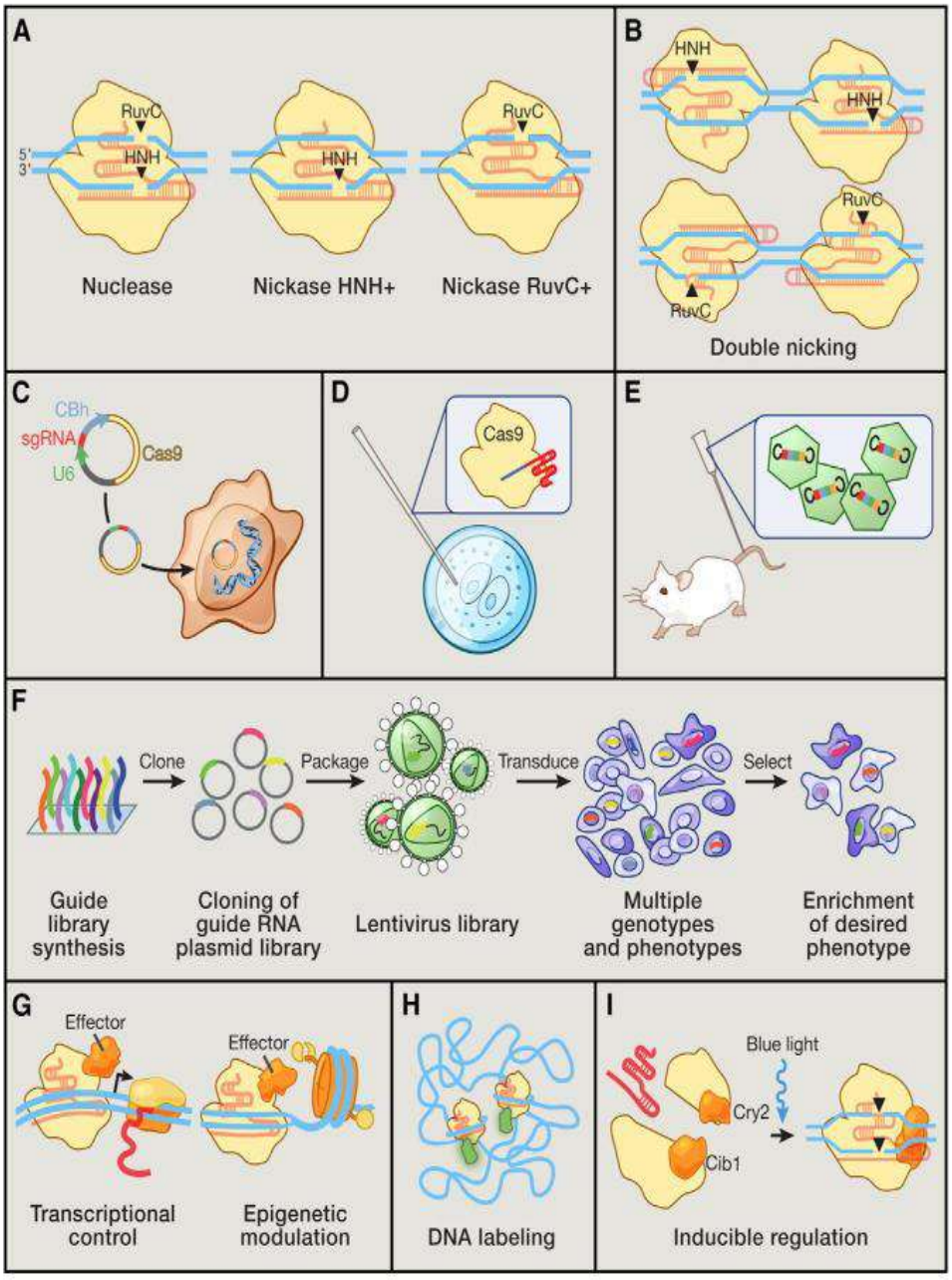


Fig. 9: Applicazioni di Cas9 come piattaforma di ingegneria del genoma (fonte Hsu, *op. cit.*).

[23] Cfr. P. D. HSU, , E. S. LANDER, F. ZHANG, *Development and applications of CRISPR-Cas9 for genome engineering*, in *Cell*, 2014, 157(6), 1262–1278. Consultabile al sito: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4343198/.

[24] *Ibidem*.

(A) La nucleasi Cas9 scinde il DNA attraverso i suoi domini nucleasi RuvC e HNH, ciascuno dei quali intacca un filamento di DNA per generare DSB a punta smussata. Entrambi i domini catalitici possono essere inattivati per generare mutanti di nickasi che causano rotture del DNA a singolo filamento.
(B) Due complessi di nickasi Cas9 con siti target opportunamente distanziati possono imitare i DSB mirati tramite nick cooperativi, raddoppiando la lunghezza del riconoscimento del target senza sacrificare l'efficienza della scissione.
(C) I plasmidi di espressione che codificano per il gene Cas9 e una breve cassetta sgRNA guidata dal promotore U6 RNA polimerasi III possono essere trasfettati direttamente in linee cellulari di interesse.
(D) La proteina Cas9 purificata e lo sgRNA trascritto in vitro possono essere microiniettati in zigoti fecondati per una rapida generazione di modelli animali transgenici.
(E) Per la modificazione genetica somatica, i vettori virali ad alto titolo che codificano i reagenti CRISPR possono essere trasdotti in tessuti o cellule di interesse.
(F) Lo screening funzionale su scala genomica può essere facilitato dalla sintesi di massa e dalla consegna di librerie di RNA guida.
(G) Cas9 cataliticamente morto (dCas9) può essere convertito in un dominio generale di legame al DNA e fuso con effettori funzionali come attivatori trascrizionali o enzimi epigenetici. La modularità del targeting e la scelta flessibile dei domini funzionali consentono una rapida espansione della cassetta degli attrezzi Cas9.
(H) Cas9 accoppiato a reporter fluorescenti facilita l'imaging dal vivo dei loci del DNA per illuminare le dinamiche dell'architettura del genoma.
(I) La ricostituzione di frammenti divisi di Cas9 tramite induzione chimica o ottica di domini eterodimeri, come il sistema cib1/cry2 di Arabidopsis, conferisce il controllo temporale dei processi cellulari dinamici.

Alcune delle ricerche relative alle malattie che applicano il sistema di editing genomico CRISPR/Cas9 sono riassunte nella figura 10[25].

[25] Cfr. W. YUSOF, *CRISPR/CAS9: an introduction to genome editing*, in *Malaysian Journal of Paediatrics and Child Health Online*, 2018/07/12. Consultabile al sito: https://www.researchgate.net/publication/326345230_CRISPRCAS9_AN_INTRODUCTION_TO_GENOME_EDITING.

Disease	Target location	Cells type	Function
Chronic granulomatous disease	*CYBB* gene	iPSCs from skin fibroblast	Restoration of oxidative burst function in iPSCs-derived phagocytes
β-thalassaemia	*HBB* gene	iPS from fibroblast	Recovery of *HBB* expression in iPSCs
β-thalassaemia	*HBB* gene	iPS from skin fibroblast	Recovery of *HBB* expression in iPSCs
Cystic fibrosis	*CTFR* gene	3D-intestinal organ cultures (organoids)	Patient's organoids showed functional recovery
Haemophilia A	*F8* gene	iPSCs from urine-derived cells	iPSCs showed functional recovery
Duchenne muscular dystrophy	*Dystrophin* gene	iPSCs from fibroblast	iPSCs showed functional recovery

iPSCs - induced pluripotent stem cells

Fig. 10: Malattie per le quali CRISPR/Cas9 è utilizzato negli studi clinici traslazionali (fonte Yusof, *op.cit.*).

Il fatto che CRISPR-Cas9 sia tra le scoperte importanti del 21° secolo è ampiamente accettato nella comunità scientifica e nelle industrie correlate.

Tuttavia, la rapida ascesa di CRISPR-Cas9 ha portato a nuove questioni bioetiche, sociali e legali in medicina, agricoltura, allevamento e ambiente.

I possibili rischi e le problematiche bioetiche legate a CRISPR-Cas9 sono riassunti nella figura 11[26].

[26] Cfr. F. B. AYANOĞLU, A. E. ELÇIN, Y. M. ELÇIN, *Bioethical issues in genome editing by CRISPR-Cas9 technology* in *Turkish journal of biology*, 2020, 44(2), 110–120. Consultabile al sito: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7129066/.

Possible risks and bioethical issues related to CRISPR-Cas9 technology.

Organism	Risks	Bioethical issues
Bacteria	Nontarget mutationsGene drifts	Ecological imbalance
Plants	Nontarget mutationsGene drifts	Ecological imbalancePatenting
Animals /chimeric animals	Nontarget mutations	Ecological imbalance Patenting Animal welfare and dignity Threatening of human dignity and identity
Humans	Nontarget mutations Side effects Cost Genetic mosaicism	Eugenics Informed consent Enhancement Accessibility Patenting Safety Incomplete or over legislations

Fig. 11: i possibili rischi e le problematiche bioetiche legate a CRISPR-Cas9 (fonte Ayanoğlu, *op.cit.*).

4. Techne, Hybris, Ethos.

In ambito medico, le implicazioni etiche nell'uso di CRISPR hanno prevalentemente a che vedere con la possibilità di creare modificazioni permanenti ed ereditabili dal genoma umano.

Una cosa è veicolare CRISPR per inattivare i geni mutati in un tumore, un'altra è veicolarlo in un embrione umano per correggere un difetto innato.

Eppure, la seconda applicazione è già tra noi: sono le bimbe cinesi in cui è stato inattivato un gene che le rende suscettibili all'infezione da HIV. I loro embrioni sono stati ingegnerizzati da He Jiankui in un istituto di Shenzen, tramite fertilizzazione in vitro, per essere protetti dalle conseguenze di avere un padre HIV-positivo. I contorni di questa vicenda ad oggi non sono chiari ma dettagli preoccupanti continuano ad emergere [27] . He Jiankui è stato condannato a 3 anni di prigione per avere nascosto ai pazienti molto di quanto

[27] Cfr. R. Cross, R. Mullin, M. Satyanarayana , J.F. Tremblay, *As claims of CRISPR use in first gene-edited babies emerge, scientists and ethicists respond*, in *Chemical & Engineering News*, November 30, 2018, Consultabile al sito: https://cen.acs.org/policy/claims-CRISPR-use-first-gene/96/i48.

aveva intenzione di fare[28].

Nonostante gli aspetti bioetici, è però chiaro a tutti quelli che si occupano di terapia genica che la promessa di liberarci di molte malattie, in particolare quelle congenite, debba passare dalla capacità di modificare il genoma. Il visionario George Church arriva ad affermare che dovremmo riscrivere il nostro genoma per renderci inattaccabili da altri organismi come i virus. E' lo «human recoding», che promette un mondo senza malattie[29].

Il 2 agosto 2022 il team del professor George Church dell'Università di Harvard e il team del ricercatore Liu Chenli dell'Institute of Synthetic Biology, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences hanno pubblicato un articolo intitolato «Multiplex base editing to convert TAG into TAA codons in the human genome» [30]. L'articolo studia l'uso della tecnologia di editing di base multiplex nel genoma umano: il team ha attivato la conversione a livello di gene dei codoni di stop TAG in TAA, ha dimostrato preliminarmente la fattibilità della conversione da TAG a TAA nel genoma umano e ha creato una singola consegna di basi sincrone in dozzine di siti non ripetitivi nel genoma umano. Il registro dell'editing di base fornisce un quadro di lavoro per l'ingegneria su larga scala dei genomi dei mammiferi. Inoltre, il software GRIT può anche essere sviluppato in una nuova piattaforma di progettazione assistita da computer (CAD) per la progettazione di genomi su larga scala.

Questo studio ha compiuto il primo passo nella preparazione di linee cellulari umane resistenti a più virus naturali mediante ricodifica del genoma e ha gettato le basi per la formulazione dell'editing composito multiplex del genoma dei mammiferi.

5. Senso del limite e rischi percepiti.

Per vedere dove si possa arrivare, ho considerato due casi reali fra i tanti.

CASO 1: La società Colossal si è assicurata 15 milioni di dollari per il progetto di riportare in vita il mammut.

Colossal è stata fondata da un docente di genetica di Harvard, George Church, e dall'imprenditore informatico Ben Lamm allo scopo di usare la tecnologia CRISPR per salvare le specie esistenti e in via d'estinzione, ma addirittura per la de-estinzione di una specie estinta. La scelta del mammut lanoso era quasi scontata, in parte perché è relativamente facile mettere le mani sul suo DNA, e in parte per il suo valore simbolico. Ma secondo Colossal resuscitare il mammut avrebbe anche conseguenze positive sul clima: l'ambizione è quella di farli

[28] Cfr. D. NORMILE, *Chinese scientist who produced genetically altered babies sentenced to 3 years in jail*, in *Science.org*, 30/12/2019, Consultabile al sito: https://www.science.org/content/article/chinese-scientist-who-produced-genetically-altered-babies-sentenced-3-years-jail.

[29] Cfr. T. VACCARI, *Genetica, è l'era di CRISPR-Cas9: come funziona e le sue applicazioni*, in *Agenda Digitale*. eu,12 Ott 2020. Consultabile al sito: https://www.agendadigitale.eu/cultura-digitale/il-xxi-secolo-sara-lera-di-crispr-come-funziona-e-le-sue-applicazioni/.

[30] L'articolo completo è disponibile in Nature Communications, consultabile al sito: https://www.nature.com/articles/s41467-022-31927-8.

tornare a pascolare nella tundra, dove la loro presenza aiuterebbe il suolo a rigenerarsi [31] . L'idea di de-estinguere una specie per salvare un intero ecosistema è affascinante, ma l'intero progetto di resurrezione del mammut pone una serie di problemi che andrebbero affrontati prima, a partire dal fatto che l'animale che verrebbe riportato in vita non sarebbe un mammut lanoso, ma un ibrido artificiale costruito a partire da un elefante asiatico modificato con geni di mammut lanoso: una nuova specie, la cui introduzione in natura potrebbe avere conseguenze inaspettate e pone seri dubbi etici[32].

CASO 2: modifica genomica per rimuovere mutazioni letali.

L'uso più controverso di CRISPR-Cas9 è la modifica del DNA dell'embrione umano, o, in altre parole, il suo uso per la terapia del genoma germinale. Nel 2015, un gruppo di ricercatori cinesi guidati da Junjiu Huang ha applicato CRISPR-Cas9 per rimuovere una mutazione che causa la β-talassemia, che è una malattia del sangue mortale, dal gene della β-globulina umana (HBB) nella linea germinale degli embrioni umani. In questa ricerca sono stati utilizzati sei embrioni anormali non adatti alla fecondazione in vitro. La mutazione potrebbe essere corretta solo in uno degli embrioni. Sebbene la mutazione possa essere corretta in altri due embrioni, si sono verificati effetti non target in altri geni. Negli altri tre embrioni non è stato possibile correggere la mutazione, sicché le modifiche che si verificano nelle cellule germinali possono essere trasferite alle generazioni future[33].

6. Etica dell'editing genomico (UE).

Come si è visto, l'avvento di nuove tecnologie di editing del genoma come CRISPR/CasX ha aperto nuove dimensioni su come siano possibili gli interventi genetici nel nostro mondo. Perciò l'European Group on Ethics (EGE/GEE) della Commissione Europea ha recentemente affrontato le profonde questioni etiche analizzando vari campi di applicazione, dalla salute umana alla sperimentazione animale, dall'allevamento del bestiame alla varietà delle colture e alle spinte genetiche.

Nel suo documento Ethics of Genome Editing [34], il Gruppo identifica le questioni di fondo e generali, tra cui i diversi significati che dovrebbero essere attribuiti all'umanità, alla naturalezza o alla diversità. Ciò consente di trarre conclusioni che forniscono prospettive panoramiche che integrano analisi più ristrette e specifiche per ogni area.

Allo stesso modo, l'EGE si occupa della dimensione globale dell'editing del

[31] Cfr. G. FERRARI, *La start-up che vuole resuscitare i mammut*, in *Focus*, 19 settembre 2021. Consultabile al sito: https://www.focus.it/ambiente/animali/start-up-che-vuole-resuscitare-mammut.
[32] *Ibidem*.
[33] Cfr. D. CYRANOSKI, S. REARDON, *Chinese scientists genetically modify human embryos*, in *Nature*, 2015. Consultabile al sito: https://www.nature.com/articles/nature.2015.17378.
[34] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR RESEARCH AND INNOVATION, EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES, *Opinion on the Ethics of Genome Editing*, Publications Office, 2021. Consultabile al sito: https://data.europa.eu/doi/10.2777/659034.

genoma e della sua regolamentazione e formula raccomandazioni con una particolare attenzione al livello internazionale. Le sue principali considerazioni generali sono le seguenti[35]:

• il modo in cui dovrebbe essere regolata la capacità umana di modificare il genoma è strettamente legato alle domande sullo stato dell'umanità nella «natura». Siamo i suoi padroni con il diritto di trasformarla, o siamo una delle tante parti di essa che prosperano tutte in relazione l'una con l'altra? La nostra crescente conoscenza su di esso postula che ce ne prendiamo cura e la proteggiamo dove possiamo? La consapevolezza di posizioni unilaterali, come l'antropocentrismo e lo specismo, può aiutarci ad impegnarci nel dibattito sull'editing del genoma sulla base dei valori della diversità, del rispetto e della responsabilità.

• L'applicazione dell'editing del genoma negli animali umani e non umani solleva interrogativi su ciò che ci definisce come esseri umani e ciò che distingue le specie l'una dall'altra. Il nostro genoma è spesso considerato il fondamento della nostra umanità, fornendoci capacità distinte. Dovremmo, o piuttosto non dovremmo, sperimentare le delineazioni che definiscono e distinguono le specie? Quali rischi e responsabilità comporterebbe? D'altra parte, l'eccezionalismo genetico e il determinismo (l'idea che il genoma svolga il ruolo centrale nel plasmare chi siamo e determini il nostro comportamento) possono impedirci di assumere una prospettiva più olistica sui molti fattori che definiscono noi e le nostre vite, così come altre specie e la loro. La consapevolezza di ciò può aiutarci a mettere in prospettiva l'editing del genoma e i discorsi al riguardo.

• La diversità, la diversità umana e la biodiversità in generale, possono essere influenzate dall'editing del genoma in modi diversi. La tecnologia può sia offrire possibilità di preservare e diversificare le biosfere, sia comportare il rischio di ridurre i pool genetici e, quindi, la diversità, sia in termini biologici che in termini di tipo di diversità socialmente apprezzata. Questo ci impone di riflettere sulle responsabilità dell'uomo nei confronti delle altre specie e del pianeta, soprattutto per quanto riguarda il cambiamento climatico antropogenico; così come nei confronti di altri esseri umani, per quanto riguarda la determinazione di quali tipi di persone una società potrebbe voler avere e quali specifiche variazioni sono o non sono un problema che necessita di una soluzione genetica e tecnologica. Quando si pensa alla diversità e all'editing genomico, bisogna quindi pensare anche alla libertà, all'autonomia e ai rischi di oppressione ed emarginazione.

• L'attenzione al quadro più ampio di questo parere aumenta anche la consapevolezza del rischio che l'editing del genoma possa essere salutato come una soluzione tecnologica per problemi di natura sociale. Un approccio che non considera l'etica e la governance dell'editing del genoma in un modo specifico della tecnologia ci consente di individuare le questioni sociali più ampie nel regno di quali tecnologie, o sistemi socio-tecnici, possono avere un impatto. In quale mondo vogliamo vivere e quale ruolo possono svolgere le tecnologie nel renderlo realtà?

• I dibattiti sull'editing del genoma spesso si concentrano sulla questione

[35] *Ibidem*, 4-5.

delle condizioni che lo renderebbero «abbastanza sicuro» per l'applicazione. Il documento richiama l'attenzione sull'importanza di sfumare e resistere a tale inquadramento: al contrario, l'etica dovrebbe servire ad affrontare ampie questioni di governance su come le tecnologie possono servire i nostri obiettivi e valori comuni, e non limitarsi a fornire un «ultimo passo» di «compensazione etica» di una tecnologia. La sicurezza, per essere un concetto sicuro, deve essere inquadrata nel suo senso più ampio, includendo le dimensioni psicologica, sociale e ambientale, nonché le domande su chi decide cosa è sufficientemente sicuro e attraverso quali processi.

• Con la crescente adozione dell'editing del genoma, si affermava che gli scienziati non solo erano in grado di leggere il «Libro della vita», ma anche di scriverlo e modificarlo. Le parole scelte per descrivere una nuova tecnologia hanno un impatto sul discorso che la riguarda: modellano il modo in cui lo percepiamo e ci impegniamo in dibattiti su di esso, inquadrano le domande che gli studiosi pongono su di esso e indagano, influenzano il modo in cui i responsabili politici rispondono ad esso e alle questioni etiche.

Sulla base dei molteplici aspetti e delle potenziali implicazioni dell'editing genomico nell'uomo, negli animali e nelle piante, inclusa una particolare attenzione ai gene drive[36] e rilevando che le raccomandazioni non devono essere viste come approvazione di specifiche tecnologie, applicazioni o aree di applicazione, il GEE raccomanda soprattutto di:

- Promuovere una deliberazione sociale ampia e inclusiva sull'editing del genoma in tutti i campi di applicazione e di portata globale:
  il dibattito pubblico dovrebbe affrontare il modo in cui esso è percepito e valutato dai cittadini, quali opinioni, speranze e paure hanno, in tutti i campi di applicazione e se la modifica del genoma germinale è considerata necessaria e/o accettabile, o lo sarebbe in quali condizioni[37].

- Sviluppare linee guida internazionali e rafforzare nazionali, regionali e strumenti di governance globale:
  l'EGE raccomanda che la Commissione Europea, insieme a organismi internazionali appropriati che stanno già lavorando in questo settore (in particolare l'OMS), sviluppino standard e linee guida per l'uso etico e sicuro dell'editing del genoma in tutte le aree di applicazione[38].

[36] «Un gene drive è un tipo di tecnica di ingegneria genetica che modifica i geni in modo che non seguano le regole tipiche dell'ereditarietà. I gene drive aumentano notevolmente la probabilità che una particolare serie di geni venga trasmessa alla generazione successiva, consentendo ai geni di diffondersi rapidamente in una popolazione e di ignorare la selezione naturale. Grazie a CRISPR-Cas9, la tecnologia di editing genetico sfruttata dai batteri, i gene drive stanno diventando più facili da costruire per i ricercatori. (..) Un gene drive è costituito da tre componenti chiave: il gene che vuoi diffondere; l'enzima Cas9 che può tagliare il DNA e CRISPR, una sequenza di DNA che identifica dove l'enzima dovrebbe tagliare. Il materiale genetico che codifica per questi tre elementi viene inserito nel DNA di un animale, al posto del gene naturale che si desidera sostituire in entrambi i cromosomi», cfr. D. COFFEY, *What is a gene drive?* in *LifeScience*, April 17, 2020. Consultabile al sito: https://www.livescience.com/gene-drive.html.
[37] EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES, o*p.cit.*, 84.
[38] *Ibidem*, 86.

7. Raccomandazioni e quadro per la governance (OMS).

Per quanto riguarda l'OMS, due nuovi rapporti pubblicati il 12/7/2021 forniscono le prime raccomandazioni globali per aiutare a stabilire l'editing del genoma umano come strumento per la salute pubblica, con particolare attenzione alla sicurezza, all'efficacia e all'etica.

I nuovi rapporti sono il risultato della prima ampia consultazione globale sull'editing del genoma umano somatico, germinale ed ereditabile. La consultazione, durata oltre due anni, ha coinvolto centinaia di partecipanti in rappresentanza di diverse prospettive da tutto il mondo, inclusi scienziati e ricercatori, gruppi di pazienti, leader religiosi e popolazioni indigene[39].

I potenziali vantaggi dell'editing del genoma umano includono diagnosi più rapide e accurate, trattamenti più mirati e prevenzione delle malattie genetiche. Le terapie geniche somatiche, che comportano la modifica del DNA di un paziente per trattare o curare una malattia, sono state utilizzate con successo per affrontare l'HIV, l'anemia falciforme e l'amiloidosi da transtiretina. La tecnica potrebbe anche migliorare notevolmente il trattamento per una varietà di tumori.

Tuttavia, esistono alcuni rischi, ad esempio, con l'editing del genoma umano ereditabile e della linea germinale che alterano il genoma degli embrioni umani e potrebbero essere trasmessi alle generazioni successive, modificando i tratti dei discendenti[40].

Il quadro di governance sull'editing del genoma umano [41], insieme alle raccomandazioni del Comitato[42], formano un insieme di due pubblicazioni che forniscono consigli e raccomandazioni sui meccanismi di governance istituzionali, nazionali, regionali e globali appropriati per l'editing del genoma umano. Un documento di posizione fornisce una sintesi.

Il quadro di governance

- attinge dalle buone pratiche nella governance delle tecnologie emergenti e le applica specificamente;
- implementabile in diversi contesti, è finalizzato ad aiutare coloro che hanno il compito di rafforzare le misure di vigilanza, indipendentemente dal fatto che questo sia a livello istituzionale, nazionale, regionale o internazionale;
- identifica valori e principi che aiutano a spiegare perché potrebbero essere necessarie tali misure e in che modo coloro che sono incaricati di rivederle o rafforzarle possono intraprendere tale compito;
- propone sette scenari per dimostrare come le varie componenti si uniscono nella pratica;
- identifica una serie di considerazioni per la corretta attuazione delle

[39] Cfr. WHO, *WHO issues new recommendations on human genome editing for the advancement of public health*, News release 12 July 2021. Consultabile al sito: https://www.who.int/news/item/12-07-2021-who-issues-new-recommendations-on-human-genome-editing-for-the-advancement-of-public-health.
[40] *Ibidem.*
[41] Cfr. WHO, *Human genome editing: a framework for governance*, Technical document 12 July 2021. Consultabile al sito: https://www.who.int/publications/i/item/9789240030060.
[42] Cfr. WHO, *Human genome editing: recommendations*, Technical document 12 July 2021. Consultabile al sito: https://www.who.int/publications/i/item/9789240030381.

misure.

Le raccomandazioni si concentrano sui miglioramenti a livello di sistema necessari per creare capacità in tutti i paesi per garantire che l'editing del genoma umano sia utilizzato in modo sicuro, efficace ed etico.

7.1 Ricerca sull'editing del genoma umano attuale, potenziale e speculativa (OMS).

Il Comitato riconosce che la ricerca attuale, potenziale e speculativa sull'editing del genoma umano (fig. 12) andrà oltre i confini nazionali, così come i possibili effetti sulla società. Ciò vale anche per l'editing del genoma umano somatico, germinale ed ereditabile, sebbene quest'ultimo sia generalmente considerato di maggiore interesse etico[43].

Pertanto, la *governance* per questa tecnologia è necessaria a livello nazionale (politiche interne comprese leggi, regolamenti e linee guida) e a livello transnazionale (comprese convenzioni e trattati, nonché coordinamento del movimento transfrontaliero di ricercatori, medici (inclusi clinici o scienziati medici) e partecipanti alla ricerca o pazienti).

Alcune delle strutture e dei processi di *governance* necessari esistono già.

Potrebbe essere necessario rafforzarli o modificarli; laddove mancano tali strutture e processi, potrebbe essere necessario colmare le lacune. Il Comitato incoraggia ma non può imporre un approccio globale coordinato.

In assenza di un tale approccio, il Comitato riconosce che giurisdizioni diverse, con regimi politici e contesti culturali, storici e religiosi diversi, probabilmente preferiranno approcci normativi diversi.

[43] Cfr. WHO, *Human genome editing: a framework for governance*, *op. cit.*, 5.

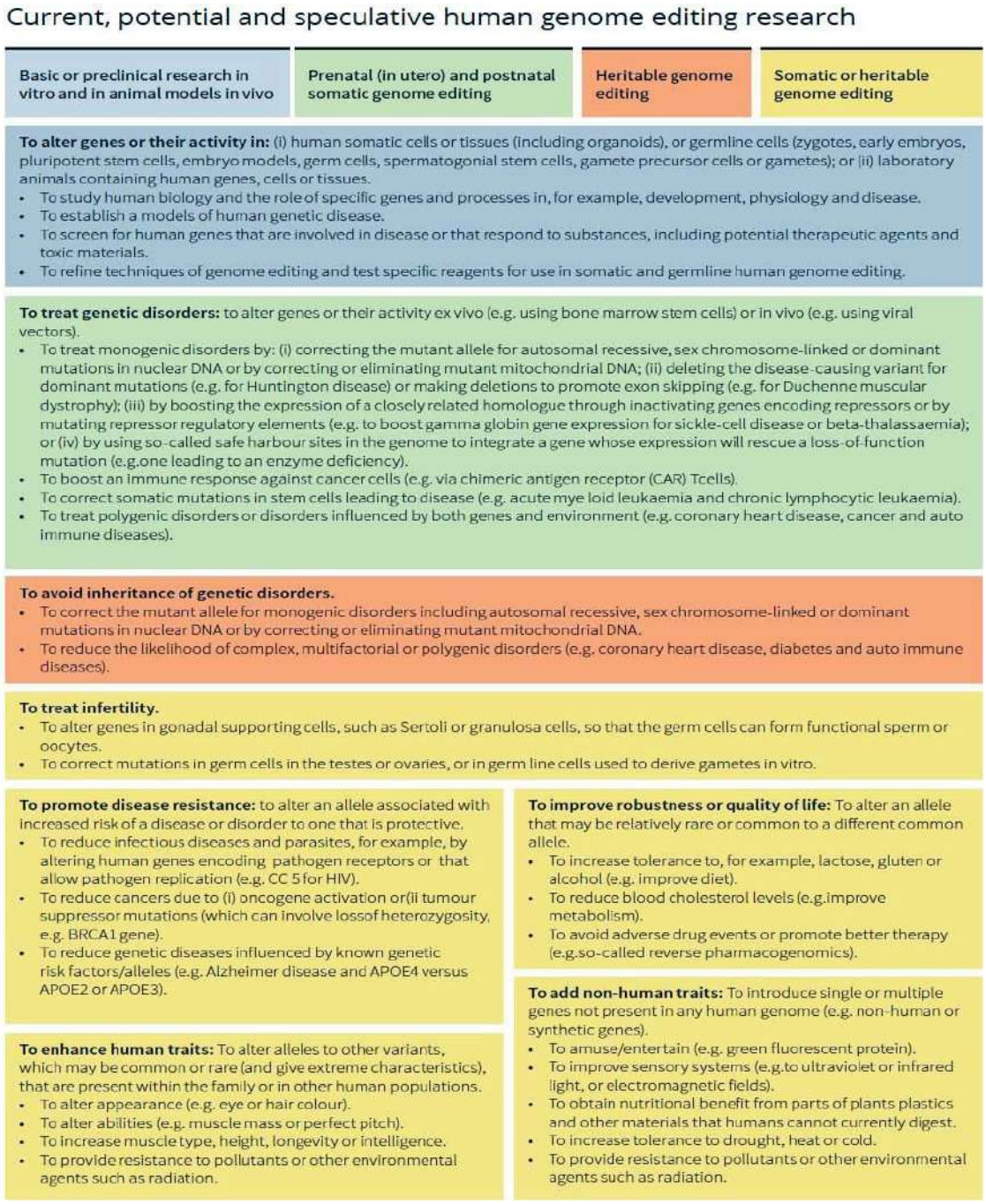


Fig. 12: Ricerca attuale, potenziale e speculativa sull'editing del genoma umano. CAR: recettore chimerico dell'antigene; AML: leucemia mieloide acuta; CLL: leucemia linfatica cronica; CCR5: recettore C-C per le chemochine di tipo 5); APOE: apolipoproteina E (fonte WHO, *Human genome editing: a framework for governance*, *op.cit.*).

• Gli esempi sono descrittivi e non normativi, cioè intendono semplicemente fornire una panoramica di ciò che potrebbe essere possibile con la scienza.
• Esisteranno chiare differenze nella complessità della scienza e qualsiasi considerazione etica a seconda che il tentativo riguardi la modifica di uno o più geni. Con le attuali tecniche di modifica del genoma, l'alterazione simultanea di

più geni aumenterebbe notevolmente la probabilità, ad esempio, di eventi errati sul bersaglio e fuori bersaglio e riarrangiamenti cromosomici, in modo tale che i rischi superino i potenziali benefici.
• In futuro, alcune applicazioni dell'editing del genoma umano potrebbero comportare l'uso di tecniche per aumentare i tassi di ereditarietà, ad esempio utilizzando tecnologie di gene-drive per consentire agli esseri umani di far fronte a cambiamenti climatici estremi.
• Esistono anche potenziali applicazioni a duplice uso; ad esempio, l'editing del genoma umano per dare resistenza agli inquinanti chimici o alle radiazioni per i viaggi spaziali potrebbe avere anche applicazioni militari rispetto alla resistenza alle armi chimiche o nucleari.
• È importante sottolineare che il Comitato non approva né suggerisce che alcun ricercatore lavori per questi potenziali usi. Piuttosto, il Comitato sostiene l'introduzione e l'attuazione di meccanismi di governance nazionali e transnazionali in grado di esaminare e valutare efficacemente non solo le prove scientifiche e cliniche, ma anche le opinioni e i valori etici e sociali pertinenti.

7.2 Ammissibilità editing genoma ereditabile (x riproduzione) per regione OMS.

Un'indagine del 2020 sui documenti rilevanti per la politica (legislazione, regolamenti, linee guida, codici e trattati internazionali) per l'editing del genoma umano ereditabile (per la riproduzione) (figura 13) conferma che strutture e processi di governance esistono già in molte giurisdizioni[44].

Table 2. Existence of policies on and permissibility of heritable human genome editing in selected countries (for reproduction), by World Health Organization region

Region (no. of countries[a])	Countries that permit, no.	Countries that prohibit, no.	Countries that prohibit with exceptions, no.	Countries that are indeterminate[10], no.	Countries with no relevant information available, no.
Africa (13)	0	5	0	1	7
Americas (17)	0	8	2	0	7
Eastern Mediterranean (10)	0	8	1	0	1
Europe (46)	0	41	2	1	2
South-East Asia (2)	0	2	0	0	0
Western Pacific (8)	0	6	0	1	1
Total (96)	0	70	5	3	18

Fig. 13: Esistenza di politiche e ammissibilità dell'editing del genoma umano ereditabile in paesi selezionati (per la riproduzione), per regione dell'Organizzazione mondiale della sanità (fonte WHO, *Human genome editing: a framework for governance*, *op.cit.*).

[44] Cfr. WHO, *Human genome editing: a framework for governance*, *op.cit.*, 9.

Peraltro, a livello di totali, la stragrande maggioranza di Paesi (70 su 96) proibisce questo tipo di editing, mentre per ben 18 di loro non risultano disponibili informazioni rilevanti.

Il Comitato conclude che l'innovazione nell'editing del genoma umano dovrebbe essere guidata dai benefici previsti per gli individui e la società in termini di salute umana e benessere collettivo. A sua volta, una buona governance delle tecnologie emergenti dovrebbe garantire che siano in atto protezioni adeguate per le persone che hanno più bisogno dei potenziali benefici e per le persone che hanno maggiori probabilità di subire i potenziali danni, che possono essere o meno le stesse persone. L'equità di accesso e di beneficio dall'editing del genoma umano è fondamentale per il Comitato[45].

8. (New) life design. L'uomo come fulcro di un 'impatto' sostenibile.

Il progresso della scienza e della tecnologia nell'ultimo mezzo secolo ha aperto orizzonti senza precedenti. Il mondo si sta trasformando, tutto sta cambiando, non solo in termini di modo in cui viviamo, ma anche in termini di durata. Con la scienza e la tecnologia che spingono sempre più indietro la frontiera della morte, è possibile che la «morte della morte» si realizzi in un lontano futuro? (Wood, 2016). C'è un distinto gruppo di pensatori che proclamano l'avvento della Singolarità, dove l'evoluzione dell'*Homo sapiens* sarà diretta da noi stessi. La Singolarità si riferisce al momento in cui tutti i progressi della scienza e della tecnologia causeranno cambiamenti biologici, culturali e sociali inimmaginabili, impossibili da prevedere o comprendere prima di questo evento. Nella Singolarità non ci sarà distinzione tra umani e macchine, o tra mondo fisico e virtuale. Raymond Kurzweil (2005) suggerisce di riflettere sul modo in cui la tecnologia si è evoluta negli ultimi 100 anni e di proiettarla nel futuro: ci sarà una crescita esponenziale di diverse forme di progresso tecnologico che potrebbe portarci a vincere la paura di una morte inevitabile eliminando l'inevitabilità della morte stessa. Molti dei difensori della Singolarità in genere sostengono qualche versione del transumanesimo[46].

Queste visioni contraddittorie delle influenze antropogeniche dividono l'opinione scientifica sul fatto che i cambiamenti indotti dall'uomo [47] siano

---

[45] Cfr. WHO, *Human genome editing: a framework for governance, op.cit.*, 9.

[46] Cfr. P. GARCÍA-BARRANQUERO, *Transhumanist immortality: Understanding the dream as a nightmare*, in *Scientia Et Fides*, 2021, 9(1), 177–196. Consultabile al sito: https://apcz.umk.pl/SetF/article/view/SetF.2021.006/28742, 178.

[47] Cfr. «La legge dei ritorni accelerati (Kurzweil, 2001) prevede che a un certo punto nel tempo, probabilmente entro il prossimo secolo (al tasso di innovazione odierno possiamo aspettarci di vedere un secolo di progresso in circa 25 anni), l'umanità incontrerà una singolarità tecnologica. Questa singolarità presuppone che il tasso di crescita e innovazione tecnologica supererà le capacità umane di controllarlo e comprenderlo. Se, tuttavia, dovessimo cercare di "vedere" oltre la singolarità quando si è verificata, avremmo bisogno di una forma di intelligenza superiore alla nostra attuale intelligenza biologica. L'ipotesi più convenzionale che descrive la nascita di una tale superintelligenza ruota attorno all'evoluzione dell'IA, vale a dire da algoritmi "ristretti" ad Intelligenza Generale Artificiale (AGI). Una volta raggiunta l'AGI, seguirà necessariamente la superintelligenza: è probabile che le velocità di elaborazione computazionale e la capacità di memorizzazione delle informazioni di un AGI superino quelle del cervello umano. Pertanto, l'acquisizione e l'apprendimento delle informazioni AGI vedrebbero un miglioramento esponenziale nel tempo, dando vita alla fine a una superintelligenza computazionale. Un altro modo in cui potremmo ottenere la superintelligenza è attraverso l'uso di tecnologie di editing genetico, come CRISPR, e miglioramento biologico. Potremmo scoprire che ci sono geni specifici che sono alla base dello sviluppo di

positivi poiché molti organismi sono favoriti dalla selezione artificiale o se la Terra si stia avvicinando alla sua sesta estinzione di massa (Dalby 2016). L'Antropocene[48] è sicuramente un periodo di processi dirompenti di massa su un pianeta che è già stato sostanzialmente alterato dagli esseri umani (Hamilton 2016), mentre le pressioni demografiche sugli ecosistemi terrestri sono in aumento esponenziale (Deb et al. 2018). È quindi inconfutabile che la distribuzione delle specie, la ricchezza delle specie e i nuovi organismi divergeranno enormemente dalla biodiversità contemporanea nell'Antropocene.

I valori culturali umani e altre strutture sociali portano a modelli comportamentali (sia degli individui che dei gruppi sociali) che si tradurranno in drastici cambiamenti ambientali (Ellis e Trachtenberg 2014). Alcuni effetti antropogenici sono ora facilmente visibili, come l'estinzione dell'habitat (Ghosh et al. 2013) e la produzione di ~ 30 trilioni di tonnellate (Tt) di materiali e artefatti della tecnosfera (Zalasiewicz et al. 2017). Alcune delle aree alterate dagli esseri umani sono considerate nuovi ecosistemi, noti come biomi antropogenici (ad esempio, anthromes; Ellis 2011).

L'Antropocene è modulato dalla cultura e dalla tecnologia umana, e le estinzioni e i cambiamenti dell'habitat si stanno verificando a ritmi incontrollati e accelerati con conseguenze inaspettate (Barnosky et al. 2012; Steffen et al. 2015).

L'ipotesi dell'antropocene bioevolutivo [49] riconosce i nuovi organismi e l'umanità come le nuove forze motrici della biodiversità (fig.14). Il futuro della biodiversità è difficilmente prevedibile con precisione, ovviamente, ma nuovi organismi, come le specie aliene e ibride e gli OGM, svolgeranno verosimilmente un ruolo chiave nelle interazioni biologiche, avranno capacità

---

vari tratti cognitivi associati all'intelligenza umana in quanto ci sono geni che determinano la crescita muscolare, la predisposizione a determinate malattie, l'altezza, il colore degli occhi, ecc. Una volta scoperti questi geni specifici, possiamo selezionare per loro in embrioni umani e curare artificialmente una classe di esseri umani biologici che rappresentano l'apice intellettuale dell'umanità. Mentre il potenziamento biologico genera una serie di problemi etici, principalmente legati a chi potrebbe accedere a tali trattamenti e se i programmi genomici sarebbero o meno sponsorizzati dallo stato, questo approccio potrebbe essere necessario all'alba della singolarità tecnologica per garantire che gli esseri umani stiano al passo con innovazione» in S. CADARIU, *The Law of Accelerating Returns, Superintelligence and The Technological Singularity*, in *AI Time Journal*, Updated October 6, 2022. Consultabile al sito: https://www.aitimejournal.com/the-law-of-accelerating-returns-superintelligence-and-the-technological-singularity.

[48] Cfr. «L'Antropocene, come dice il nome stesso coniato nel 2000 dal chimico e premio Nobel olandese Paul Crutzen, è l'era dell'uomo, quel periodo in cui gli esseri umani hanno un impatto enorme su tutto l'ecosistema terrestre. (..) Già nel 1864 George Perkins Marsh notò nel saggio L'uomo e la natura la superficie terrestre modificata per opera dell'uomo che gli esseri umani stavano condizionando negativamente la natura e il pianeta, mettendo a rischio la propria sopravvivenza. Poco dopo, nel 1873, il geologo italiano Antonio Stoppani teorizzò per la prima volta che l'uomo aveva "una nuova forza tellurica con potenza e universalità comparabile con le grandi forze del pianeta" e chiamò questa epoca "era antropozoica". (..) Gli studiosi prevedono che in futuro, a meno che una catastrofe naturale non interrompa il dominio dell'uomo, gli impatti sull'ambiente circostante continueranno a farsi sentire. La sensibilità delle nuove generazioni per uno sviluppo sostenibile potrà dare una mano a limitare questi impatti, ma per il momento sembra difficile che possa invertire la rotta», come si legge nell'analisi di PICTET, *Antropocene: benvenuti nell'era dell'umanità che domina la natura*, novembre 2019. Consultabile al sito: https://am.pictet/it/blog/articoli/sviluppo-sostenibile/antropocene-benvenuti-nell-era-dell-umanita-che-domina-la-natura.

[49] Cfr. P.J.F. PENA RODRIGUES, C.F. LIRA, *The Bio-Evolutionary Anthropocene Hypothesis: Rethinking the Role of Human-Induced Novel Organisms*, in *Evolution. Biol Theory*, 2019, 14, 141–150. Consultabile al sito: https://iiraorg.com/2021/04/19/the-bio-evolutionary-anthropocene-hypothesis-rethinking-the-role-of-human-induced-novel-organisms-in-evolution/.

evolutive divergenti o creeranno pressioni diverse sugli ecosistemi naturali e antropizzati e altereranno la distribuzione, la ricchezza e i modelli ecologici della biodiversità locale e globale e condurranno a percorsi evolutivi nuovi e inaspettati.

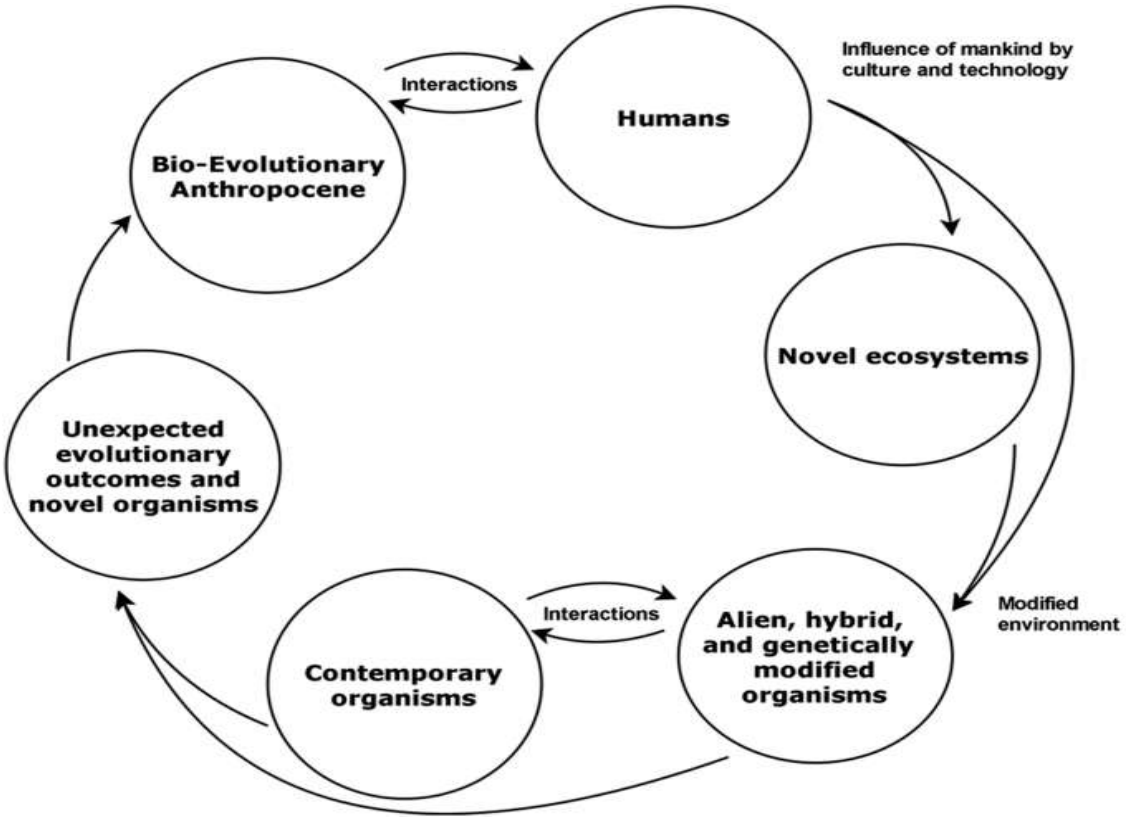


Fig. 14: l'Antropocene bioevolutivo e le sue complesse interazioni (fonte Pena Rodrigues, cit.).

In realtà, anche dal punto di vista della salute pubblica, è noto che le scelte individuali dipendono dal contesto poiché molti fattori socioeconomici influenzano la salute. La responsabilità è quindi intesa come una «responsabilità politica collettiva» (Grinbaum e Groves, 2013). Di conseguenza, sia che implichi l'obbligo di proteggere e migliorare la salute e il benessere della popolazione, la responsabilità per i servizi medici resi o le scelte individuali, la nozione di responsabilità nella salute è plurale[50].

Esistono molte interpretazioni dei pilastri/fattori essenziali che creano la sostenibilità. In quella di *FutureLearn* la sostenibilità è suddivisa in tre pilastri, rappresentati da un diagramma di Venn e definiti come protezione ambientale, fattibilità economica e uguaglianza sociale: i tre pilastri devono essere in equilibrio affinché il sistema sia considerato sostenibile (fig. 15).

[50] Cfr. O. DEMERS-PAYETTE, P. LEHOUX, G. DAUDELIN, *Responsible research and innovation: a productive model for the future of medical innovation*, in *Journal of Responsible Innovation*, 2016, 3:3, 188-208. Consultabile al sito: https://www.tandfonline.com/doi/full/10.1080/23299460.2016.1256659 .

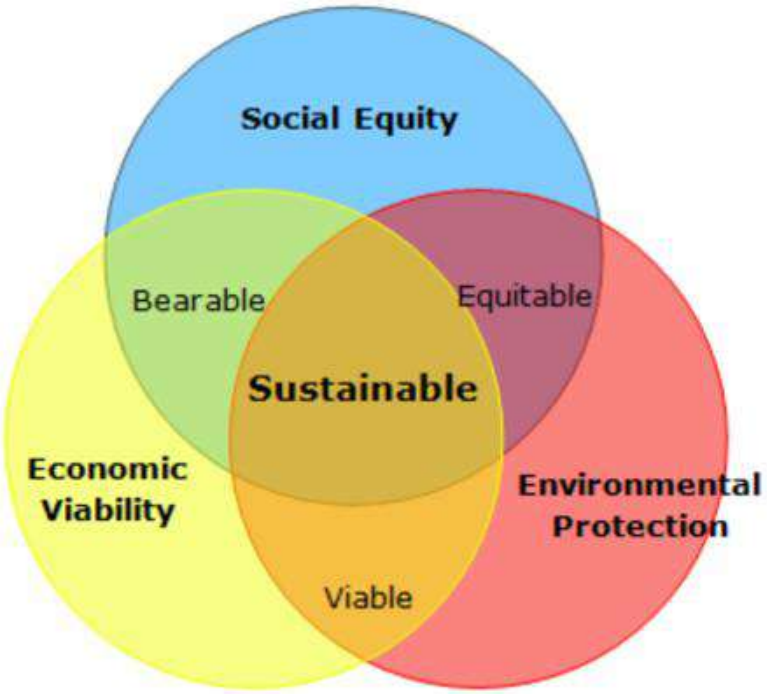


Fig. 15: I tre pilastri della sostenibilità (fonte: https://www.futurelearn.com/info/courses/sustainability-society-and-you/).

Produttori e aziende hanno un altro modo di vedere le cose, ma indipendentemente dall'interpretazione, l'obiettivo principale della sostenibilità rimane chiaro: se vogliamo salvare noi stessi e preservare il nostro pianeta, dobbiamo tutti essere molto più sostenibili in tutto ciò che facciamo.

La più accreditata definizione di sviluppo sostenibile è stata elaborata nel 1987 dalla Commissione Mondiale sull'Ambiente e lo Sviluppo all'interno del noto Rapporto Brundtland «Our Common Future»: «lo sviluppo sostenibile, lungi dall'essere una definitiva condizione di armonia, è piuttosto processo di cambiamento tale per cui lo sfruttamento delle risorse, la direzione degli investimenti, l'orientamento dello sviluppo tecnologico e i cambiamenti istituzionali siano resi coerenti con i bisogni futuri oltre che con gli attuali».

Sviluppo sostenibile e sostenibilità sono concetti trasversali che implicano la coesistenza di benessere economico, sociale e ambientale. Infatti, sviluppo sostenibile significa vivere e migliorarsi a livello sociale ed economico nei limiti consentiti dal nostro Pianeta, rispettando gli equilibri della natura e le sue capacità di rigenerarsi e assorbire le modifiche apportate dalle nostre attività produttive.

La sostenibilità attraverso la tecnologia è stata salvifica negli ultimi anni, ma l'adozione deve avvenire a livello mondiale affinché la nostra specie sia

veramente sostenibile. Allo stesso tempo, le tecnologie e le pratiche devono continuare a migliorare[51].

9. Innovazione sostenibile. Bridging the sustainability gap.

Secondo la Commissione Europea, la ricerca e l'innovazione responsabili (RRI) costituiscono un approccio che anticipa e valuta le potenziali implicazioni e le aspettative della società per quanto riguarda la ricerca e l'innovazione, con l'obiettivo di promuovere la progettazione di ricerca e innovazione inclusive e sostenibili[52].

La RRI è stata utilizzata nel programma Horizon 2020 per raggruppare concetti trasversali di aspetti sociali della scienza e dell'innovazione nell'ambito dell'obiettivo dell'agenda Scienza con e per la società (SwafS).

Nella teoria del quadro elicoidale dell'innovazione (Etzkowitz e Leydesdorff, 2012), utilizzata nell'economia dell'innovazione e nelle teorie della conoscenza, ogni settore è rappresentato da un cerchio (elica), e le sovrapposizioni mostrano le interazioni.

RRI può assistere nella gestione delle relazioni tra i diversi gruppi di stakeholder della quadrupla elica (Quadruple Helix[53]), ad esempio tra la società civile e coloro che gestiscono programmi di R&I. È una soluzione efficace che consente un processo trasparente e interattivo in cui attori sociali e diversi, responsabili e non responsabili dell'innovazione, diventano reciprocamente responsabili del processo di innovazione. In tal modo genera «impatto» positivo, consentendo una sufficiente incorporazione dei progressi scientifici e tecnologici nella nostra società (fig.16).

[51] Cfr. A. KROSOFSKY, *What Are the Six Factors of Sustainability, and How Can We Adhere to Them?* in *Greenmatters*, March 12 2021. Consultabile al sito: https://www.greenmatters.com/p/six-factors-of-sustainability.

[52] Cfr. J. PECKHAM, *What is responsible innovation, and why should tech giants take it seriously?* in *Techradar*, August 27, 2018, Consultabile al sito: https://www.techradar.com/news/what-is-responsible-innovation-and-why-should-tech-giants-take-it-seriously.

[53] «Il modello Quadruple Helix è stato originariamente concettualizzato da Elias Carayannis e David Campbell come una spirale con quattro filamenti. Il nostro adattamento osserva l'elica dall'alto. Dimostra chiaramente che i quattro componenti fondamentali di un sistema di innovazione - università, industria, governo e società - non sono coinvolti in relazioni unidirezionali push-pull, ma piuttosto in interazioni multistrato, dinamiche e bidirezionali. Ciò evidenzia il ruolo della società come attore principale nei sistemi di innovazione nazionali, nonché l'importanza di integrare attivamente il pubblico nei progetti di innovazione», come si legge in F. SCHÜTZ, M. L. HEIDINGSFELDER, M. SCHRAUDNER, *Co-shaping the Future in Quadruple Helix Innovation Systems: Uncovering Public Preferences toward Participatory Research and Innovation*, in *She Ji: The Journal of Design, Economics, and Innovation*, 2019, 5, 2, 128-146. Consultabile al sito: https://www.sciencedirect.com/science/article/pii/S2405872618301394.

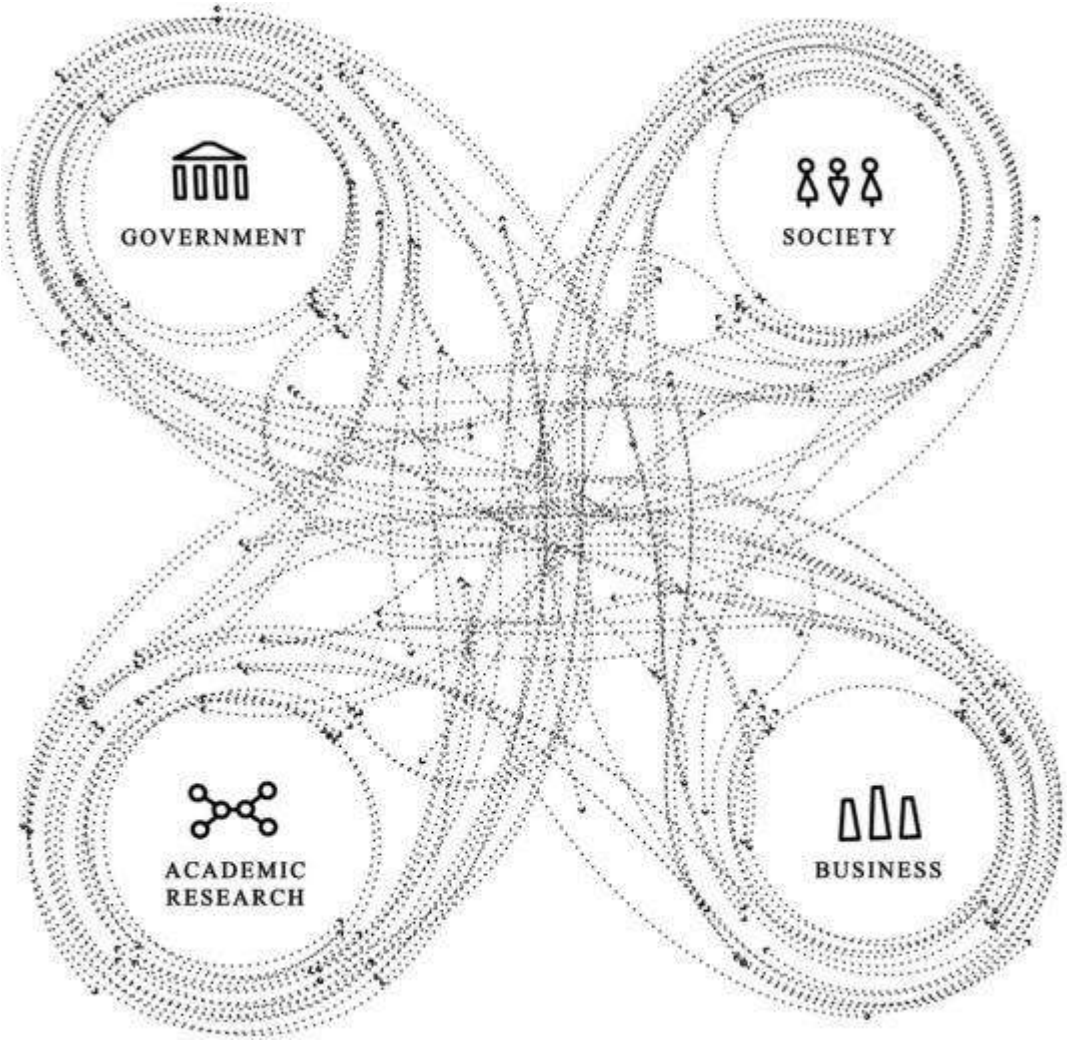


Fig. 16: Il modello a quadrupla elica adattato da Fraunhofer (2016), originariamente sviluppato da Carayannis e Campbell (2009) (Copyright © 2015 Fraunhofer).

RRI supporta strategie avanzate di Ricerca & Innovazione (R&I). Per contribuire a integrarla nel modo in cui lavorano ricercatori e innovatori, sono stati definiti i cinque temi chiave che i responsabili politici devono prendere in considerazione, indicati come le chiavi RRI[54]:

- Parità di genere: affronta il divario tra donne e uomini, ad esempio garantendo che le dimensioni di genere siano prese in considerazione nella R&I, nel processo decisionale, nell'assegnazione dei finanziamenti e nella composizione di gruppi e organizzazioni.
- Accesso aperto: tentativi di rendere la scienza trasparente e accessibile. Sottolinea che i risultati della ricerca finanziata con fondi pubblici (pubblicazioni e dati) dovrebbero essere resi liberamente accessibili per l'uso pubblico online.

[54] Cfr. https://tetrris.eu/what-is-responsible-research-and-innovation-rri/, progetto che ha ricevuto finanziamenti dal programma di ricerca e innovazione Horizon 2020 dell'Unione Europea nell'ambito della convenzione di sovvenzione nº 872550.

- Coinvolgimento dei cittadini: sottolinea che il pubblico, comprese le organizzazioni della società civile, dovrebbe partecipare congiuntamente al processo di ricerca e innovazione, piuttosto che i tradizionali pilastri di ricercatori, industria e responsabili politici che tradizionalmente lo hanno alimentato.
- Educazione scientifica: affronta la sfida di preparare meglio i futuri ricercatori e altri attori sociali, fornendo loro gli strumenti e le conoscenze necessarie per partecipare pienamente al processo di ricerca e innovazione, nonché fornendo ai cittadini gli strumenti per prendere parte alla formazione delle politiche scientifiche.
- Etica: richiede alla R&I il rispetto dei diritti fondamentali e dei più elevati standard etici al fine di garantire una maggiore rilevanza sociale e una maggiore accettazione dei risultati della ricerca e dell'innovazione.

Un'altra autorevole definizione di innovazione responsabile ha solitamente incluso quattro dimensioni; anticipazione, riflessività, inclusione e reattività (fig. 17)[55].

[55] Cfr. P. MACNAGHTEN, *The Making of Responsible Innovation*, in *Researchgate.net*, 2020. Consultabile al sito: https://www.researchgate.net/figure/Four-dimensions-of-responsible-innovation_tbl1_342714845.

Dimension	Indicative techniques and approaches	Objectives of techniques and approaches
Anticipation	Foresight Horizon scanning Scenarios Technology assessment Risk assessment Life cycle assessment Vision assessment Socio-literary techniques	Identification and appraisal of possible and plausible impacts of research and innovation pathways
Inclusion	Consensus conferences Citizen assemblies Focus groups Science shops Deliberative mapping Multi-stakeholder partnerships Lay membership of expert bodies User-centred design Open innovation	Public and stakeholder deliberation on the visions, impacts and broader socio-economic questions associated with research and innovation
Reflexivity	Multidisciplinary collaboration and training Embedded social scientists and ethicists in laboratories Midstream modulation Ethical technology assessment	Socio-technical integration and interdisciplinarity in research and innovation practice
Responsiveness	Constitution of grand challenges and thematic research programmes Regulation and standards Open access and other mechanisms of transparency Niche management Value-sensitive design Moratoriums Stage-gates Codes of conduct	Policy and governance mechanisms for the practical implementation of responsible innovation

Fig. 17: le quattro dimensioni dell'innovazione responsabile (fonte Macnaghten, *op. cit.*).

Il quadro dell'elica dell'innovazione quintupla descrive le interazioni università-industria-governo-pubblico-ambiente nell'ambito di un'economia della conoscenza (fig.18)[56].

La struttura dell'elica quintupla può essere descritta in termini di modelli di conoscenza che estende e di cinque sottosistemi (eliche) che incorpora; in un modello a quintupla elica, la conoscenza e il know-how vengono creati e trasformati e circolano come input e output in un modo che influisce sull'ambiente naturale, come l'innovazione per affrontare lo sviluppo sostenibile[57].

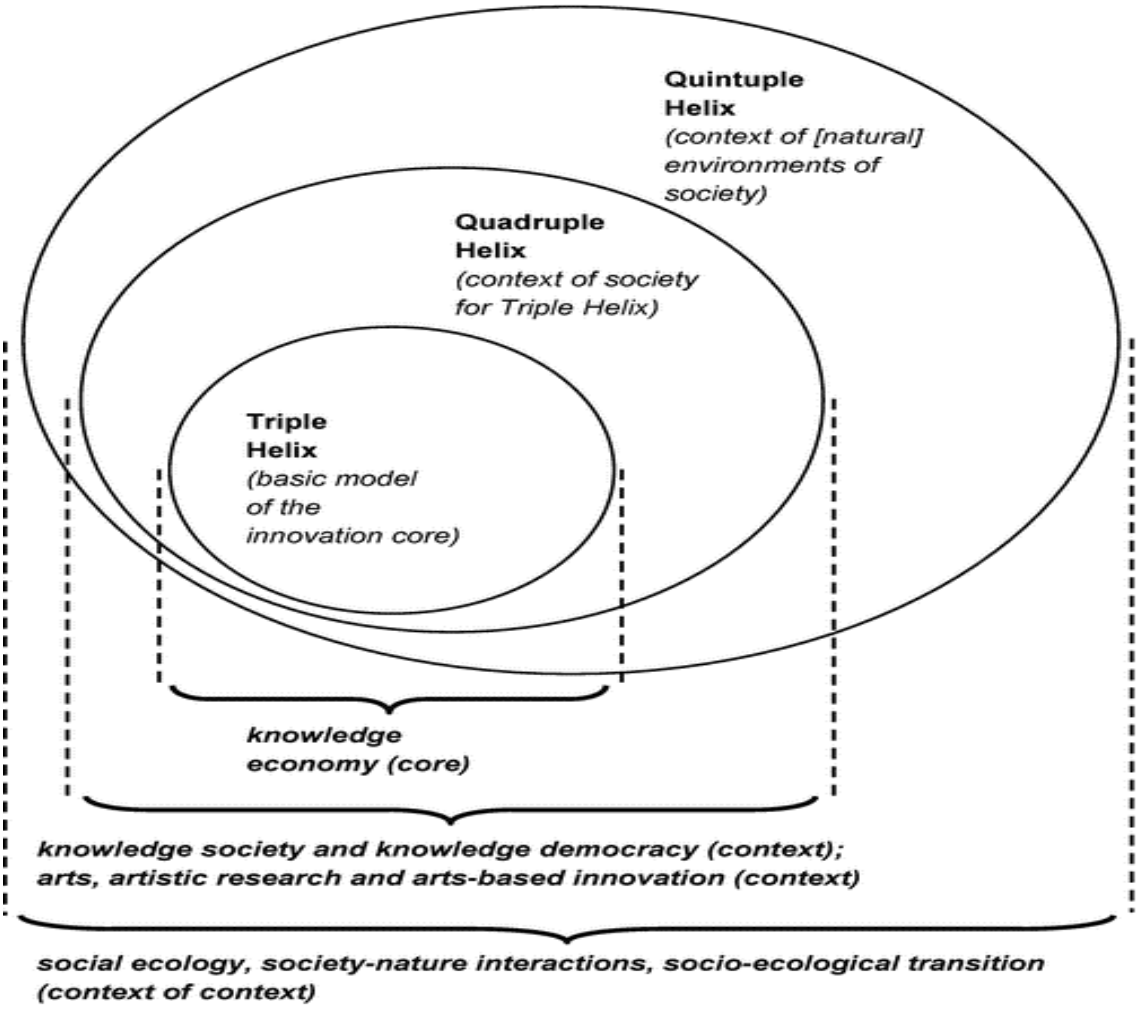


Fig. 17: il quadro dell'elica dell'innovazione quintupla descrive le interazioni università-industria-governo-pubblico-ambiente nell' economia della conoscenza (fonte Abu Bakar, *op. cit.*).

[56] Cfr. N. A. ABU BAKAR, *Quadruple and quintuple innovation helix framework*, in *People.utm*, May 10, 2020. Consultabile al sito: https://people.utm.my/nurazaliah/2020/05/10/quadruple-and-quintuple-innovation-helix-framework/.
[57] *Ibidem.*

La R&I ha migliorato il nostro mondo e le nostre vite in molti modi. Tuttavia, accanto all'impatto positivo sul benessere materiale e fisico della società, la scienza e la tecnologia talvolta creano nuovi rischi e dilemmi etici. RRI risponde a queste sfide coinvolgendo tutti gli attori (da ricercatori e innovatori a governi e cittadini) attraverso metodologie inclusive e partecipative. Per essere efficace, la partecipazione avviene in tutte le fasi del processo e a tutti i livelli di governance della R&I (dalla pianificazione del programma, attraverso la progettazione, l'attuazione e la valutazione). Così la ricerca e l'innovazione affronteranno le sfide della società e saranno in linea con i valori, le esigenze e le aspettative del grande pubblico[58].

Proprio in quest'ottica, la nostra Startup[59] ha nei programmi dell'area di ricerca «Technological Sustainability by design» la realizzazione della survey multidisciplinare «Sostenibilità delle ricerche ad impatto sull'uomo del futuro e relativa comunicazione pubblica». Sul tema organizzeremo un premio per i migliori contributi, al quale potranno partecipare tutti gli studenti UNISOB e gli associati ALSOB e per le valutazioni verrà designato un Comitato Scientifico (tra Protech, Recepl, *et al.*).

Conclusioni.

In «Il Canto della Cella. Un'esplorazione della medicina e del nuovo essere umano»[60], l'autore è alle prese con le implicazioni di esseri umani potenziati che traggono beneficio dall'armeggiare cellulare (cellular tinkering) [61]. Questi «nuovi umani» non sono cyborg o persone potenziate con superpoteri, ma il famoso oncologo e scrittore intende «un essere umano ricostruito di nuovo con cellule modificate che sembra e si sente (principalmente) come te e me». Ma ingegnerizzando le cellule staminali in modo che una persona con diabete possa produrre la propria insulina o impiantando un elettrodo nel cervello di qualcuno che soffre di depressione, Mukherjee ipotizza che le abbiamo cambiate in qualche modo fondamentale. Gli esseri umani sono una somma delle loro parti, ma le terapie cellulari attraversano un confine, trasformando le persone in una «nuova somma di nuove parti»[62].

Nel riecheggiare il famoso esperimento filosofico sulla Nave di Teseo, rispetto ai «nuovi umani» potrebbero essere poste alcune domande: quante cellule devono essere alterate per renderci nuovi? Alcune cellule contano più di

[58] Cfr. https://tetrris.eu/what-is-responsible-research-and-innovation-rri/, cit..

[59] SUSTAIHUBLE IMPACT LAB (https://www.facebook.com/Sustaihuble-Impact-LAB-Pro-105184078667035) è un progetto Startup di ricerca e analisi ESG e corporate governance che supporterà aziende e organizzazioni nello sviluppo e implementazione di strategie di investimento, gestione e comunicazione responsabili e sostenibili. L'obiettivo è la realizzazione di soluzioni innovative e di alta qualità – anche AI-based - per aiutare aziende, enti, promotori, iniziative sia profit che no profit ed investitori a misurare e valorizzare la sostenibilità by design nei propri progetti, politiche e pratiche.

[60] Cfr. S. HARRISON, *Book Review: The Magic and Mystery of Human Cells*, in *Undark,* 11/18/2022. Consultabile al sito: https://undark.org/2022/11/18/book-review-the-magic-and-mystery-of-human-cells/.

[61] Cfr. «L'"armeggiare" cellulare è fondamentale per stabilire una nuova disciplina ingegneristica che porterà alla prossima generazione di tecnologie basate sui mattoni della vita», come si legge in A.S. KHALIL, C.J. BASHOR,T.K. LU, *Engineering Life*, in *The Scientist Magazine*, August 1, 2013. Consultabile al sito: https://www.bu.edu/khalillab/_papers/khalil-scientist2013.pdf.

[62] Cfr. HARRISON,*op. cit.*.

altre? O gli esseri umani possiedono una sorta di integrità intrinseca che influisce su questi calcoli?[63]

Articolando ulteriormente queste preoccupazioni, John Harris scrive[64]: «lo spazio tra conoscere il bene e fare il bene è una regione interamente abitata dalla libertà. La conoscenza del bene è sufficiente per aver resistito, ma la libertà di cadere è tutto. Senza la libertà di cadere, il bene non può essere una scelta; e la libertà scompare e con essa la virtù».

Allargando la responsabilità al contesto pubblico, nel suo documento di maggio 2021 il GEE ha fornito importanti prospettive sul ruolo dei valori in Europa e nella comunità globale, proponendo un coinvolgimento centrale e proattivo dell'etica nella governance[65]. La dichiarazione mette in luce le connessioni tra etica e diritti fondamentali, democrazia e stato di diritto, concludendo con una raccomandazione all'UE di massimizzare le opportunità di partecipazione pubblica al processo decisionale.

D'altronde abbiamo visto come molte norme della ricerca promuovano una varietà di altri importanti valori morali e sociali, come la responsabilità sociale, i diritti umani, il benessere degli animali, il rispetto della legge e la salute e sicurezza pubblica[66].

In definitiva, i valori e l'etica non sono limiti o ostacoli all'innovazione e al cambiamento; sono l'essenza dell'innovazione e del cambiamento[67]. Rappresentano la bussola che indica quali sono le modalità di costruzione del futuro responsabili, inclusive e sostenibili.

---

[63] *Ibidem*.

[64] Cfr. D. De Grazia, *Moral enhancement, freedom, and what we (should) value in moral behavior*, in *Journal of Medical Ethics*, 2014, 40, 361-368. Consultabile al sito: https://jme.bmj.com/content/40/6/361,365.

[65] European Commission, Directorate-General for Research and Innovation, *Values for the future. The role of ethics in European and global governance*, Brussels, May 2021. Consultabile al sito: https://op.europa.eu/en/publication-detail/-/publication/849e7ec4-cf13-11eb-ac72-01aa75ed71a1/language-en/format-PDF/source-245102876.

[66] Cfr. D.B. Resnik, *What Is Ethics in Research & Why Is It Important?* in *National Institute of Environmental Health Sciences,* December 23, 2020. Consultabile al sito: https://www.niehs.nih.gov/research/resources/bioethics/whatis/index.cfm.

[67] Cfr. European Commission, Directorate-General for Research and Innovation, *Values for the future. The role of ethics in European and global governance*, *op. cit.*.

Sanem Yilmaz S, Deniz Seval H, 'Mind over matter: Examining the implications of machine brain interfaces on privacy and data protection under the GDPR' (2022) 2 EJPLT, 347-361.
DOI: https://doi.org/10.57230/EJPLT222SSYHDS

EJPLT
ISSN 2704-8012



Mind over matter: Examining the implications of machine brain interfaces on privacy and data protection under the GDPR.

SABIRE SANEM YILMAZ
LLB, LLM
Maltepe University Technology and Intellectual Property Law Research Centre

HABIBE DENIZ SEVAL
Ph.D. (c) University of Ottawa, Centre for Law, Technology and Society

Abstract

Machine-brain interfaces (MBI) affect General Data Protection Regulation (GDPR), users' privacy and data protection. MBIs can transform industries and improve lives by directly connecting human brains to computers. However, these advances raise worries about personal data misuse and abuse and the need for robust regulatory frameworks to protect privacy and data. The article examines the relationship between privacy and MBIs in the context of the GDPR and closely examines surveillance risks posed by MBIs. The article also considers MBIs' ethicality and privacy as a human right. Thus, this essay examines the GDPR's current condition considering the the Brussels Effect and sustainability.

© The author(s) 2022, 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: Machine-Brain Interfaces, Privacy, Data Protection.

Summary: Introduction. – 1.1. Definition of Machine Brain Interfaces. – 1.2. Overview of Privacy Rights and Data Protection. – 2. Impact of MBIs on privacy rights. - 2.1. Impact of MBIs on Data Protection. – 2.2. Surveillance and MBIs. – 3. Risks MBIs towards the right to privacy as a fundamental right. – 3.1. Risks and Democracy Paradox. – 3.2. Can MBIs be Ethical? – 4. Brussels effect and MBIs – 4.1. Outsourcing or Crowdsourcing. – 4.2. Sustainability, Brussels Effect and MBIs. – Conclusion and Recommendations.

Introduction.

This article will explore the implications of MBIs on data protection and privacy laws. MBIs allow for direct communication between the human brain and machines and have the potential to revolutionize many aspects of our lives. However, the development and use of MBIs also raise important questions about privacy and data protection, particularly in the context of the GDPR[1], which imposes strict rules on processing personal data.

We will begin briefly explaining what MBIs, stating that they enable direct brain-machine communication. MBI users can control and communicate via channels other than the brain's muscles and peripheral nerves. We will then delve into the impact of MBIs on data protection and privacy, including the potential for surveillance. Next, we will discuss the ethical aspects of MBIs and the Brussels effect, which refers to the phenomenon in which the regulations and standards established by the EU have a global impact. Finally, we will conclude our findings and recommendations for the responsible development and use of MBIs.

MBIs generate a large amount of data that can be used to infer sensitive information about an individual's thoughts, emotions, and behaviours. The GDPR imposes strict rules on the processing of personal data, including data generated by MBIs. Hence, this raises important questions about how companies developing and using MBIs can ensure compliance with the GDPR and protect the privacy rights of their users. For instance, one of the significant challenges regarding MBIs is the issue of legal consent. Under the GDPR, companies must obtain the explicit consent of individuals before processing their personal data. Therefore, one potential solution to this would be the implementation of robust consent mechanisms. By requiring users to consent to the collection and processing of their data actively, companies can ensure that individuals are fully aware of how their data will be used and can opt out if they do not wish to share their data. In addition to obtaining explicit consent, companies should also consider implementing other privacy-enhancing measures, such as pseudonymization and

[1] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

encryption, to protect the security and confidentiality of MBI data. These measures can help to reduce the risk of unauthorized access to or misuse of sensitive personal data.

Besides data protection and privacy, ethical concerns need to be addressed. MBIs can be used to determine a person's willingness to accept abuse and hazardous content by acting as a warning. Also, one of the main points that will also be discussed in this article is the phenomenon of the Brussels Effect. It is a term used to explain the global impact of regulations and standards established by the EU, influencing the laws and practices of other countries worldwide. In the context of MBIs, the Brussels effect could have significant implications for how these technologies are developed and used, both within the EU and globally. By examining the legal framework governing MBIs, the types of data that may be collected through these interfaces, and the potential impacts of MBIs on the broader society, we can better understand the complex issues surrounding the development and use of MBIs and identify best practices for protecting users' privacy and data protection rights. Overall, the Brussels effect highlights the importance of considering the potential global impact of new technologies and the need for the responsible and ethical development and use of MBIs. In this article, through our analysis, we aim to understand better the complex issues surrounding the development and use of MBIs in the EU and identify best practices for protecting users' privacy and data protection rights.

1.1. Definition of Machine Brain Interfaces.

In 1973, researchers described a series of experiments meant to demonstrate that direct brain-computer communication is possible.[2] By using electrodes placed on the surface of the head or surgically implanted within the brain, these devices can detect and process brain signals, providing the user with a new way to interact with the world around them.

The MBIs are a type of technology that allows machines to communicate directly with the human brain.[3] These interfaces have the potential to revolutionize many aspects of our lives, including healthcare, education, and entertainment. Users of MBIs can control and communication channels independent of the brain's usual output channels of muscles and peripheral nerves.[4] By allowing direct communication between the brain and machines, MBIs could facilitate the development of new treatments for brain disorders, enhance learning and memory, and create immersive virtual reality experiences. However, the development and use of MBIs also raise important questions about privacy and data protection. However, there are still many challenges that need to be

[2] JJ Vidal, 'Toward Direct Brain-Computer Communication' (1973) 2 Annu. Rev. of Biophys and Bioen., pp. 157.
[3] T Bonaci, R Calo and HJ Chizeck, 'App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces', 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering.
[4] O Landau, R Puzis and N Nissim, 'Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space' (2021) 53 ACM Computing Surveys, pp. 1.

addressed before these technologies can be widely adopted. One major challenge is the need to improve the accuracy and reliability of MBIs.

1.2. Overview of Privacy Rights and Data Protection.

As a fundamental human right, the right to privacy is protected by various national and international laws and, therefore, an essential aspect of human life and they protect an individual's privacy. These rights are outlined in national and international laws and are intended to safeguard individuals from unreasonable intrusions into their personal lives. Furthermore, the right to privacy is undoubtedly an essential part of the modern legal system and serves as a fundamental check on government power and a source of protection for individuals. There are several essential theories on privacy to better understand, interpret it and how to embed in laws. For instance, Warren and Brandeis asserted that individuals have a right to be left alone and free from unwanted intrusions into their personal lives.[5] According to them, privacy is a fundamental human right.[6] On the other hand, the informational privacy theory proposed by Westin states that privacy is the ability of an individual to control the collection, use, and dissemination of their personal information.[7] Privacy and data protection are closely related, as protecting personal data is often an important way to protect privacy. Data protection ensures that only authorized parties can access personal information, protecting an individual's privacy. The GDPR, an EU law on data protection and privacy for EU and EEA citizens, is one of the most important privacy laws. It addresses personal data exports outside the EU and EEA. It aspires to return personal data control to individuals and simplify international business regulation by harmonizing EU regulation.

2. Impact of MBIs on privacy rights.

Privacy, ethical, and human rights problems are all brought up by the close ties between individuals' data and various MBI applications. As a result, it comes as no surprise that current data protection rules are being applied in the context of MBIs, and that these laws are being amended to address specific challenges. In the case of MBIs and privacy, different perspectives must be considered. For instance, it appears necessary to distinguish between neural data and mental data to determine the extent of privacy protection in the domain of the mind.[8] Neural data refers to the raw data collected from the brain, such as electrical activity or neural firing patterns, through various technologies like EEG, fMRI, or other neuroimaging tools. In its raw form, this data does not necessarily reveal specific

[5]SD Warren and LD Brandeis, 'The Right to Privacy' (1890) 4 Harv. L. Rev., pp. 193.
[6]ibid.
[7] A Westin, Privacy and Freedom (1967, New York: Atheneum).
[8] L Gatt, IA Caggiano, MC Gaeta, AA Mollo, 'BCI Devices And Their Legal Compliance: A Prototype Tool for Its Evaluation and Measurement' (2022) 1 EJPLT, 301-314.

thoughts, emotions, or mental experiences, but it can be analyzed to infer information about a person's mental state potentially. On the other hand, mental data refers to the actual content of a person's thoughts, emotions, memories, or subjective experiences. Therefore, this data is considered more intimate and private, as it directly relates to an individual's identity, beliefs, and personal experiences. Therefore, when deciding the scope of privacy of the mind, it is essential to distinguish between neural and mental data. Since mental data may reveal more private details about a person's life than neural data, for instance, they require different sensitivity levels. Although there have been considerable breakthroughs in neuroimaging and MBIs, there is still room for improvement in humans' abilities to decipher mental content effectively and reliably from neural data. The necessity to safeguard mental data may grow as our knowledge and technology advance. Another of the potential challenges of MBIs is that they may generate a large amount of data that could be used to infer sensitive information about an individual's thoughts, emotions, and behaviors. This raises important questions about privacy and data protection, particularly in the context of the GDPR, which imposes strict rules on the processing of personal data. To ensure compliance with the GDPR, it will be important for companies developing and using MBIs to carefully consider the types of data that may be collected through these interfaces, and to implement appropriate safeguards to protect the privacy of their users. Another potential issue with MBIs is the potential for discrimination and ethical risks that has posed by this technology. While MBIs have the potential to revolutionize healthcare, education, and entertainment, there are ethical risks such as certain groups being left behind or disadvantaged if they are unable to access or afford these technologies. It will be important for policymakers and industry leaders to consider the potential impact of MBIs on the broader society and to develop strategies to ensure that the benefits of this technology are distributed fairly and equitably.

Overall, addressing the privacy and data protection challenges posed by MBIs will require a multi-faceted approach that involves both industry self-regulation and government oversight. By taking a proactive and collaborative approach, it is possible to ensure that the development and use of MBIs is responsible and ethical, and that the potential benefits of this technology are realized for all members of society.

2.1. Impact of MBIs on Data Protection.

As mentioned earlier, MBIs are a type of artificial intelligence (AI) system designed to mimic human brains' abilities, allowing computers and machines to think and reason as humans do. This technology has immense potential applications in data protection and security, as it can be used to identify patterns quickly and accurately in large amounts of data quickly and accurately. Therefore, one of the main concerns with MBIs is the potential for the devices to collect and transmit large amounts of sensitive personal information. For example, MBIs may be able to collect data on an individual's thoughts, emotions, and even memories.

This data could be used for various purposes, such as targeted advertising or medical research. At this point, data protection is an important issue as more MBIs become more common. However, with so much information stored digitally, there is always a risk that someone could gain access to personal data without consent. Therefore, organisations must have effective data protection systems in place to protect personal data and the right to privacy in specific to use cases of MBIs.

2.2. Surveillance and MBIs.

'Nothing was your own except the few cubic centimeters inside your skull.'[9]

One potential impact of MBIs on surveillance is that it could make it possible for governments and other organizations to monitor people's thoughts and emotions without their knowledge or consent. For instance, this could be done by placing sensors in people's homes or workplaces or using non-invasive techniques such as functional magnetic resonance imaging to read brain activity from a distance. Hence, this would allow organizations to gather vast information about individuals, including their personal beliefs, opinions, and emotional states, which could be used for various purposes, such as targeted advertising or political manipulation. It is important to refer to the fact that, if others, including the state, expose an individual to dangers that the individual has no way of knowing are present, this is unfair and will violate the individual's autonomy.[10] Furthermore, MBIs can be used to create mind-reading devices that could be used by law enforcement and intelligence agencies to extract information from suspects or to monitor the activities of individuals deemed to be a threat to national security. This could be done by attaching sensors to a person's head to read their brain activity and extract information about their thoughts, memories, and intentions. Essentially, George Orwell's portrayal of a totalitarian government's constant surveillance in his novel 1984, where Big Brother watches every move of its citizens, with the goal of total control and manipulation, will be a possible scenario in this regard.[11] Another potential risk is hackers' ability to access MBI-enabled devices and steal sensitive personal information. As MBI devices become more prevalent, hackers will likely develop methods to access them, enabling them to steal personal information such as financial data, medical records, and other sensitive information. Moreover, MBI technology could also be used for commercial purposes, such as targeted advertising. Companies could use MBI technology to gather information about people's emotional states, preferences and interests and use that information to target them with advertising.[12] This breach of privacy allows companies to access personal thoughts and emotions, which can also be considered a violation of 'decisional privacy'.[13]

---

[9]G Orwell and E Fromm, 1984 (Signet Classics 2017).
[10] L Austin,'Privacy and the Question of Technology' (2003) 22 Law & Philosophy, pp. 119.
[11]Orwell and Fromm, 1984 (n 9).
[12]RJ Neuwirth, The EU Artificial Intelligence Act: Regulating Subliminal AI Systems (1st edn, Routledge 2022).
[13] L Gatt, IA Caggiano, MC Gaeta, AA Mollo, 'BCI Devices And Their Legal Compliance' (n 8), pp, 308.

On the other hand, MBI technology could also positively impact privacy by allowing people to control technology with their thoughts rather than using physical interfaces such as keyboards or touchscreens. This would make it possible for people to use devices and access information without anyone knowing.

It is important to assess the effectiveness of GDPR in protecting citizens from surveillance risks posed by MBIs. This will help ensure that personal data is collected and used responsibly and lawfully. The GDPR can be effective in addressing privacy risks associated with the use of MBIs in several ways. Firstly, the GDPR requires organizations to be transparent about their data collection and processing activities.[14] This means that organizations would have to inform individuals about the collection and use of their brain data and obtain their explicit consent before collecting and processing it. Secondly, due to the principle of data minimization by the GDPR, organizations can collect and process only the data necessary for a specific purpose.[15] This could be applied to MBI data by limiting the type and amount of data collected and ensuring that it is only used for specific, legitimate purposes. Thirdly, the GDPR requires organizations to implement data protection measures from the design stage of a product or service.[16] This means that organizations would have to ensure that MBIs are designed with privacy in mind and include appropriate security measures to protect brain data from unauthorized access or processing. However, in this regard, the ambiguity regarding the concept of privacy by design will likely cause uncertainties and problems.

In summary, the GDPR seems like it is providing a comprehensive framework that can be applied to the use of MBIs to ensure that data is collected and processed lawfully. However, are there any flip sides of the GDPR when it comes to surveillance risks posed by the MBIs? The first weakness arises due to the GDPR's vagueness regarding non-invasive techniques. The GDPR applies to collecting and processing personal data through various means, including non-invasive procedures such as functional magnetic resonance imaging. However, neither the GDPR nor any guidelines do not address using these techniques for surveillance or gathering information about people's thoughts, emotions, and intentions without their knowledge or consent. Secondly, although MBIs use cases are widespread, there is no specific guidance on how to protect data collected through MBIs and ensure that it is only used for specific, legitimate purposes. Thirdly, while GDPR provides individuals with certain rights about their data, these rights may be limited when it comes to MBIs. For example, the right to access and delete brain data may be more difficult to exercise and may need to be more effective in protecting privacy.

MBIs collect sensitive personal data, making data protection difficult. Unfortunately, current laws like the GDPR are based on traditional privacy concepts that don't always reflect new technologies, making them insufficient for

[14]The GDPR (n 1).
[15] Ibid.
[16] Ibid.

user protection. Future-proofing privacy regulations ensures adequate protection regardless of technology. Since the GDPR was implemented in 2018, MBI technology has advanced rapidly. Thus, MBIs may not be fully addressed. For instance, neuro-marketing uses brain-computer interfaces to monitor and analyze consumers' brain activity to improve marketing strategies. GDPR restricts commercial data collection. It may not fully address neuro-ethical marketing's issues, such as consumer manipulation and lack of informed consent.

3. Risks MBIs towards the right to privacy as a fundamental right.

3.1. Risks and Democracy Paradox.

Due to their nature, MBIs constantly expose them to violating the right to privacy, which is a fundamental right. These technologies, which should be ethically audited, also act as a reminder about human rights and privacy impact assessments. Because the algorithm's unique design and MBI customization are fundamental rights issues. Ownership and exclusivity of the algorithm safeguard the end user from manipulative MBIs that could undermine her freedom of expression or personality.[17] Violating the right to privacy as a fundamental right disrupts the structure of the democratic environment in the long run. For instance, reading and deciphering thoughts outside of clinical studies on analysing neuro data is unlawful processing of personal data. Hence, protecting the right to privacy in the design and innovation phases of MBIs is possible by complying with the GDPR per the principle of interoperability. Therefore, it is important to address the risk and challenges under fundamental rights and Democracy in protecting the right to privacy.[18]

Today, democracy requires privacy protection. GDPR's data minimisation, pseudonymisation, limitation of purpose, anonymisation, and data protection safeguard data subjects' democratic rights. MBIs' effects on democracy and self-determination cannot be disregarded. However, depending on how Democracy is perceived in the country in which MBIs are used, pluralism, democratic participation, transparency, and accountability are not yet fully validated. Hence, these technologies directly target Democracy. For example, the concern arising from using MBIS technology will be the direction of choices and manipulating groups of people who develop uniform thinking. Will their past cognitive abilities reinstate the MBI's-winning cognitive skills? However, it is even more alarming when it comes to the fact that different human brains connect to a machine and benefit from each other's abilities. Because then people will be connected to a wireless network, such as modems that provide multiple Internet, and will be able to warn each other about talent and cognitive skills. At this point, the impairment

[17] B Custors, G Malgieri, 'Priceless Data: Why the EU Fundamental Right To Data Protection Is At Odds With Trade In Personal Data' (2022) 45 CLSR, pp. 5.
[18] A Krausová, 'Legal Aspects of Brain-Computer Interfaces' (2014) 8(2) Masaryk Univ. J. of Law and Technol., pp. 203.

of the will and the active cognitive skill may send manipulative signals.[19] For instance, EMOTIV[20] is a device that uses the EPOC headset raised two main topics, such as transferring human brainwaves through the connection of devices and recording silent communication, beyond being a work of performance. The precision data of the neural data that provides mutually silent communication and the connection of sensitive data to specific processing conditions and explicit consent in GDPR Art. 9[21] also prevents the destruction of Democracy and fundamental rights.[22] Furthermore, using state-of-the-art technology to protect sensitive data in cyberspace, not processing data outside of its intended processing, and taking open consent based on informational results at the last point in Democracy. In MBIs, neural data is processed by AI tools and combined with large data sets. It has several tools that may cause the individual to move away from the democratic environment, such as automatic decision-making and profiling, which can result in a horizontal violation of the right to privacy. Horizontal infringement is a form of infringement that also impacts other fundamental rights.

Data protection by design and default is crucial for fundamental rights and democracy, as stated in GDPR art. 25.[23] As mentioned above, MBI sensors should be designed to limit data protection to a high level of technological methods and preserve fundamental rights and democracy by protecting device privacy.[24] Privacy is vital when one needs to be made aware of the right decisions. Democratic society will require these modern technologies to guarantee fundamental rights like privacy. They'll create some preferences and article 25[25] emphasizes that. Thus, MBIs must retain privacy by default and design without notifying the user before interacting with brain waves.[26]

Elon Musk's Neuralink[27] project aims to connect everyone's brain to a machine, but how do democracy and human rights will get affected by this? The GDPR protects government data. What if the machine, schooled by the human brain, says the idea is hers? Human opinions are owned by staying naked in private. Democracies abuse fundamental rights by demanding and not intervening. Self-intervention in a democracy protects fundamental rights and legalizes action. MBI risk surveillance. All at-risk people will be victims now. For surveillance, MBI

[19] M Ienca, G Malgieri, 'Mental Data protection and GDPR', (2022) 1(19) Journal of Law and the Biosciences, pp. 11.
[20] The EMOTIV, <https://www.emotiv.com/about-emotiv/> accessed 19 January 2022.
[21] The GDPR, Article 9 (n 1).
[22] Z Polina, P Chapman, M Ma, F Pollick, 'A Wireless Future: Performance Art, Interaction and Brain- Machine Interfaces' (2014) ICT, pp. 3.
[23] The GDPR, article 25 (n 1).
[24] B Francesca and others, 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities' (2015) 20, Law, Governance and Technology Series, pp. 12.
[25] The GDPR, article 25 (n 1).
[26] TZ Zarsky, 'Incompatible: The GDPR in the age of Big Data', (2017) 4(2) Seton Hall L. Rev., pp. 8.
[27] The Neuralink, < https://neuralink.com> accessed 19 January 2022.

creates a digital identity that compromises fundamental rights.[28] In a democracy, is oversight legal, appropriate, and necessary?

As we mentioned earlier, if MBIs are used to assess performance of then this application will be mandatory. The employee is given explicit consent to protect their personal data, and the application is required. It doesn't offer an alternative method to the workplace. In this case, there will be a breach of fundamental rights due to processing is unlawful and does not even fall under the scope of legitimate interest. When you think that performance assessments are used to develop a new MBI system in another employer's company and that there is no clear consent from employees, all these actions must complete the questions we asked above.[29] According to the High-Level Expert Group[30], to implement and achieve trustworthy AI, seven requirements need to be met;

- human agency and oversight,
- technical robustness and safety
- privacy, data quality, integrity
- transparency
- diversity and fairness,
- sustainability, environmental friendliness, social impact, and democracy.
- accountability

These principles should also be imported to the origin of the MBIs. The further away from these principles, the higher the risk is for Democracy and fundamental rights. In this context, the MBIs have a reverse ratio between what it wants to achieve and Democracy, fundamental rights and the right to privacy which will create a paradox.

3.2. Can MBIs be Ethical?

It is also important to consider the significant ramifications of protecting mental privacy and demand proper ethical and legal thought to evaluate the operational specifics of MBIs.[31] Hence, the ethical issue resembles a mime artist with two different facial expressions regarding privacy and, therefore, the protection of fundamental rights. MBIs pose risks in determining willpower to accept abuse and harmful content because they process sensitive data from its first source.

Given that MBIs are used in the health sector, how can one determine the infringement of privacy rights and the extra data collection activities that will contribute to the treatment process from an ethical perspective? The right to

[28] The European Comission, 'High Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI' (2019), pp. 12.
[29] V De Stefano 'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection' (2018) 1 Comp. Lab. L. & Pol'y. J., pp. 10.
[30] High-Level Expert Group on Artificial Intelligence, 'Trustworthy AI', (n 28).
[31] L Gatt, IA Caggiano, MC Gaeta, AA Mollo, 'BCI Devices And Their Legal Compliance' (n 8), pp.310.

demand human ethical monitoring, self-determination without harming society, privacy, and the benefit of therapy or MBIs will maintain the balance between self-determination and society. Floridi emphasises the need to steer clear of ;ethics blue washing,' the act of making unfounded or deceptive assertions regarding the ethical merits and advantages of digital processes, products, services, or other solutions, to avert the misleading ramifications of such ethical choices.[32] Thus, to tackle this issue, it is imperative to establish comprehensive ethical impact assessments, which shall regulate the field and guarantee sincere compliance with digital ethics. Therefore, ethical impact assessments will address whether this field can be regulated.[33] The ethical and human rights impact assessments should go smoothly because the rule is open to technological advances. The ethicality of a black box AI system is a crucial concern. How will shared ethical values be determined throughout societies? In 1950, the Turing Test organised only the introduction of the ethical aspect of the 1980-year Chinese Room argument with different aspects of testing and criticising the decision of machines instead of people.[34] In this context, we cannot go past the development of Kant's philosophy.[35]

The requirement for the operation does not make it legal to exclude the AI systems used for MBIs from a system that can be explained and calculated. Even if you are in a position not to be able to disclose the actual consent of the user, the legal representatives of the user or the decision-making ethics board should explain how the system went to the decision-making point and the algorithm that made the decision.

4. Brussels effect and MBIs.

4.1. Outsourcing or Crowdsourcing.

Although the regulatory aspect of MBIs and the Brussels Effect[36] needs a more extensive study, it is beneficial to mention it to explore its more profound impacts on privacy. As with the regulation of other new technologies, the regulation of MBIs will be open to the opinions of industry representatives, NGOs, member states, and technology beneficiaries.[37]

The recent AI Act indicates responsibilities what MBIs will have as well. Also, Ad Hoc Committee on Artificial Intelligence (CAHAI) was established in September

[32] L Floridi, 'Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical' (2019) Philosophy & Technology pp.185–193.
[33] M Pizzi, M Romanoff, T Engelhardt, (2020) 102 'AI for Humanatarian Action: Human Rights and Ethics' Int. Rev. The Red Cross, pp. 154.
[34] The Standford Encycilopedia of Philosolophy, (2003) < https://plato.stanford.edu/entries/turing-test/> accessed 19 January 2023.
[35] O Ulgen, 'Kantian Ethics in The Age of Artificial Intelligence and Robotics' (2017) Quest. Int. L., pp. 70.
[36] A Renda, 'Beyond the Brussel Effect' (2022) Friedrich-Ebert-Stiftung Report 17 (220301 beyond the brussels effect.pdf (feps-europe.eu) accessed 24 January 2023.
[37] P Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence' (2018), pp. 10.

2019 to determine human rights, the rule of law, and democratic standards in designing, developing, and implementing AI. It is an important study in Brussels, seeking digital sovereignty, benefits from Strasbourg's common sense. Representatives of non-EU countries and academics closely follow the meetings to provide opinions. The EU supports outsourcing to regulate technologies, even if it is not a member of the EU while assigning value to these views. It will be possible to use and transfer data across the border, to transfer data that is needed from the cross-border space but to exchange common views and to fulfil certain warranties by non-member states.[38] In particular, the cross-border flow of data and secondary uses of health care are becoming increasingly important. During the pandemic, the need for cross-border flows has increased with the development of new technologies.

Protection of the right to privacy has also been the scene of widespread debate within human rights standards.[39] There are also horizontal impact discussions with regulations such as data governance, digital markets act, data act, and Digital Services Act[40] (DSA).[41] With Brussels focusing on legislation and supporting technological developments, human rights have been balanced by CAHAI to establish ethical principles in establishing standards of the rule of law. In its feasibility study, transparency, explainability, human oversight, the non-discrimination of AI and the human dignity need to be considered be on the axis of MBIs.[42] In this context, Brussels will need to use various resources or externally receive services while regulating space for a more transparent, more explainable AI. Therefore, outside the EU territory, Brussels has become welcoming for innovators and developers because data must flow to the USA to benefit for Brussels to have continuous operation of technology products.

The Brussels effect is reflected in the regulation process as a risk-based approach. In CAHAI, a risk-based approach has drawn the body of AI with red lines which are also transferred to the AI Act. On the one hand, Brussels is making progress on the horizontal axis with various regulations for the growth of the digital market. The GDPR replaces the Data Protection Directive and The European Convention No. 108+[43] follows the DSA and Digital Marketing Act (DMA)[44] on the horizontal axis. Within these regulations, the GDPR and AI Act are the great older brother of others. On the other hand, Brussels also wants to lead the way in markets such as USA, China, and Korea to ensure that data flow is legal and compliant with human rights. Therefore, it is closely monitoring the data

[38] A Renda, Beyond the Brussel Effect (n 35), pp. 20.
[39]A Mantelero, 'Beyond Data' (T.M.C. Asser Press, 2022), pp. 161.
[40] 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).
[41] European Commission, '2030 Digital Compass: the European way for the Digital Decade,' COM (2021), pp. 118.
[42] AR Young, 'The European Union as a global regulator? Context and comparison' (2015) 22 (9) J. Eur. Public Policy, pp. 1233.
[43] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108.
[44] 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).

protection laws and relevant laws of states to ensure that states work on the same axis as Brussels.[45] In this context, the lack of an interoperable law of states will be one of the factors directly affecting the market.[46] For example, the Data Governance Act[47], which is being worked on for the creation of common data sets platforms for data management, describes how the system will operate in concrete terms and the Brussels front.

At this point, it is a fact that Brussels cares about the creation of data sets that MBIs will use or mechanisms that can share secure data sets after anonymising the data they have obtained. They are trying to complete horizontal legal regulations in this area. However, MBIs will have a challenging position in case of the GDPR. Therefore, the Brussels front is very concerned about the data minimisation and purpose limitation stage and the control mechanisms. Privacy by design and by default phenomena also follow these principles. The signals recorded by the devices used in Brussels's MBIs are kept in the country where the device is manufactured. The possible regulations for storing signal data are also will be compliant with GDPR art. 46[48]. So, keeping the data in the country in which the device is manufactured will be a method Brussels would not agree to. The country of the instrument must take the necessary measures at this point in terms of the protection of the AI Act and the GDPR. Furthermore, Brussels effect, which we can also refer to as Bradford's influence, cares about the Europeanization of data. We believe that this angle is very clear in the domain of GDPR.[49] The determination of the GDPR country in a way that includes the services that non-EU countries provide to EU citizens also led countries serving EU citizens to adopt the scope of GDPR and enforce their best practices and regulations in accordance with GDPR or try to do their best. In this context, the GDPR has spawled the concept of spreading European data.

4.2. Sustainability, Brussels Effect and MBIs.

Sustainability is an important and hidden phenomenon meaning to regulate technology and monitor it after post-regulation. Due to the high risk of computer MBIs, it is mandatory to follow the lawfulness of products allowed to operate in the market as much as the prohibition of applications that eliminate basic rights to protect the fundamental rights of data subjects.

Because of the need for neuro data, MBIs must process sensitive data. Hence, periodical privacy impact assessments, guidance on using privacy-enhancing

[45] LA Bygrave, 'The Strasbourg Effect on Data Protection in Light of The Brussels Effect: Logic, Mechanics and Prospects', (2020) 8 CLSR, pp. 10.
[46] K Sahin and T Barker 'Europe's Capacity to Act in the Global Tech Race: Charting a Path for Europe in Times of Major Technological Disruption' (DGAP Report, 6) (2021) Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V., https://nbn-resolving.org/urn:nbn:de:0168- ssoar-73445-7 16. accessed 24 January 2023.
[47] Proposal for a Regulation of The European Parliament And Of The Council on European Data Governance (Data Governance Act).
[48] The GDPR, Article 46 (n 1).
[49] LA Bygrave, The Strasbourg Effect on Data Protection in Light of The Brussels Effect, (n 41), 11

technologies, repeating explicit consent in each processing state, and follow-ups as objective changes are necessary. While other horizontal regulations regulate data processing processes other than GDPR[50], horizontal regulations greatly contribute to sustainability. By regulating the processes of non-personal data processing, DSA also strengthens the presence of GDPR, such as the Data Governance Act, which regulates the smooth use of data in all sectors without discrimination of personal and non-data and further details the rights of data subjects.[51]

There are also areas where sustainability is still problematic, such as creating secure data sets for the transfer of neuro data processed in MBIs outside the GDPR's territory. Although MBIs are more likely to show up in areas such as gaming and performance measurement, medical diagnosis and treatment processes have been used in the past and will be used more often. When EEG data is acknowledged to give the most accurate results in processing brain signals, three scales on how data subjects will impact their rights before data processing can be maintained at the heart of the right. Three scales are human rights impact assessment, ethical impact assessment, and privacy impact assessment.[52] Another key area to ensure sustainability is ensuring that data protection authorities can interoperability and effectively use the object rights granted to the data subject. The MBI market will be partially EU-based, and services will be purchased from different locations may result in the country of conflict being other countries or the mechanisms of objection being combined with several data protection authorities. We don't want to discuss issues such as jurisdiction because this article is different from the article's subject. However, the importance of data protection authorities acting on common platforms and common law is inevitable.[53] The closest we have seen in the Covid 19 process is that an EU data protection field that ignores data subject rights cannot be sustained. The Brussels effect closely followed inventions, medication monitoring, continuous health data monitoring, etc. to handle the pandemic.[54]

5. Conclusion and Recommendations.

As with any new technology, it is essential to carefully consider the implications and develop appropriate regulations and guidelines to protect privacy and

[50] AB Tickle and others, 'The Truth Will Come to Light: Directions and Challenges in Extracting the Knowledge Embedded Within Trained Artificial Neural Networks' (1998) 9 IEEE Transactions on Neural Networks, pp. 1057.
[51] LA Bygrave The Strasbourg Effect on Data Protection in Light of The Brussels Effect (n 41), 13.
[52] W Samek and others., 'Evaluating the Visualization of What a Deep Neural Network Has Learned, IEEE Transactions on Neural Networks and Learning Systems' (2016); MT Ribeiro and others 'Why Should I Trust You? Explaining the Predictions of Any Classifier', (22016) Proceedings of the 22nd Acm Sigkdd International Conference on Knowledge Discovery And Data Mining.
[53] E Palmerini, 'Algoritmi E Decisioni Automatizzate Tutele Esistenti E Linee Evolutive Della Regulazione' (2021) Editoriale Scientifica, pp. 13.
[54] L Edwards, M Veale, 'Slave to the Algorithm? Why a Right to An Explanation is Probably Not The Remedy You Are Looking For' (2017) 18, Duke L. & Tech. Rev., pp. 69.

individual rights. Mitigating risks is important to develop appropriate regulations and guidelines to protect privacy and individual rights.

New technologies like MBIs introduce new issues that, in the absence of legislative amendments, must be resolved through the interpretation and application of existing rules. These outdated rules also need to be changed to provide more clarity and to better address the challenges brought by new technologies like MBIs.[55] Additionally, to progress MBIs while preserving citizens' rights to privacy and other basic liberties, legislators will need to find a middle ground between the demands of corporations and governments. However, it won't be sufficient to enforce new regulations that apply to cutting-edge technologies like MBIs. In order to have multi-layered efficacy, it is essential to include protections and limits that are relevant to these new technologies, such MBIs. Also, we mentioned how sustainability involves regulating and monitoring technology and how data subject rights became even more critical with the rise of MBIs. Also, the connection between MBIs and the legal side of the Brussels Effect have serious implications regarding privacy which needs to be monitored closely.

One potential solution to the privacy and data protection challenges posed by MBIs is the implementation of robust consent mechanisms. Under the GDPR, companies must obtain the explicit consent of individuals before processing their personal data. This includes data generated through MBIs. By requiring users to actively consent to the collection and processing of their data, companies can ensure that individuals are fully aware of how their data will be used and can opt-out if they do not wish to share their data. In addition to obtaining explicit consent, companies should also consider implementing other privacy-enhancing measures, such as pseudonymization and encryption, to protect the security and confidentiality of MBI data. These measures can help to reduce the risk of unauthorized access to or misuse of sensitive personal data.

MBI industry standards and guidelines are other options. These standards could address data protection, privacy, and ethics. In addition, companies and researchers may ensure that MBIs are responsibly developed and used by creating clear rules. Finally, it will be important for regulators and policymakers to closely monitor the development and use of MBIs and to act as necessary to ensure compliance with relevant laws and regulations. This may include issuing guidance or issuing enforcement actions against companies that fail to adequately protect the privacy and data protection rights of their users.

[55] F Martin-Bariteau T Scassa eds., Artificial Intelligence, and the Law in Canada (Toronto: LexisNexis Canada, 2021).

LIST OF AUTHORS OF THIS EJPLT ISSUE

ILARIA AMELIA CAGGIANO – Full Professor of Private Law, Università degli Studi Suor Orsola Benincasa, EJPLT Vice-Director.

GIOVANNA D'ALFONSO – Associate Professor of Private Law, Università degli Studi della Campania Luigi Vanvitelli.

MATTEO DE PAMPHILIS – Contract Professor of Product Safety, Product Liability and Automotive, Alma Mater Studiorum Università di Bologna.

MASSIMO DE FELICE – Full Professor, Sapienza Università di Roma.

ANDREA DEL FORNO – Ph.D.(c) Università degli Studi di Siena e Foggia.

ANTONELLA DI CERBO – Ph.D (c) in Private Law, Università degli studi del Sannio.

FRANCESCA DI LELLA – Researcher in Private Law, lecturer in Biolaw, Università degli Studi di Napoli Federico II.

SIMONE FABIO DICORATO – MEng in Advanced Motorcycle Engineering, Motorvehicle University of Emilia Romagna.

LUCILLA GATT – Full professor of Private Law, Università degli Studi Suor Orsola Benincasa, EJPL Editor in Chief.

SERGIO GUIDA – Independent Scholar, Founder & Team Leader Sustaihuble Impact LAB.

CHIARA IORIO – Postdoctoral Research Fellow, Università degli Studi di Macerata.

LUIGI IZZO – Ph.D. (c) in *Humanities and Technologies: an integrated research path*, Università degli Studi Suor Orsola Benincasa.

SEYED MILAD MAHMOOD KASHANI – Ph.D. (c) Università degli Studi di Napoli Federico II.

ROBERTA MARINO – Associate Professor of Private Law, Università degli Studi di Napoli Federico II.

ALESSIA MIGNOZZI – Associate Professor of Private Law, Università della Campania Luigi Vanvitelli.

ANNA ANITA MOLLO – Postdoctoral Research Fellow in Private Law, Scuola Superiore Meridionale, Lawyer.

DOMENICO NAPOLITANO – Postdoctoral Research Fellow in business organisation, Scuola Superiore Meridionale, Lawyer.

ELENA QUARTA – Director Area 'Derecho penitenciario', Instituto Juridico "Arte del derecho" Lima Perù.

RANIERI RAZZANTE – Contract Professor of Techniques for Anti-Money Laundering Risk Management at Alma Mater Studiorum Università di Bologna, Contract Professor of Techniques and Rules of Cybersecurity at Università degli Studi Suor Orsola Benincasa.

FRANCESCO RIBEZZO – Ph.D. (c) Università degli Studi di Bari Aldo Moro

HABIBE DENIZ SEVAL – Ph.D. (c) University of Ottawa.

LUIGI MARIA SICCA – Full professo of business organisation, Università degli Studi di Napoli Federico II.

SABIRE SANEM YILMAZ – LLB, LLM, Maltepe University Institute of Informatics and Technology.

FABIO ZAMBARDINO – Assegnista di Ricerca, Università degli Studi della Campania Luigi Vanvitelli.