ISSN: 2704-8012

SUOR ORSOLA BENINCASA
UNIVERSITÀ EDITRICE

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

www.ejplt.tatodpr.eu



2024/1

EJPLT
ISSN: 2704-8012

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

Directed by Lucilla Gatt

2024/1

SUOR ORSOLA BENINCASA
UNIVERSITÀ EDITRICE

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

Co-funded by the European Union

The Journal was born in 2018 as one of the results of the European project "Training Activities to Implement the Data Protection Reform" (TAtoDPR), co-funded by the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191. From 2019-2022, the Journal was supported by the Erasmus+ Programme of the European Commission within the European Project Jean Monnet Chair 'European Protection Law of Individuals in relation to New Technologies' (PROTECH) (611876-EPP-1-2019-1-IT-EPPJMO-CHAIR).

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

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

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

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

Indexed in

https://doi.org/10.57230/EJPLT
https://doi.org/10.57230/EJPLT241

Editing Luciana Trama

Design Flavia Soprani

Development Maria Teresa Lo Conte

© Copyright 2024 by Suor Orsola Benincasa Università Editrice, published in June 2024
ISSN: 2704-8012
The intellectual property of the individual contributions remain with the authors.
The Issue and the individual contributions are licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND
All the details at: *https://creativecommons.org/licenses/by-nc-nd/4.0*
Free access to the Issue at: *www.ejplt.tatodpr.eu*

European Journal of Privacy Law & Technologies

EJPLT
ISSN: 2704-8012

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

VICE-DIRECTOR
Prof. Ilaria Amelia Caggiano – Università degli Studi Suor Orsola Benincasa di Napoli, Italy

COORDINATOR OF THE EDITORIAL AND REFEREES BOARD
Ph.D. Avv. Maria Cristina Gaeta – Università degli Studi Suor Orsola Benincasa, Italy

ADVISOR BOARD – SCIENTIFIC COMMITTEE
Prof. Pasquale Arpaia – Università degli Studi di Napoli Federico II, Italy
Prof. Matthew Dyson – University of Oxford, United Kingdom
Prof. Valeria Falce – Università Europea di Roma, Italy
Prof. Indranath Gupta – O.P. Jindal Global University, India
Porf. Juan Ernesto Gutiérrez Otiniano – Universidad Autonoma del Perù, Peru
Prof. Pim Haselager – Radboud University, Netherlands
Prof. Toni Jaeger-Fine – Fordham University School of Law, United States
Prof. Antonios Karaiskos – Ryukoku University, Japan
Prof. Roberto Montanari – Università degli Studi Suor Orsola Benincasa, Italy
Prof. Roberta Montinaro – Università degli Studi di Napoli l'Orientale, Italy
Prof. Andrew Morris – University of Loughborough, United Kingdom
Prof. Juan Pablo Murga Fernandez – Universidad de Sevilla, Spain
Prof. Alex Nunn – Leeds Trinity University, United Kingdom
Prof. Avv. Salvatore Orlando – Sapienza Università di Roma, Italy

REFEREES
Prof. Jaime Alcalde Silva – Pontificia Universidad Católica de Chile, Chile
Prof. Jeremy Antippas – Université de Bretagne Sud, France
Prof. Miguel Álvarez Ortega – Kyoto University, Japan, and Universidad de Sevilla, Spain
Prof. Claudia Benanti – Università di Catania, Italy
Prof. Andrea Bertolini – Scuola Superiore Sant'Anna di Pisa, Italy
Prof. Carlos Antonio Agurto Gonzáles – Universidad Nacional Mayor de San Marcos, Peru
Prof. 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. Alberto Giulio Cianci – Università degli Studi di Perugia, Italy
Prof. Maria Antonia Ciocia – Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Valentina Vincenza Cuocci – Università di Foggia, Italy
Prof. Giovanna D'Alfonso – Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Carlos de Cores Helguera – Universidad CLAEH del Uruguay, Uruguay
Prof. Manuel Espejo Lerdo de Tejada – Universidad de Sevilla, Spain
Prof. Elżbieta Feret – Uniwersytet Rzeszowski, Poland
Prof. Marco Giacalone – Vrije Universiteit Brussel, Belgium
Prof. Giovanni Iorio – Università degli Studi di Milano Bicocca, Italy
Prof. Arndt Künnecke – Hochschule des Bundes für öffentliche Verwaltung, Germany
Prof. Leysser Luggi Leon Hilario– Pontificia Universidad Católica del Perú
Prof. Martin Maguire – University of Loughborough, United Kingdom
Prof. Paola Manes – Alma Mater Studiorum Università di Bologna, Italy
Prof. Giovanni Martini – Università degli Studi della Campania Luigi Vanvitelli, Italy

European Journal of Privacy Law & Technologies

EJPLT
ISSN: 2704-8012

Prof. Michala Meiselles – University of Derby, United Kingdom
Prof. Alessia Mignozzi – Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Salvatore Monticelli – Università di Foggia, Italy
Prof. Cinzia Motti – Università di Foggia, Italy
Prof. Nora Ni Loideain – Institute of Advanced Legal Studies of London, United Kingdom
Prof. Taiwo Oriola – University of Derby, United Kingdom
Prof. Vincenzo Ricciuto – Università degli Studi di Roma Tor Vergata, Italy
Prof. Francesco Rossi – Università degli Studi di Napoli Federico II, Italy
Prof. Gemma Rubio – Universitat de Barcelona, Spain
Prof. Avv. Laura Valle – Libera Università di Bolzano, Italy
Prof. Isabel Zurita Martin – Universidad de Cádiz, Spain
Prof. Lihong Zhang – East University of Political Science and Law, Shanghai, China

MEMBERS OF THE EDITORIAL BOARD

Prof. Sara Lorenzo Cabrera – Universidad de La Laguna, Spain
Prof. Manuel Pereiro Càrceles – University of Valencia, Spain
Prof. Carlo Ciliberto – University College London, United Kingdom
Prof. Maria Ioannidou – Queen Mary University of London, United Kingdom
Prof. André Janssen – Radboud University Nijmegen, Netherlands
Prof. David T. Karamanukyan – Siberian University, Russian Federation
Prof. Jacopo Martire – University of Bristol, United Kingdom
Prof. Avv. Ranieri Razzante – Università degli Studi di Bologna, Italy
Prof. Avv. Alessandra Sardu – Università degli Studi di Modena e Reggio Emilia, Italy
Prof. Sara Tommasi – Università del Salento, Italy
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. Valeria Manzo – Università degli Studi della Campania Luigi Vanvitelli, Italy
Ph.D. Avv. Anita Mollo – Scuola Superiore Meridionale, Italy
Ph.D. Avv. Michael William Monterossi – Universität Luzern, Switzerland
Ph.D. Sara Saleri – Alma Mater Studiorum Università di Bologna, Italy
Ph.D. Ph.D. Hans Steege – University of Stuttgart, Germany
Ph.D. Kamil Szpyt – Andrzej Frycz Modrzewski Krakow University, Poland
Ph.D. Emiliano Troisi – Università Suor Orsola Benincasa di Napoli, Italy
Ph.D. (c) Noel Armas Castilla – Universidad de Sevilla, Spain
Ph.D. (c) Davide D'Aloia – Università degli Studi Suor Orsola Benincasa, Italy
Ph.D. (c) Alessandra Fabrocini – Sapienza Università di Roma, Italy
Ph.D. (c) Gabriela García Vera – Uniwersytet Rzeszowski, Poland
Ph.D. (c) Emanuele Garzia – Università Suor Orsola Benincasa di Napoli, Italy
Ph.D. (c) Simona Ghionzoli – Università degli Studi di Napoli l'Orientale, Italy
Ph.D. (c) Pablo Guédon – Université Jean Moulin Lyon 3, France
Ph.D. (c) Luigi Izzo – Università degli Studi Suor Orsola Benincasa, Italy
Ph.D. (c) Marie Potus – Université Jean Moulin Lyon 3, France
Ph.D. (c) Michele Scotto di Carlo – Università degli Studi di Napoli Federico II, Italy
Ph.D. (c) Chiara Vitagliano – Università degli Studi di Napoli l'Orientale, Italy

pp.

Editorial

GERARDO VILLANACCI – *The evolutionary constitutional interpretation and the deception of contextualism. | L'interpretazione costituzionale evolutiva e l'inganno del contestualismo.* 9

Section I: **Articles**

ROBERTA MONTINARO – *Responsible data sharing for AI: a test bench for EU Data Law. | Condivisione responsabile dei dati per l'IA: un banco di prova per la normativa UE sui dati.* 17

CLAUDIA IRTI – *Riflessioni sull'impatto delle applicazioni tecnologie nell'ambito sanitario, tra regole etiche e regole giuridiche. | Reflections on the impact of technology applications in healthcare, between ethical rules and legal rules.* 34

JUAN SEBASTIÁN ALEJANDRO PERRILLA GRANADOS – *Lineamientos para implementar la inteligencia artificial en el derecho privado. | Guidelines for implementing artificial intelligence in private law.* 42

GEMMA RUBIO GIMENO – *Vulnerabilidad y digitalización en la contratación de consumo: la perspectiva Española. | Vulnerability and digitalization in consumer contracting: the Spanish perspective.* 59

NIKOLA DACEV, MEVLUDIN IBISH – *Legal Arrangements of Artificial Intelligence in the European Union and the Republic of North Macedonia. | Disposizioni giuridiche sull'intelligenza artificiale nell'Unione europea e nella Repubblica di Macedonia del Nord.* 79

PAOLO GAGGERO, CALOGERO ALBERTO VALENZA – *Le nuove prassi valutative del merito creditizio tra GDPR, CCD II e AI Act. | New Creditworthiness assessment practices between GDPR, CCD II and the AI Act.* 98

MARCO GIACALONE, GIOIA ARNONE – *Dispute Resolutions for Digital Assets in a Decentralized Virtual World. | La risoluzione delle controversie per i beni digitali in un mondo virtuale decentralizzato.* 117

LORENZO DEL FEDERICO – *Riaffermazione e modernizzazione dei diritti dei contribuenti nella trasformazione digitale. | Reaffirmation and modernization of taxpayers' rights in digital transformation.* 136

STEFANO GATTI – *Dalla portabilità alle "portabilità": l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati. | From portability to "portabilities": the evolution in the plural of a key right (and concept) in European data law.* 157

Section II: **Focus papers**

CRISTINA ELENA POPA TACHE, CĂTĂLIN SILVIU SĂRARU, KONSTANTINOS KOUROUPIS – *Different perspectives concerning the right not to use the internet and some analogies with education. | Diverse prospettive sul diritto a non usare internet ed alcune analogie con l'istruzione.* 179

RAMZI MADI – *Protecting Consumer Privacy Under Resolutions on Marketing Through Phone Calls in the UAE. | Protezione della Privacy dei Consumatori secondo le Risoluzioni sul Marketing tramite Chiamate Telefoniche negli Emirati Arabi Uniti.* 194

GIULIO SANTONI – *Un approccio comparatistico all'interpretazione degli obblighi dei gatekeepers nel Digital Markets Act. | A comparative approach to the interpretation of gatekeepers' obligations in the Digital Markets Act.* 205

LUIGI IZZO – *EO Satellite Data Management and Privacy Law. | La gestione dei dati satellitari nell'osservazione della Terra e la tutela della privacy.* 219

FRANCESCA FERRETTI – *Human enhancement ed identità genetica dell'embrione. | Human enhancement and genetic identity of the embryo.* 231

List of authors 252

SECTION I
EDITORIAL

Villanacci G, 'The evolutionary constitutional interpretation and the deception of contextualism' (2024) 1 EJPLT, 9-15.
DOI: https://doi.org/10.57230/EJPLT241GV

EJPLT
ISSN 2704-8012



The evolutionary constitutional interpretation and the deception of contextualism

L'interpretazione costituzionale evolutiva e l'inganno del contestualismo

GERARDO VILLANACCI
Full Professor of Private Law
Università Politecnica delle Marche

Abstract
It is an incontrovertible fact that the hierarchical relationship between principles and values must be defined on the basis of assumptions of contemporary social and economic. A process that, although it is composite, can be carried out due to indeterminacy, the generality and simplicity of the constitutional provisions, which lend themselves to an interpretation that is subject to constant change. However, this can only be done by checking the relevance of the terms used in advance, in the course of time, they may have acquired a different meaning from their original meaning. In the absence of legislation that is in step with new social and economic needs, the only possibility for the judge to reach a resolution of specific cases and at the same time avoid the insidious possibility that certain provisions, even if not strictly unconstitutional, may be anachronistic, is to preserve their operation, through an evolutionary and constitutionally oriented interpretation.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
È un dato incontrovertibile che il rapporto gerarchico tra principi e valori debba essere delineato sulla base di presupposti di contemporaneità sociale ed economica. Un procedimento che per quanto composito può essere attuato in ragione dell'indeterminatezza, genericità e semplicità espositiva delle disposizioni costituzionali che si prestano ad un'interpretazione piegata ai continui cambiamenti. Tuttavia, ciò è possibile soltanto mediante una preventiva verifica dell'attualità del significato delle espressioni utilizzate, che nel tempo potrebbero aver acquisito una diversa accezione rispetto a quella originaria. In difetto di una legislazione al passo con le nuove esigenze sociali ed economiche, l'unica possibilità per il giudice di giungere alla risoluzione di casi concreti e al contempo eludere l'insidiosa possibilità che talune disposizioni, anche se non propriamente incostituzionali, risultino essere anacronistiche, è preservarne la loro operatività, attraverso un'interpretazione evolutiva e costituzionalmente orientata.

Keywords: interpretation; Constitution; contextualism; principles.

Summary: 1. The increase in inter-source conflict supported by the health emergency. – 2 The interpretation in social and economic current affairs. – 3. The judge's resolution of questions of doubtful constitutionality. – 4. The significance of interpretative activity in international jurisprudence. – 5. The prerogatives of judicial interpretation.

1. The increase in inter-source conflict supported by the health emergency.

The health emergency has considerably exacerbated existing problems, from economic and social to legal ones, which have raised new questions for legal interpreters.

Issues that had already been the subject of complex and frequently abstract debates in the past have suddenly and unexpectedly become central to the resolution of the concrete cases. These include the unresolved conflict between the sources and their hierarchy which, due to the partial and largely unimplemented constitutional reforms of recent decades, could not be resolved through systematic interpretative criteria. In today's more than ever evident uncertainty that the reforms have not been decisive and that the unsustainable and incessant legislative productivity has not infrequently been characterized by contradictions and illogicality, a fixed point are the principles and values expressed by the Constitutional Charter which, however, being devoid of behavioral indications aimed at preordaining obligations and prohibitions, cannot be subsumed into preordained schemes being, among other things, in a continuous dialectical relationship between them in which extemporaneous elements are inserted, determining their hierarchical priority.

Generally, it is the Constitution itself that establishes criteria for the greater relevance of principles and values; for example the restriction on movement for health reasons (Article 16 of the Constitution) implies that the protection of the health of the population or even its safety, prevails over freedom of movement insofar as it cannot be compromised by persons carrying contagious diseases. Nonetheless, freedom of movement, as it pertains to the relationship

of the person with the territory, is assisted by a reinforced reservation of the law in the event of its contraction as a result of the exercise of state sovereignty, so that restrictions can only be imposed in a general way and inescapably justified by reasons of health and security.

2. The interpretation in social and economic current affairs.

It is quite common for the hierarchical relationship between principles and values to be delineated on the basis of assumptions of social and economic contemporaneity, albeit in the wake of an interpretation in conformity with the Constitution, the capacity of which to adapt to the needs and prerogatives of society cannot be doubted. On the other hand the vagueness, generality and expositional simplicity of the constitutional provisions lend themselves to an interpretation bent to continuous changes in order to arrive at a specificity aimed at providing an exhaustive answer to the question posed, even if this is only possible through a prior verification of the actuality of the meaning of the expressions used, which over time may have acquired a different meaning from the original one.

Thus, the judge, who is obliged o respect the interpretation in conformity with the Constitution, finds himself having to choose between a substantive profile, taking into account social evolution, or a purely formal one. There is a tendency towards an evolutionary interpretation in cases where, a in the case of the environment we are dealing with matters that are still in the functional construction phase, so as to allow protection also for nascent rights.

However, it would be unjustified not to consider that at times the interpretation in conformity with the Constitution is in divergence with the living law to the point of, in some cases, undermining the relationship between constitutional legality and the prevailing jurisprudential indications. A criticality that inevitably reverberates on the economic system while exacerbating the conflict that has never been resolved between the Constitutional Court and the Court of Cassation, especially with regard to the ownership of the nomofilactic function legitimately claimed by the latter. As will be seen, this is a central issue, which, although more attenuated today than in the past, deserves to be addressed and resolved within a limited timeframe.

In addition, there is an evident increase in the demotivation to resort cross-examination due to the ever more frequent declarations of the Constitutional Court of manifest inadmissibility of questions of unconstitutionality submitted to it. Such decisions are openly taken on the assumption that the referring court instead of resolving a doubt of constitutionality is attempting to have question raised endorse a particular interpretation.

Ultimately what is criticised is that before the finding of unconstitutionality was made, no attempt was even made to the interpret the law in a way that could be constitutionally oriented.

Among the possible consequences is the certainly not minor one of the abuses of constitutionally compliant interpretations which is brought about precisely by the implemented closures of the Constitutional Court.

The concrete risk or rather more relevant risk is not the most feared one of

the reforms at the subsequent levels of judgement of decisions pronounced in clear divergence from the consolidated jurisprudential practice, since innovative interpretation based on the updated review of constitutional principles and values are aimed at overcoming a static condition that is ill-suited to the fluidity of a dynamic society. Rather there is the more insidious possibility that methodological contrapositions allow certain provisions, which if not strictly unconstitutional are evidently anachronistic, to maintain their operativeness. On the other hand, interpretation in conformity with the Constitution implies constant reference to the values and principles contained therein, but also to the fundamental rules and institutions of the state structural system without ever losing sight of the law times relationship.

Ignoring the evolution of society entails failing to recognise that constitutional provisions over time may have assumed, as frequently happens, a semantic valence different from the original one.

A circumstance that obliges the interpreter to a process of adjustment of all norms that have become of dubious constitutional legitimacy in order to recover their harmony with the historical context in which they are to be applied. It's clear that social, but also technical and linguistic changes by emptying the concepts that inspired the norms at the time of their promulgations of their meaning have given rise to new rights and legal situations deserving of protection of which the legislator could not be aware and to whose will, consequently, the interpreter cannot make exclusive reference. Today more than in the past the latter is required in addition to a more careful semantic investigation to take account of the changes that have taken place in order to be able to carry out an interpretation while also assessing the consequences that might reverberate on the related provisions.

Among the possible examples, it is worth mentioning the identifiability of damages from injury to legitimate interests, once excluded since it was recognised only for subjective interests on the basis of a literal restrictive interpretation of the phrase "just damage" as per article 2043 of the Civil Code. In the absence of a specific provision that directly contemplates the identifiability of damage due to injury to legitimate interest, there can be no doubt that the new although consolidated jurisprudential orientation has intervened in consideration of the renewed social political context in which the impunity of the public administration is no longer tolerated due to its unfairness.

3. The judge's resolution of questions of doubtful constitutionality.

The origins of the dispute between ordinary judges and the Constitutional Court which began operating in the spring of 1956, with the sole power to issue rulings either to uphold or reject questions of constitutionality submitted to it, date back to the time when the latter enucleated the innovative typology of interpretative rulings through which provisions deemed to be of dubious constitutionality are reinterpreted. This was a not insignificant leap to overcome the guaranteeist barrier that only required it to perform the interpretation of constitutional norms reserving that of all other laws to the

judge. Leaving aside here the important issue of a correct qualification and distinction between interpretative rulings of rejection and those of acceptance which have engaged scholars of the subject matter, it cannot be overlooked that the dispute in question has been characterised by various phases until the current season in which the broader operative spaces recognised to the common judge are inversely proportional to its abandonment in the face of doubts of constitutionality.

This is a very complex and delicate activity in which he is called upon to assess the concrete needs of society in view of its new values. But also to identify the correct semantic valence of words that in the past had a different one from the contemporary one. As can be seen, this is a composite function that must nevertheless be performed without incurring the abuse of the instrument by avoiding creative – interpretative excesses in the concrete implementation of the new values. There is no doubt that the current conditions of a greater relaxation of relations between the Constitutional Court and the common judges, or rather the Court of Cassation, can make the task easier for the interpreter – judge who is nonetheless burdened with the difficult task of interpreting in conformity with the Constitution without abusing the law while preserving delicate balance between the constitutional and legal order.

Adaptation of the Constitutional Charter to the needs of the community is certainly possible through an evolutionary interpretation that, however, presents alongside significant positive aspects, including first and foremost that of non proceeding to continuous revisions of the constitutional text while substantially updating it, problems that could lead to conditions of regression rather than development if the constitutional principles and values were interpreted predominantly, if not exclusively, in the light of the current context. A pitfall, that of contextualism, arguably greater than all the others, since a central role is assigned to extemporaneous phenomena, even extranormative ones, in the performance of the interpretative function. On closer inspection, this is an anti literalist position that recognises the meaning of the legal rule on the basis of criteria derived from the context. Therefore, an activity that is more than interpretative which being preordained on inductive methods of judicial reasoning could lead to an overordination of the judge's activity, legitimising the opinion of those who believe that the judge creates rather than merely interprets the law albeit in the appreciable but erroneous conviction that he is expressing the will and interests of citizens. A prerogative proper and non expropriatable to representative democracy.

4. The significance of interpretative activity in international jurisprudence.

In this cultural, even before the legal ferment, interpretative activity is increasingly playing a leading role in law also at the international level, due to the increased incidence and relevance of treaties. Among other things, globalization has brought rapid changes that the law must take into account in order to maintain the necessary connection with reality while being aware of the limitations posed by the complexity of the legislative production mechanism. The fight against regulatory obsolescence can only be

implemented through an interpretative method that leaves the legislative provision unchanged and updates it by giving it a more contemporary meaning. However, there is still no unambiguous definition or even detailed analysis of the theoretical assumptions of the concept of evolutionary interpretation. A lack of uniformity that has given rise to different modes of application of the same with which, in any event, it is possible to identify a basic model where there is always an external factor that determines the need for an evolutive interpretation and at the same time the referent object thereof, the original intention of the parties that could also be superseded if it's now deemed devoid of any factual relevance.

5. The prerogatives of judicial interpretation.

In the absence of legislation in step with the new social and economic needs, the only possibility is to access an evolutionary interpretation of the existing rules, while avoiding a legislative amendment. The latter eventuality is highly probable due to the fragile and not always perceptible distinction between the two activities is productive of *ex tunc* effects whereas amendment of the law has *ex nunc* validity as it is limited to the subsequent period of the amended provision.

The considerations made thus far should not lead one to believe that the evolutionary interpretation can be reduced to the extensive one, which unlike the former characterized by a dynamism resulting from external change is static and used to make the most accepted choice.

Not only; the breadth of the category of interpretation requires a more detailed qualification of legal interpretation in order to better understand its constitutional conformity starting from the assumption that insofar as it is directly functional to the application of the law to specific cases, it must combine the generality and abstractness of the regulatory text with the peculiar problems of the case to which the interpreter is called upon to provide an answer.

A process that must be carried out by moving from provisions that can legally qualify situations and therefore not limited to a reconnaissance function of the legislator's will but to its concrete application in compliance with the mandatory rules of conduct imposed by the legal system. Denying the possibility of a constitutional adaptation to social changes fearing that this might legitimise recourse to a creative jurisprudence harbinger of restrictions on fundamental freedoms, reserving exclusively to the legislator the task of updating the Constitution to the changing times rather than proceeding with an interpretation of the same in line with social transformation, means re-proposing outdated textualist theories characterised by the anachronistic search for the meaning of the expressions contained in the rule taking them back to the time of its promulgation.

In reality the real issue is to provide clear guidelines for the implementation of the interpretative process in order to prevent the updated provisions from being abstract and personalistic as well as lacking a balanced relationship with the purposes pursued by the legislator.

The priority assigned to literal interpretation must however be combined, especially with regard to rules of law dating back in time for which there is an inevitable disconnection with the historical – social context in which they are to be applied with an effective interpretative technique that is consistent with cultural, social and economic change, since only in this way can it be sensitive to the factual values of which society is the bearer.

Nonetheless, since the Provisions of the law in general came into force before the Constitution, it's well to give an account of the still non entirely resolved contrast as to the possibility of applying the interpretative mechanism of Art. 12 to constitutional provisions. A contrariety also endorsed by the deemed superfluousness of said interpretation given the indeterminate character of constitutional provisions with factual values, the expression of the historical social moment in which they are called upon to operate. This is all the more so if one considers that such indeterminateness is the result of their hierarchical prevalence and function of norms that are the bearers of values and principles that are the foundations of our society.

On the other hand, a different orientation is that of those, who tend to extend the applicability of Art. 12 of the "Provisions on the law in general" on the assumption that the latter has a general scope. And in any event the vagueness of the wording of the constitutional provision is not a hindrance since it is a characteristic common to all legal norms, including ordinary laws, which are characterized by the vagueness of the terms and linguistic expressions used.

SECTION II
ARTICLES

Montinaro R, 'Responsible data sharing for AI: a test bench for EU Data Law' (2024) 1 EJPLT, 17-33.
DOI: https://doi.org/10.57230/EJPLT241RM

EJPLT
ISSN 2704-8012



Responsible data sharing for AI: a test bench for EU Data Law

Condivisione responsabile dei dati per l'IA: un banco di prova per la normativa UE sui dati

ROBERTA MONTINARO
Full Professor of Private Law
Università degli Studi di Napoli L'Orientale

Abstract
The paper addresses data sharing contracts for AI development and training, entered into by parties participating in AI value chains, in order to assess the incentives for responsible data sharing under European data law. As the governance of AI training data is mainly entrusted to party autonomy and the principles of the GDPR, the analysis first assesses whether contract theory, as it is traditionally conceptualized, is an appropriate tool to promote responsible data sharing. Then the paper delves into the impact of the mandatory data protection framework on data sharing contracts, to conclude that the principle of accountability in its organizational dimension requires the parties to 'contractualize' good data sharing practices. Lastly, the analysis comprises a brief overview of the relevant provisions of the AI Act that deal with data governance and AI value chains, to highlight their impact on the relationship between the entities participating in these value chains.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Il documento affronta i contratti di condivisione dei dati per lo sviluppo e l'addestramento dell'IA, stipulati dalle parti che partecipano alle catene del valore dell'IA, al fine di valutare gli incentivi per una condivisione responsabile dei dati ai sensi della normativa europea sui dati. Poiché la governance dei dati relativi all'addestramento dell'IA è principalmente affidata all'autonomia delle parti e ai principi del GDPR, l'analisi valuta innanzitutto se la teoria dei contratti, così come è stata tradizionalmente concepita, sia uno strumento appropriato per promuovere una condivisione responsabile dei dati. In seguito, il contributo approfondisce l'impatto del quadro normativo obbligatorio in materia di protezione dei dati sui contratti di condivisione dei dati, per concludere che il principio di responsabilità nella sua dimensione organizzativa richiede alle parti di "contrattualizzare" le buone pratiche di condivisione dei dati. Infine, l'analisi comprende una breve panoramica delle disposizioni rilevanti della legge sull'IA che riguardano la governance dei dati e le catene di valore dell'IA, per evidenziare il loro impatto sulle relazioni tra le entità che partecipano a queste catene di valore.

Keywords: data sharing; contracts; AI value chains; data protection; European data law.

Summary: 1. Introduction. – 2. Data sharing contracts seen from the viewpoint of traditional contract theory. – 2.1. Recent Evolutions in EU Data Law. – 2.2. Model Rules on Contracts for the Provision of Data: Fit for AI Training Data? – 2.3. Shortcomings of Traditional Contract Theory. – 3. The Impact of GDPR on Data Sharing Contracts for AI. – 4. The AI Act: Data Governance and AI Value Chains. – 5. Conclusions.

1. Introduction.

Responsible data governance with respect to Artificial Intelligence (hereinafter 'AI') is a field of research that tries to reconcile two perspectives which underpin European Union data law (hereinafter 'EU data law')[1]: on the one hand, fostering innovation by favoring the availability of data and, on the other hand, ensuring protection to personal data and, more broadly, to the fundamental rights of the individuals and groups affected by the deployment of AI applications. The Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act, hereinafter 'AI Act')[2] seeks as well to bridge these two perspectives. It states that one of the main purposes of the Regulation is to promote a high level of protection of fundamental rights, according to the Charter of Fundamental Rights of the European Union (hereinafter the 'Charter'), starting from the development phase of AI applications (Article 1 and Recital 1 AI Act). At the same time, the Ai Act acknowledges that access to

[1] N Riis, 'Shaping the field of EU Data Law' (2023) 14 JIPITEC, 54. See also T Streinz 'The Evolution of European Data Law', in P Craig, G de Búrca (eds), *The Evolution of EU Data Law* (Oxford University Press USA, 2021), 903.
[2] European Parliament and Council Regulation (EU) 1689/2024 of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] OJ L. (Artificial Intelligence Act).

data, namely to data of high quality, plays a vital role in preventing and mitigating any risk of harm to those rights (Recitals 66 and 67 AI Act).

When machine learning techniques are applied, data comes into consideration in view of its function as training data and any lack of data quality or any deficiency in the data generation and management processes can be a source of harm to the fundamental rights of data subjects, particularly when AI is used in decision-making processes that impact individuals or groups.[3]

Data sharing for AI mainly takes place by means of contracts that can be simple arrangements between two parties or multilateral complex agreements. These contracts are often entered into in the context of the so-called AI value chains in which multiple entities may participate, including entities contributing data.

The aim of this paper is to explore data sharing contracts[4] for the purpose of developing and training AI, entered into by parties participating in AI value chains, to assess the incentives to engage in responsible data sharing for AI under EU data law.

Responsible data sharing entails, at the very minimum, compliance with personal data regulations, prevention of bias and discrimination and respect for human rights.

As will be noted in paragraph 2, the normative instruments recently enacted by the EU fall short to promote the accountability of the parties to a data sharing contract. Regulation (EU) 2022/868 on European data governance (Data Governance Act, hereinafter 'DGA')[5] and Regulation (EU) 2023/2854 on harmonized rules on fair access to and use of data (hereinafter 'Data Act')[6] are both concerned with establishing a 'data economy' and entrust the protection of fundamental rights to Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation, hereinafter 'GDPR')[7], as well as to other relevant EU and national laws.[8]

As a consequence, the governance of AI training data is mainly entrusted to party autonomy and to the principles of the GDPR.

Data sharing contracts are indeed subject to the applicable contract law regimes of Member States. Against this background the analysis will firstly consider the viewpoint of contract theory (as it is traditionally conceptualized),

---

[3] H Suresh, J Guttag, 'A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle' (2021) Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO '21), 1 <https://doi.org/10.1145/3465416.3483305> accessed 1 February 2024. See also P Hacker, 'A Legal Framework for AI Training Data - From First Principles to the Artificial Intelligence Act' (2020) Law, Innovation and Technology, 12 <https://ssrn.com/abstract=3556598> or <http://dx.doi.org/10.2139/ssrn.3556598> accessed 1 February 2024.

[4] Within the present paper, the terms 'supply' and 'sharing' of data will be used interchangeably, to describe a one-way provision of data, as well as a two-way provision of data, where the parties provide data to one another.

[5] European Parliament and Council Regulation (EU) 868/2022 of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L152/1 (Data Governance Act).

[6] European Parliament and Council Regulation (EU) 2854/2023 of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 [2023] OJ L. (Data Act)

[7] European Parliament and Council Regulation (EU) 679/2016 of 27April 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 [2016] OJ L119/1. (General Data Protection Regulation).

[8] See in this regard Recitals 7 and 8 Data Act.

referencing some relevant soft law instruments which have been devised with the aim to set out model rules on data sharing contracts.

Then paragraph 3 will analyze how the GDPR interacts with contract law, to conclude that the data protection framework constrains the autonomy of the parties to a data sharing agreement by shaping the contractual relationship.

Lastly, the analysis will conclude with a brief overview of the relevant provisions of the AI Act which deal with data governance and AI value chains, to highlight their impact on the relationship between the parties to data sharing contracts (paragraph 4).

The AI Act sets out requirements on the quality of training data and mandates the use of adequate data governance practices. This results in due diligence obligations, but only for providers of AI applications that fall under the definition of high-risk systems. The AI Act Proposal was only intended for providers and users of AI systems, not including those who provide data for the development and training of such systems,[9] whereas the AI Act recognizes the complexity of AI value chains and consequently requires third parties involved in the development of AI systems to cooperate with providers of high-risk AI systems to enable them to comply with the requirements therein set out (Recital 88).[10] In this way, the Regulation entrusts the accountability of all participants in AI value chains to the agreements between the parties and to 'model clauses' to be drafted by the AI Office.

2. Data sharing contracts seen from the viewpoint of traditional contract theory.

2.1. Recent Evolutions in EU Data Law.

As above mentioned, the EU legal framework currently comprises the DGA and the Data Act, which have been added to the GDPR in order to implement the 'European strategy for data'[11]. As clarified by their respective preambles, both the DGA and the Data Act are mainly concerned with fostering the establishment of a European 'data economy'. As a consequence, they do not directly address the role played by data in the context of AI development and training.

The DGA focuses on ensuring the neutrality and accountability of data intermediaries falling within its scope of applications with regard to non-personal and personal data in general. It entrusts the protection of the

[9] Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)' COM (2021) 206 final.

[10] It is worth noting that the AI Act Proposal with the amendments adopted by the European Parliament on 14 June 2023 (hereinafter 'AI Act Proposal of June 2023') contained explicit reference to those providing data for the development of AI systems: "all relevant third parties, in particular those that are involved in the development, sale and the commercial supply of […] data incorporated into the AI system" shall cooperate with providers of AI systems to enable them to comply with the AI Act (Recital 60 of the AI Act of June 2023).

[11] See Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data' COM (2020) 66 final.

fundamental rights of data subjects to the relevant EU legislations, most notably, to the GDPR.

There is much evidence to support this. Under the DGA, the data intermediaries only bear a fiduciary duty towards the data subjects - to act in their best interest - when their business model is centered on facilitating the exercise of data subjects' rights (Article 12 (l)). Duties of care of data intermediaries with regard to third parties' rights are only provided for with respect to non-personal data, such as: *i)* taking the necessary legal, organizational and/or technological measures (see Articles 10 and 12 DGA) to avoid transmission and access to non-personal data which is unlawful under Union or national law; *ii)* adopting measures necessary to ensure an adequate level of security for the storage and transmission of non-personal data (Article 10, (1) DGA).

Moreover, the scope of application of the DGA only covers data sharing services aiming at intermediating between an indefinite number of data holders and data users, excluding data sharing services that are meant to be used by a closed group of data holders and users (see Recital 28 DGA). This requirement may leave outside the reach of the DGA several data governance models that are especially suitable for the development and training of AI, for instance, data clearinghouses (which may come in various forms; e.g. data transfer, consent management etc.) and data pools, [12] whenever the governance of the pooled data is entrusted to an intermediary that facilitates data sharing between predefined data holders and users.[13]

The Data Act sets out obligations for data holders to make both personal and non-personal data available to users of connected products and related services; it establishes rules for business-to-business and business-to-consumer data sharing, as well as rules on unfair terms related to data access and use between enterprises (see Article 1 Data Act).[14]

Examining this in detail, its scope of application covers data agreements on: *i)* access and use of data concerning the performance, use and environment of connected products and related services [Chapter II]; *ii)* private sector data that is subject to statutory data sharing obligations under Article 5 of the Data Act or under national legislation adopted in accordance with Union law (Chapter III); and *iii)* private sector data accessed and used on the basis of a contract between enterprises (Chapter IV).

Like the GDA, the Data Act is not directly concerned with protecting the rights of third parties that may be affected by the data sharing agreement, such as a right arising from the GDPR. Rather, the Data Act merely clarifies that its provisions do not affect the protection of personal data and that the sharing of

[12] See A Wernick, C Olk, M Grafenstein, 'Defining Data Intermediaries. A Clearer View through the Lens of Intellectual Property Governance' (2020) 2 Technology and Regulation, 70 <https://doi.org/10.26116/techreg.2020.007> accessed 28 January 2024.

[13] See Recital 28 DGA: "Examples of data intermediation services include […] data pools established jointly by several legal or natural persons with the intention to license the use of such data pools to all interested parties in a manner that all participants that contribute to the data pools would receive a reward for their contribution".

[14] M Hennemann, G Ebner, B Karsten, 'The Data Act Proposal – Literature Review and Critical Analysis - Part I (Art. 1-13, 35)' (2023) University of Passau Institute for Law of the Digital Society Research Paper 1/2023, 6 <www.jura.uni-passau.de/irdg/publikationen/research-paper-series> accessed 25 January 2024.

personal data can only lawfully take place if there is a legal basis in accordance with the GDPR (see Recital 7[15] and Article 4 (12) Data Act)[16].

The Data Act does take into account the quality of the data covered by the data sharing agreement in some of its provisions. In particular, Articles 4 (1) and 5 (1) Data Act stipulate that the data holder must make accessible to the counterparty data of the same quality as is available to the data holder. The rationale of these provisions, however, seem to lie in the need to regulate the interests of the parties. At the same time, according to Article 13 (4) (g) Data Act, contract terms relating to data quality cannot be modified by a unilaterally imposed term, which would be unfair and thus not binding on the other party. Since this is a type of unfair clause, here too it is reasonable to argue that such a provision is intended to address contractual imbalances that may hinder fair access to and use of data by the parties to such agreements.

Thus, despite these recent regulations that have been added to European data law, data governance for AI remains predominantly in the realm of party autonomy, as will be demonstrated in the following analysis. However, it will also be argued that the GDPR - and, albeit to a much lesser extent, the AI Act - shape the autonomy of the parties to data-sharing contracts, in ways that will be discussed in paragraphs 3 and 4.

2.2. Shortcomings of Traditional Contract Theory.

Traditional conceptualizations of private autonomy - whereby the parties to a contract are only bound by what is agreed between them with a view to protecting their own interests - are put 'under strain' when data is the subject matter of the contract. Personal data, in particular, is at the heart of several regulations, such as the GDPR. The latter, on the one hand, takes into account the private dimension inherent in the circulation of personal data and its use for economic purposes; on the other hand, it also aims to protect the rights and interests of the natural persons concerned by the processing.

The parties to a data sharing agreement regard data as a commodity, but, at the same time, they are aware that the data sharing may involve a number of legally protected interests, including rights protected by mandatory legislations. As a consequence, they tend to be risk-averse and inclined to design the contract terms in such a way to satisfy their interests and to manage the risk of being held accountable for non-compliance with public law regimes or incurring liability for any harm to third parties' rights under tort law regimes enacted at a national level or at the level of EU law.

Indeed, one of the functions of such regimes is precisely to deter unlawful forms of data sharing. This, however, provided that they have an adequate level of effectiveness.

If we consider tort law, and namely, the EU product liability regime, as it

[15] According to Recital 7 Data Act the legal basis for sustainable and responsible data processing, even where data sets include a mix of personal and non-personal data, is provided for solely by the GDPR.

[16] Article 4 (12) of the Data Act :"Where the user is not the data subject whose personal data is requested, any personal data generated by the use of a connected product or related service shall be made available by the data holder to the user only where there is a valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled." In this vein, see also Article 5(7) of the Data Act.

currently stands, we can find that it only insufficiently contributes to promoting responsible data sharing for AI. It suffices to mention two aspects that are relevant for the purpose of this analysis.

Under the Council Directive 85/374/EEC of 25 July 1985 concerning liability for defective products (Product Liability Directive, hereinafter "PLD")[17], it is debated whether AI systems and input data, due to their nature as intangible goods, can be regarded as a product (or a component thereof); at the same time, the complexity and opacity of AI systems entail that it is difficult for the injured party to meet the burden of proof.[18]

These obstacles are likely to be overcome if the PLD will be updated by the Proposal for a Directive on Liability for Defective Products (proposal for a New Liability Directive, hereinafter "NLD")[19]. Therein, the definition of 'component' appears to be broad enough to include the data supplied to the value chains of an AI system (see Article 4 (2) NLD)[20]. A mechanism of disclosure is provided for in Article 8 NLD to alleviate the burden of proof resting on the claimant.[21]

Entrusting the governance of AI training data to party autonomy entails further shortcomings.

First, contract terms providing for limitation or exclusion of liability for breach of contract agreed upon by the parties to a data sharing contract may shift the risk of being held accountable onto one party. Under Article 13 of the Data Act, such contract terms are not binding when they are included in data contracts between enterprises,[22] but only if the breach of contracts results from intentional acts or gross negligence of the party who imposed the

[17] Council Directive 1985/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (Product Liability Directive) OJ L 210/29.

[18] C de Meeus 'The Product Liability Directive at the Age of the Digital Industrial Revolution: Fit for Innovation?' (2019) 8(2) EuCML, 149. See also BEUC The European Consumer Bureau, 'How to make product liability fit for consumers in the digital age' (07 May 2020, BEUC-X-2020-024) <www.beuc.eu/sites/default/files/publications/beuc-x-2020-024_product_liability_position_paper.pdf> accessed 27 January 2024.

[19] Commission, 'Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products' COM (2022) 495 final/2.

[20] Article 4 (2) NLD: "'component' means any item, whether tangible or intangible, or any related service, that is integrated into, or inter-connected with, a product by the manufacturer of that product or within that manufacturer's control". Whether this definition covers, as well, data is a matter of interpretation.

[21] However, the mechanism of disclosure provided for in Article 8 NLD can only be used in the course of the litigation and on condition that the plaintiff has provided sufficient elements to substantiate the plausibility of its claim. In the same vein, under Article 3 of the Proposal for a Directive of the European Parliament and the Council of 28 September 2022 on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM (2022) 496 final), the presumption of causation also applies to damage caused by high-risk AI systems whenever the court deems it excessively complex for the injured party to prove the causal link. See R Gellert, A Janssen, 'The Impact of Artificial Intelligence on European Contract Law: Talking Stock to an Ongoing Process', in A Janssen, M Lehmann, R Schulze (eds.), *The future of European Private Law,* (Nomos 2023) 169-194.

[22] See Article 13 (1) Data Act: "1. A contractual term concerning access to and the use of data or liability and remedies for the breach or the termination of data related obligations, which has been unilaterally imposed by an enterprise on another enterprise, shall not be binding on the latter enterprise if it is unfair". According to Article 13 (2) Data Act: "In particular, a contractual term shall be unfair for the purposes of paragraph 3, if its object or effect is to: (a)exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence; (b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in the case of non- performance of contractual obligations, or the liability of the party that unilaterally imposed the term in the case of a breach of those obligations; (c) give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any contractual term".

contract term. Therefore, this rule aims to rebalance unequal relationships between economic operators active in data markets. It differs from provisions which prohibit exclusion or limitation clauses contravening public order[23] and, in particular, clauses on the exclusion or limitation of contractual liability for physical harm or harm to personality rights.[24]

Second, liability under contract law does not extend beyond the parties to the contract and, hence, it fails to promote the accountability of all those who share data for AI development (for instance, in the case of a chain of data sharing contracts).

Moreover, the third parties impacted by the deployment of AI applications are not entitled to claim damages under contract law, unless they qualify as end-users that can seek compensation from the seller under Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services (hereinafter 'DCDS Directive')[25] and Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods (hereinafter 'CSD')[26]. In this case, incentives for developers of AI systems to comply with data protection principles can only arise from the right of redress that the seller can exercise against a person in the previous links of the transaction chain, whose action or omission resulted in the lack of compliance (see Article 18 CSD and, in the same vein, Article 20 DCDS Directive).[27]

2.3. Model Rules on Contracts for the Provision of Data: Fit for AI Training Data?

The party autonomy logic above described is reflected in some soft law documents aiming to set out uniform model rules and implied terms for the cross-border flows of data.

According to the American Law Institute and the European Law Institute's Principles for a Data Economy: Data Transactions and Data Rights (hereinafter 'ALI/ELI Principles for a Data Economy')[28], in contracts for the 'supply' or 'sharing' of data, the data recipient must be enabled "rightfully to exercise control over the data" (Principle 7(2)(c)(ii))[29]. At the same time, "the data

[23] The Italian civil code qualifies as null and void any terms that exclude or limit liability for breach of contract for intentional acts and gross negligence, irrespective of whether these terms are unilaterally imposed (Article 1229 Italian civil code).

[24] See H Claes, M Herbosch 'Artificial Intelligence and Contractual Liability Limitations: A Natural Combination?' (2023) ERPL 31 (2-3), 475.

[25] European Parliament and Council Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1.

[26] European Parliament and Council Directive (EU) 2019/771 of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L 136/28.

[27] P Hacker, 'A Legal Framework for AI Training Data - From First Principles to the Artificial Intelligence Act' (2020) 18 Law, Innovation and Technology, 11 <https://ssrn.com/abstract=3556598> or <http://dx.doi.org/10.2139/ssrn.3556598> accessed 1 February 2024.

[28] The American Law Institute, The European Law Institute, 'Principles for a Data Economy: Data Transactions and Data Rights' (2023) <www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy.pdf> accessed 20 January 2024.

[29] The rationale behind Principle 7(2)(c)(ii) of ALI/ELI Principles for a Data Economy is explained as follows: "the usefulness of data to the recipient would be undermined if the recipient did not obtain rightful control over the data at the time it is supplied". "The supplier must therefore ensure that, for example, there are no

recipient may utilize the data […] for any lawful purpose and in any way that does not infringe the rights of the supplier or third parties […]" (Principle 7(2)(c)(iv)).[30]

In the same vein, under the Default rules for data provision contracts (hereinafter 'UN Default rules for data provision contracts') issued by the United Nations Commission on International Trade Law[31], the data must be provided lawfully (Article 7 (2)(d)). Moreover, the data recipient is entitled to use the data for any lawful purpose (so "that the data recipient can exercise its rights to use the data under the contract")[32] and in a manner that does not infringe the rights of third parties (Article 8 (1) (a) and (2) (a)).

In a nutshell, the lawfulness of the data provided or made accessible under these contracts pertains to the conformity of the data[33] and covers compliance with any applicable legal requirements;[34] at the same time, lawfully using the data is a contractual obligation towards the data supplier that the data recipient must comply with, to ensure that the data provider is not held liable under the law.

Some conclusions can be drawn from these soft law documents. The contract terms therein devised are shaped by the private interests of the parties. They do not reflect the legal status of data which differs from tradable commodities.[35]

The ELI/ALI Principles for a Data Economy do recognize the existence of third parties' rights, including rights with *erga omnes* effect, which may be affected by data sharing or 'data activities' (e.g. how data are handled, their quality, security, etc.). However, these Principles: *i)* on the one hand, adopt a 'tort law logic' in that they merely reiterate that the data processing activity may be unlawful towards third parties holding *erga omnes* rights; ii) on the other hand, entrust the determination of legal remedies available to the affected third parties to the applicable law (see Principles 4, 28, 29). Similarly, with regard to the matters of the effects of the transmission of data on the protection of others and direct actions by a data supplier towards a downstream recipient these Principles refer the matter to the applicable law(see Part IV, Chapter B,

---

legal barriers that would prevent the recipient from rightfully gaining control. Legal barriers could be barriers stemming, e.g., from data privacy/data protection law, from intellectual property law, or from trade secrets law".

[30] From the perspective of the ALI/ELI Principles for a Data Economy, third party rights, including fundamental rights, help to define the data rights conferred on the recipient of the data under the contract. See ALI/ELI Principles for a Data Economy, p. 10: "Among the policy choices recommended by these Principles in the context of supply or sharing of data is the default position that, when the data is fully transferred, the data may be used by the recipient for any lawful purpose that does not infringe the rights of third parties".

[31] Working Group IV on Electronic Commerce, 'Default rules for data provision contracts (first revision): Note by the Secretariat' (United Nations Commission on International Trade Law, Vienna 16-20 October 2023) <https://documents-dds-ny.un.org/doc/UNDOC/LTD/V23/064/75/PDF/V2306475.pdf?OpenElement> accessed 22 January 2024.

[32] UN Default rules for data provision contracts (2023) 13.

[33] In this respect, these soft law instruments mirror Article 10 DCDS Directive: Third-party rights: "Where a restriction resulting from a violation of any right of a third party, in particular intellectual property rights, prevents or limits the use of the digital content or digital service in accordance with Articles 7 and 8, Member States shall ensure that the consumer is entitled to the remedies for lack of conformity […]".

[34] See Article 7 (2) (d) UN Default rules for data provision contracts.

[35] See V Janeček, G Malgieri, 'Data extra commercium', in S Lohsse, R Schultze and D Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?* (Hart Publishing/Nomos 2020), 2 <https://ssrn.com/abstract=3400620> accessed 1 February 2024.

Principles 32 and 33 respectively), only suggesting that a 'model rule' is one that provides for due diligence obligations for the party supplying the data with respect to wrongful activities of the other parties in the chain of contracts for the provision of data.

Above all, the soft law instruments already mentioned do not take into account the peculiarities of the data used in the context of AI development/training. As explained by experts in the field of machine learning, the data used for this purpose is not a static artefact; on the contrary, it is the result of choices and practices to be implemented during the phases of data collection and generation and model development. Possible sources of harm to fundamental rights may result from poor choices and practices at these stages.

In order to prevent such harms, the terms of data-sharing agreements should include good practices, such as: *i)* requiring 'data traceability', *ii)* setting forth transparency requirements (for instance, documentation on how input data are generated and managed), *iii)* mandating to identify adequate technical standards/practices.

Soft law alone appears ill-suited to ensure that good practices and technical standards become binding and thus subject to enforcement. It is therefore relevant to identify the incentives offered by European data law to engage in responsible data governance, in particular, with regard to personal data used for the development of AI applications.

3. The Impact of the GDPR on Data Sharing Contracts for AI.

The interaction of the GDPR with contract law challenges the corollaries of traditional contract theory above mentioned.

Owing to the peculiar nature of data, when the subject matter of a contract is the provision of data, several legally protected interests may come into play, including the right to the protection of personal data and other fundamental rights, such as the right not to be discriminated against.

Indeed, the provision of personal data to the recipient of the data pursuant to a data sharing agreement implies a form of processing within the meaning of Article 4 (2) GDPR. Accordingly, the data protection legal framework applies, which aims, inter alia, to protect the fundamental rights and freedoms of natural persons (see Article 1 (2) GDPR).

Under EU data law, where non-personal and anonymized data are processed, and technological developments make it possible to turn this data into personal data, the data protection framework comes into play (see Recital 9 of the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union (hereinafter 'FFDR')[36]). In light of this, the key concept for defining the character of data is 'identifiability' (see Article 4(1)

[36] European Parliament and Council Regulation (EU) 1807/2018 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303. According to Recital 9 FFDR "Recital 9 of the FFDR "If technological developments make it possible to turn anonymized data into personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 is to apply accordingly".

GDPR). As highlighted by legal scholars and case law,[37] identifiability is a dynamic and context-dependent concept. There is a strong argument that the qualification of data as personal must take into account inter alia the 'life cycle' of the data. This can be deduced from Recital 26 GDPR, which refers to anonymous data, i.e. data rendered anonymous in such a manner that the data subject is not or is *no longer* identifiable.

Against this background, the relevant international technical standards (ISO/IEC 27701) rely on the concept of *Personally Identifiable Information* (hereinafter 'PII')[38]. These standards suggest that any data that *i)* can be used to establish a link between the information and the natural person to whom it relates or *ii)* can be directly or indirectly linked to a natural person should be regarded as PII and managed by taking into account any risk of harm to third parties. Therefore, the substantive scope of application of the data protection framework is not narrow, as some scholars point out.[39]

The public law regime set out by the GDPR entails constraints on party autonomy, since personal data can only be processed in conformity with the principles of lawfulness and fairness enshrined in article 5 GDPR. The requirements arising from the data protection framework translate into limits on entitlements and rights of the parties to data sharing contracts, as well as into duties for the same parties.[40] These constraints and duties shape the contractual relationship between the parties to such contracts.

For instance, in the Italian legal system, as interpreted by the Supreme Court (no. 15824/2014), compliance with duties of care arising from public law regulations, such as the EU Regulation on food safety, constitutes a contractual obligation resting with both the parties to a sales contract: they are required to proactively comply with the regulation in order to ensure a high level of protection of the rights of consumers; failing to fulfil such obligations may result in liability for breach of contract and/or contract termination. Some legal scholars point out that duties of this kind lie in the grey area between tort and contractual liability, having their origin in the fact that the liable party is entrusted with the protection of the person or property of the other party and/or a third party.[41]

A similar finding holds with regard to Article 16 DCDS Directive: "In respect of personal data of the consumer, the trader shall comply with the obligations

---

[37] Judgment of 19 October 2016, *Patrick Breyer vs Bundesrepublik Deutschland*, C-582/14, EU:C:2016:77 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0582>. See, as well, I Graef, R Gellert, M Husovec, 'Towards a holistic regulatory approach for the European data economy: why the illusive notion of non-personal data is counterproductive to data innovation' (2018) 29 TILEC Discussion Paper, 7 <https://ssrn.com/abstract=3256189> or <http://dx.doi.org/10.2139/ssrn.3256189>.

[38] E Podda, M Palmirani 'Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data', in V Rodríguez-Doncel, M Palmirani, M Araszkiewicz, P Casanovas, U Pagallo, G Sartor (eds), *AI Approaches to the Complexity of Legal Systems XI-XII: AICOL 2020, AICOL 2018, XAILA 2020. Lecture Notes in Computer Science*, vol 13048 (Springer, 2021) 4.

[39] N Purtova 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) Law Innov. Technol., 40-81<https://doi.org/10.1080/17579961.2018.1452176> accessed 29 January 2023.

[40] S Orlando 'Il coordinamento tra la direttiva 770/2019 e il GDPR. L'interessato-consumatore' (2023) 2 Persona e mercato, 232.

[41] C Castronovo 'L'obbligazione senza prestazione ai confini tra contratto e torto', in G Alpa and others, *Le ragioni del diritto. Scritti in onore di Luigi Mengoni* (Giuffré, 1995) vol I, 147. See L Nivarra 'Alcune precisazioni in tema di responsabilità contrattuale' (2014) 1 Europa e diritto privato, 73.

applicable under Regulation (EU) 2016/679". This provision can be read as it entails that non-compliance with the GDPR is also relevant from the point of view of contract law.[42]

Moreover, the data protection framework covers automated decision-making that often involves the deployment of AI systems which may have significant adverse impacts on individuals (Article 22 (1) GDPR).[43] Automated decision-making of this sort is per se prohibited, but Article 22 (2) GDPR provides for several exceptions. When one of these exceptions applies, transparency requirements are set out and the adoption of adequate measures is mandated (Article 22 (3)) according to the principles of accountability and privacy by design (see Articles 5, 22, 24 and 25; Recital 71 GDPR), in order to prevent such impacts.[44]

These principles interact with party autonomy by establishing duties of care on the parties that share and manage data for the purpose of training/developing AI applications.

As highlighted by some authors, the principle of accountability has an organizational dimension, since it places on controllers the duty to also adopt the 'legal' measures that enable them to comply with the GDPR. Therefore, the parties to these contracts are required to arrange adequate data sharing architectures, starting with the choice of the contract type and contract terms,[45] which should be made taking into account the complexity and severity of the risks entailed in the processing (which are a variable of the purpose of the AI system and type of data needed). As for the choice of contract type, for instance, where there is a large number of data contributors, the creation of data pools instead of a chain of contracts can be considered in line with these principles. In fact, this type of agreement allows each party to monitor whether the other parties comply with data protection requirements. In this way, all the parties to the contract are required to responsibly manage the data.

Moreover, when an AI application is meant to be used for decision making purposes, the parties that confer the training data are required to ensure data quality and use adequate processes of data generation and management. This aspect has been underlined by the EDPB-EDPS Joint Opinion on the interplay between the AI Act and the GDPR:[46] AI systems should be conceived and developed having in mind data protection principles and rules, such as the ones which require to adopt adequate safeguards to prevent any harmful impact arising from automated decision making having legal or similarly significant effects on a data subject (Article 22 and Recital 71 GDPR).

---

[42] G Resta, *Autonomia privata e diritti della personalità* (Jovene, 2005) 281.

[43] Judgment of 7 December 2023, *OQ vs Land Hessen*, C-634/21, EU:C:2023:957 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0634>.

[44] ME Kaminski 'The right to explanation, explained' (2019) 34(7) Berkeley Technology Law Journal <https://ssrn.com/abstract=3196985> or <http://dx.doi.org/10.2139/ssrn.3196985> accessed 31 January 2024.

[45] S Stalla-Bourdillon and others, 'Data protection by design: Building the foundations of trustworthy data sharing' (2020) 2 Data & Policy, 5.

[46] EDPB-EDPS, 'Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)' (21 June 2021) point 58 <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en> accessed 31 January 2024.

One way to comply with the principle of accountability and privacy by design is to choose adequate contract terms. This means that the duties of care arising from the data protection framework can be 'contractualized' and turned into due diligence contract terms included in the data sharing contracts.

Contract terms of this sort may compel the parties to such contracts to adopt: i) technical and procedural standards and practices on matters such as the ones mentioned in Paragraph 2.2 ii) mechanisms to oversee compliance with these standards/practices by all the parties (for instance, mandating to carry out internal audits or reporting) and iii) enforcement mechanisms (for instance, penalty clauses, contract termination clauses etc.) in the event of non fulfilment of these duties. Along the same lines are contract terms requiring the parties to monitor whether sub-suppliers comply with data protection requirements.

As a consequence, the adoption of good practices and standards is not left to market drivers.[47] On the contrary, it is triggered by the public law provisions at play and notably by the principle of accountability which is a regulatory model for the protection of personal data based on a hybrid form of enforceable self-regulation.[48]

The GDPR already provides for some form of private enforcement. According to Article 82 GDPR, data controllers (and processors) are liable for damage resulting from a processing that does not comply with the rules and principles laid down in the GDPR. However, a right to compensation is afforded under certain conditions. i.e. an infringement of the Regulation, the existence of a material or non-material damage and a causal link between these two elements (Article 82(1) GDPR). Furthermore, when a processing is complex and involves multiple parties and processing operations, these parties may qualify as *i)* processors or separate and independent controllers (or a combination of the two) or *ii)* as joint controllers. The claimant must therefore prove the existence of all such conditions. It is correct that an easing of the burden of proof is provided for in Article 82 (4) GDPR, according to which the multiple parties involved in the same processing may be held jointly and severally liable. In this case, the full amount of compensation may be recovered from one of these multiple parties, but only provided that the requirements of Article 82 (2) and (3) GDPR are met, in addition to their '*involvement*' in the processing.

Above all, the one just described is a form of tort liability having a compensatory function.[49] A further policy objective is to prevent infringements of data protection regulations and the resulting harm to data subjects. This objective underpins Article 26 GDPR which mandates joint controllers to clarify their roles and responsibilities in an agreement (Article 26 GDPR). The agreement to be adopted by the joint controllers under this provision is

[47] K Peterkova Mitkidis, 'Sustainability Clauses in International Supply Chain Contracts: Regulation, Enforceability and Effects of Ethical Requirements' (2014) 1 Nordic Journal of Commercial Law, 7 <www.researchgate.net/publication/299269785_Sustainability_Clauses_in_International_Supply_Chain_Contracts_Regulation_Enforceability_and_Effects_of_Ethical_Requirements> accessed 22 August 2024.

[48] A Spina, 'Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al regolamento (Ue) 2016/679' (2016) 1 Rivista della regolazione dei mercati, 148. See also G Comandé 'Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità' (2019) 1 Analisi giuridica dell'economia, 184.

[49] See Judgment of 4 May 2023, *UI vs Österreichische Post AG*, C-300/21, EU:C:2023:370 <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62021CJ0300>.

intended to ensure the lawfulness of joint data processing activities and, therefore, to perform an ex ante protection function, whereas liability under Article 82 GDPR only comes into play once damage has occurred.

However, providing evidence of the existence of joint control in a concrete case can be arduous and generate uncertainty. In this respect, the EDPB Guidelines on the concepts of controller and processor in the GDPR are emblematic when they state that "The fact that several actors are involved in the same processing does not mean that they are necessarily acting as joint controllers of such processing. Not all kind of partnerships, cooperation or collaboration imply qualification of joint controllers as such qualification requires a case-by-case analysis of each processing at stake and the precise role of each entity with respect to each processing".[50] The decisive factor is the existence of purposes and means of processing determined jointly by the controllers. In this respect, it is added that "the exchange of the same data or set of data between two entities without jointly determined purposes or jointly determined means of processing should be considered as a transmission of data between separate controllers".[51] Being well aware of these challenges, the French CNIL felt the need to provide guidance that specifically addresses where joint controllers can be involved in the use of personal data for the development and training of AI applications.[52]

On the contrary, good practices/standards on data governance, once turned into contract terms, become binding on all parties to a data sharing contract, regardless of how these parties qualify under the data protection legal framework. Furthermore, they can be enforced through the contractual remedies available under the applicable contract law regime, such as contract termination and/penalty clauses.

Contract law remedies stand alongside the forms of public and private enforcement envisaged by the GDPR by contributing to promoting the accountability of all those who share data for the training and development of an AI application, even in the context of complex value chains.

4. The AI Act: Data Governance and AI Value Chains.

The AI Act aims to establish a legal framework that is mainly addressed to providers of high-risk AI systems (which may not coincide with data controllers) and deals with all the stages (input data collection, design and development of models etc.) leading to the deployment of AI systems. Inter alia, it mandates providers of high-risk systems to adopt adequate data governance practices and to ensure the quality of training data (Article 10 AI Act). It also sets out transparency and documentation duties for providers of systems of this kind

[50] EDPB, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (07 July 2021) point 69 <www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf>.

[51] Ibidem, point 70.

[52] See CNIL, 'Déterminer la qualification juridique des acteurs' (8 April 2024) <www.cnil.fr/fr/determiner-la-qualification-juridique-des-fournisseurs-de-systemes-dia>: "Plusieurs acteurs peuvent intervenir dans le développement d'un système d'IA, avec divers degrés d'implication sur les traitements de données personnelles".

with reference, as well, to data governance and data quality (see Articles 11 and 13 (3) (vi) AI Act). These requirements, however, only apply to high-risk AI systems.

Moreover, the AI Act Proposal did not take into account the fact that the provider of an AI system rarely coincides with its developer and almost never carries out in-house all the steps leading up to the AI system being placed on the market or put into service. As a result, it was left to AI providers to promote the accountability of the other participants in the value chain, also by adopting contract terms under which the latter are required to guarantee compliance with the AI provisions on data quality, documentation etc. This policy option relied on the assumption that the AI provider is the economic operator in a dominant position vis-à-vis these participants. This assumption, however, was criticized for being too simplistic and failing to take into account that possible imbalances of economic power between the parties do not always see AI providers assuming the role of 'strong' parties in the relationship with participants in the AI value chain.

In the light of such criticism the approved text of the AI Act acknowledges the complexity of AI value chains, which may include multiple third parties involved in the development and in the supply of components. Hence, it prescribes that these third parties must cooperate, as appropriate, with providers of AI systems to enable them to monitor compliance with the requirements set out by the AI Act. To this end, third parties are required to disclose in writing to AI providers all information necessary for this purpose (Article 25 (4) AI Act).[53]

This obligation to cooperate sets an incentive for AI providers and value chain participants to 'contractualize' and document how they share responsibility for complying with requirements on high-risk AI systems, including data governance. This brings a number of benefits but also possible risks.

AI providers and value chain participants can theoretically agree on a fair distribution of the responsibilities between them. On the other hand, risks arise from possible imbalances of bargaining power among the contracting parties, for instance, where AI providers are in a position of economic dominance vis-à-vis the other participants in the value chain, such that the former can impose contractual terms under which the costs of compliance with the requirements of the IA Act or the fines provided for therein are passed on to the latter.

In order to address possible inequalities in bargaining power within AI value chains, the AI Act Proposal of June 2023 explicitly qualified contract terms unilaterally imposed by AI providers on a SME or start-up aimed at excluding or limiting the liability of the party imposing the term for intentional act and gross negligence (or excluding or limiting access to remedies available to the other party) as unfair and non-binding.[54] In addition, the AI Act Proposal of June 2023

[53] Article 25 (4) AI Act: "The provider of a high-risk AI system and the third party that supplies an AI system, tools, services, components, or processes that are used or integrated in a high-risk AI system shall, by written agreement, specify the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art, in order to enable the provider of the high-risk AI system to fully comply with the obligations set out in this Regulation".

[54] See Article 28a AI Act Proposal of June 2023. See, as well, Recital 62 AI Act Proposal of June 2023: "In order to ensure a high level of trustworthiness of high-risk AI systems, those systems should be subject to a

stated that "*A contractual term is also unfair if it has the effect of shifting penalties referred to in Article 71 or associated litigation costs across parties to the contract, as referred to in Article 71(8)*" (Article 28a).

These provisions have not been included in the final text of the IA Act. Instead Article 28 (4) AI Act empowers the AI Office to develop and recommend voluntary model terms for contracts between providers of high-risk AI systems and those involved in the value chain. The fact that such model terms can be adopted on a voluntary basis is further evidence that the governance of AI value chains is left to national or EU regulations on unfair terms in business contracts. Likewise, the validity of clauses on penalties or claims arising from non-compliance with the IA Act included in contracts between suppliers and participants in IA value chains must be assessed under national contract law.[55]

5. Conclusions.

The paper addressed data sharing contracts for AI development and training, entered into by parties participating in AI value chains, in order to assess the incentives for responsible data sharing under European data law.

The normative instruments recently enacted by the EU, such as the DGA and the Data Act, are concerned with establishing a 'data economy' and fall short to promote the accountability of the parties to a data sharing contract. As a consequence, the governance of AI training data is mainly entrusted to party autonomy and to the principles of the GDPR, where the latter is applicable.

As demonstrated, the terms included in data sharing contracts tend to be exclusively shaped by the private interests of the parties. These terms do not reflect the legal status of data which differs from tradable commodities, nor do they take into account the peculiarities of the data used in the context of AI development/training. The data used for this purpose is not a static artefact; on the contrary, it is the result of choices and practices to be implemented during the phases of data collection and generation and model development, in order to tackle possible sources of harm to fundamental rights.

The analysis showed that leaving the governance of AI training data to party autonomy entails several shortcomings. The parties are incentivized to comply with mandatory regulations, such as those which protect personal data and the right to privacy, only if the public law and tort law regimes at play show an adequate level of effectiveness. Moreover, liability under contract law does not extend beyond the parties to the contract and, therefore, it fails to promote the accountability of all those who share data for AI development.

---

conformity assessment prior to their placing on the market or putting into service. *To increase the trust in the value chain and to give certainty to businesses about the performance of their systems, third-parties that supply AI components may voluntarily apply for a third-party conformity assessment.*"

[55] In reality, the AI Act Proposal of June 2023 contained a provision (Article 71 (8a)) under which: "*The penalties referred to in this article as well as the associated litigation costs and indemnification claims may not be the subject of contractual clauses or other form of burden-sharing agreements between providers and distributors, importers, deployers, or any other third parties*". Although clarifying, this provision merely reasserted a principle common to many legal regimes, i.e. that private autonomy is not allowed to alter the allocation of liability between the parties, which is established by public law remedies.

However, it was demonstrated that the interaction of the data protection framework with contract law challenges the corollaries of traditional contract theory. The public law regime set out by the GDPR entails constraints on party autonomy, since data can only be processed in conformity with the principles of lawfulness and fairness enshrined in article 5 GDPR. Moreover, the data protection framework also covers automated decision-making that often involves the deployment of AI systems which may have significant adverse impacts on individuals. In these cases, transparency requirements are set out and the adoption of adequate measures is mandated according to the principles of accountability and privacy by design (see Articles 5, 22, 24 and 25; Recital 71 GDPR), in order to prevent such impacts. These principles interact with party autonomy by establishing duties of care on the parties that share and manage data for the purpose of training/developing AI applications.

As highlighted in the paper, the principle of accountability has an organizational dimension and places on controllers the duty to take the 'legal' measures that enable them to comply with the GDPR. Therefore, the parties to these contracts are required to arrange adequate data sharing architectures, starting with the choice of the contract type and contract terms.

This means that the duties of care arising from the data protection framework can be 'contractualized' and turned into due diligence contract terms included in the data sharing contracts. Contract terms of this sort may compel the parties to such contracts to adopt: *i)* technical and procedural standards and practices *ii)* mechanisms to oversee compliance with these standards/practices by all the parties (for instance, mandating to carry out internal audits or reporting) and *iii)* enforcement mechanisms (for instance, penalty clauses, contract termination clauses, etc.) in the event of non fulfilment of these duties. Along the same lines are contract terms requiring the contracting parties to monitor whether sub-suppliers comply with data protection requirements.

As a consequence, the adoption of good practices and standards is not left to market drivers. On the contrary, it is triggered by the public law provisions at play and notably by the principle of accountability which is a regulatory model for the protection of personal data based on a hybrid form of enforceable self-regulation. Contract law remedies stand alongside the forms of public and private enforcement envisaged by the GDPR and contribute to promoting the accountability of all those who share data for the training and development of an AI application, even in the context of complex value chains.

Lastly, the analysis comprised a brief overview of the relevant provisions of the AI Act that deal with data governance and AI value chains. This new body of legislation acknowledges the complexity of AI value chains, which may comprise multiple entities, such as parties involved in the supply of data. It is therein prescribed that these third parties must cooperate, as appropriate, with providers of AI systems to enable them to monitor compliance with the requirements set out by the AI Act. However, the AI Act does not address inequalities of bargaining power between the various economic actors involved. This gap risks undermining the policy objective of making all those participating in value chains for high-risk AI systems accountable.

Irti C, 'Riflessioni sull'impatto delle applicazioni tecnologie nell'ambito sanitario, tra regole etiche e regole giuridiche' (2024) 1 EJPLT, 34-41.
DOI: https://doi.org/10.57230/EJPLT241CI

EJPLT
ISSN 2704-8012



Riflessioni sull'impatto delle applicazioni tecnologie nell'ambito sanitario, tra regole etiche e regole giuridiche

Reflections on the impact of technology applications in healthcare, between ethical rules and legal rules

CLAUDIA IRTI
Professore ordinario di Diritto Privato
Università Ca' Foscari di Venezia

Abstract

Le recenti politiche europee sulla salute incentivano lo sviluppo della e-Health e la sempre maggiore diffusione delle applicazioni della IA nell'ambito sanitario. Si tratta di un percorso obbligato che, certamente, rappresenta una enorme risorsa per il sistema sanitario pubblico, per gli operatori del settore e, non da ultimo, per la salute dei pazienti, ma che, altresì, pone alcuni interrogativi dal punto di vista etico-giuridico sui quali questo lavoro intende (seppur brevemente) far riflettere.

Recent European health policies encourage the development of e-Health and the increasing spread of AI applications in healthcare. This is an obligatory course of action that certainly represents an enormous resource for the public health system, for those working in the sector and, not least, for the health of patients, but which also raises a number of questions from an ethical-legal point of view on which this paper intends (albeit briefly) to reflect.

*Questo articolo è stato presentato alla conferenza internazionale "Il diritto dell'innovazione tecnologica. Jam Session internazionale tra giuristi", 8-9 marzo 2023, Fondazione Einaudi, Roma.
Comitato scientifico: Vincenzo Ricciuto (Univ. Tor Vergata di Roma), Lucilla Gatt (Univ. Suor Orsola Benincasa di Napoli), Carla Solinas (Univ. Tor Vergata di Roma), Mariló Gramunt Fombuena (Universitat de Barcelona).
Inoltre, il contributo è destinato allo special issue in memoria del Prof. Cesare Massimo Bianca e del Commentario al D. Lgs. 30 giugno 2003, n. 196 «Codice della privacy» da lui curato con il Prof. Francesco Donato Busnelli nel 2007 (Cedam).

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: sanità digitale; intelligenza artificiale; e-health.

Summary: 1. Le più recenti politiche europee sulla salute e la "sanità digitale". – 2. Le implicazioni dell'uso dell'intelligenza artificiale nell'ambito medico per l'utente/paziente. – 3. Quali regole per le applicazioni della intelligenza artificiale in ambito sanitario?

1. Le più recenti politiche europee sulla salute e la "sanità digitale".

La situazione emergenziale dovuta ai recenti eventi pandemici ha posto all'attenzione dell'Unione Europea e dei singoli Stati membri il problema immediato di sostenere ed efficientare un sistema che nel corso degli anni è stato gravemente "depotenziato" (per le note esigenze di sostenibilità del quadro macroeconomico), finendo così con il riportare la sanità, dopo molte decadi, al centro dell'agenda politica[1]. Molti dei problemi presenti e futuri di questo complesso settore si ritiene possano e debbano essere risolti attraverso l'implementazione dell'uso delle nuove tecnologie e, più in particolare, dell'intelligenza artificiale a servizio della salute[2], accelerando quel processo già in atto da alcune decadi che va sotto il nome di e-Health[3].

La direzione (senza ritorno) assunta dalle più recenti politiche europee sulla salute[4], sostenuta dalla consapevolezza – comune e condivisa – che l'uso della

[1] Non sorprende, dunque, come una delle missioni del Piano Nazionale di Ripresa e Resilienza (la sesta) sia interamente dedicata alla "Salute", con uno stanziamento di 18,5 miliardi per finanziamenti destinati in larga parte a modernizzare e digitalizzare il sistema sanitario. Tra gli obiettivi del PNRR si segnala quello di «potenziare e innovare la struttura tecnologica e digitale del servizio sanitario nazionale a livello centrale e regionale al fine di garantire un'evoluzione significativa delle modalità di assistenza sanitaria, migliorando la qualità e la tempestività delle cure; valorizzando il ruolo del paziente come parte attiva del processo clinico assistenziale; e garantendo una maggiore capacità di governance e programmazione sanitaria guidata dalla analisi dei dati, nel pieno rispetto della sicurezza e della tutela dei dati e delle informazioni».

[2] Secondo lo studio «Artificial Intelligence and life in 2030 – One Hundred Year Study on Artificial Intelligence», pubblicato dall'Università di Stanford nel 2016, il settore sanitario è uno degli otto settori in cui l'impatto dell'intelligenza artificiale sarà maggiormente rilevante. Il mercato dell'intelligenza artificiale è inoltre uno dei più fiorenti; secondo un report della Coherent Market Insights il mercato dell'AI, dal valore attuale di 3285 milioni di dollari, crescerà di oltre ventidue volte nei prossimi sei anni, arrivando al valore complessivo di 74650 milioni di dollari nel 2027 (https://www.coherentmarketinsights.com/market-insight/artificial-intelligence-in-healthcare-market-436)

[3] Con il termine e-Health si è soliti far riferimento a quell'ambito sanitario che emerge nell'intersezione tra informatica medica, sanità pubblica e attività economica, ricomprendente tutti quei servizi e quelle informazioni sanitarie forniti o condivisi attraverso l'uso di tecnologie informatiche e di telecomunicazione, così G. EYSENBACH, What is e-health?, in Journal of Medical Internet Research, 2021, Vol. 3, 2, 20 (traduzione della scrivente).

[4] Nel 2004 è stato pubblicato il primo piano d'azione per implementare la cosiddetta "sanità digitale" - l'e-Health Action Plan - poi rinnovato per mezzo della Comunicazione 2012/736. Successivamente con la Comunicazione 2018/233, «relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana», la Commissione è tornata ad enfatizzare i benefici ottenibili grazie alla digitalizzazione dei sistemi sanitari, fra cui la possibilità di «accrescere il benessere di milioni di cittadini e cambiare radicalmente il modo in cui i servizi sanitari e assistenziali vengono forniti ai pazienti», sottolineando come lo sviluppo dei servizi sanitari digitali consentirebbe di «sostenere la riforma dei sistemi sanitari e la loro transizione verso nuovi modelli di assistenza, basati sui bisogni delle persone, e (di) consentire un passaggio da sistemi incentrati sugli ospedali a strutture assistenziali integrate e maggiormente basate sulle comunità». La Commissione europea ha altresì chiarito come il raggiungimento di tali obiettivi sia stato sinora frenato dall'assenza di un'effettiva interoperabilità dei dati sanitari e dalla frammentazione del mercato, fattori che «rappresentano un

Intelligenza artificiale possa rappresentare una enorme risorsa per il sistema sanitario pubblico, per gli operatori ma, anche e soprattutto, per la salute dei pazienti, rende vieppiù necessario guardare alle interrelazioni tra le applicazioni della IA[5] e l'ambito sanitario rivolgendo attenzione anche a quelli che sono i rischi che l'uso di queste tecnologie è destinata a portare con sé, in primo luogo quelli di natura etica[6], specie in un settore, come quello medico, dove i principi bioetici per la ricerca clinica e l'assistenza sanitaria sono da tempo ben consolidati.

2. Le implicazioni dell'uso dell'intelligenza artificiale nell'ambito medico per l'utente/paziente.

Negli Stati Uniti la Food and Drug Administration ha sino ad oggi approvato l'uso di almeno 64 dispositivi medici che utilizzano algoritmi di intelligenza artificiale e apprendimento automatico nell'ambito medico e della assistenza sanitaria (soprattutto in ambiti radiologici, cardiologici ed endocrinologici) e nel 2018 ha approvato la prima diagnosi totalmente basata sull'uso della IA[7]: una avanzata dal ritmo incalzante – almeno oltre oceano – che pone plurime questioni al centro dell'attenzione della politica e dei regolatori.

L'aumento di interventi diagnostici e terapeutici che si basano su soluzioni di AI-Health porta - in primo luogo - i pazienti a condividere sempre più dati personali[8], nella specie quelli sanitari che esternano gli aspetti più vulnerabili

ostacolo ad un approccio integrato alla prevenzione delle malattie e ad una cura e assistenza meglio adattate alle esigenze dei cittadini». Nel contesto attuale, infatti, le attività di condivisione e scambio dei dati sanitari a livello europeo sono limitate alla cooperazione volontaria fra paesi membri, i quali si avvalgono a tal fine di una eHealth Digital Service Infrastructure: la cooperazione è tuttavia rimasta circoscritta allo scambio dei fascicoli sanitari dei pazienti e delle prescrizioni in formato telematico. È per questo motivo che la Commissione europea ha assunto un impegno concreto volto all'adozione di standard europei per la qualità, affidabilità e sicurezza dei dati sanitari e per l'adozione di un formato europeo che renda possibile la standardizzazione delle cartelle cliniche elettroniche e quindi lo scambio (Raccomandazione (UE) 2019/243 della Commissione, del 6 febbraio 2019, relativa a un formato europeo di scambio delle cartelle cliniche elettroniche). Più di recente – con la Comunicazione A European Health Data Space: harnessing the power of health data for people, patients and innovation[4], che accompagna la Proposta di Regolamento sullo spazio europeo dei dati sanitari [4] per la costituzione di uno European Health Data Space – la Commissione è tornata a ribadire come la digitalizzazione sia assolutamente essenziale per il futuro dell'assistenza sanitaria e la trasformazione digitale sia fondamentale per fornire un'assistenza sanitaria migliore ai cittadini, per costruire sistemi sanitari economicamente e qualitativamente stabili e affidabili, per sostenere la competitività e l'innovazione a lungo termine nel settore medico dell'UE. In tale documento la Commissione ha altresì riaffermato come i dati siano una risorsa indispensabile che, se utilizzata in modo responsabile e nel pieno rispetto dei diritti fondamentali, possa apportare immensi benefici a ogni aspetto della nostra vita quotidiana, compresa la salute.

[5] L'uso stesso del termine IA richiede ulteriori chiarimenti, poiché sono stati proposti diversi sottotipi e il suo significato può essere vago: con il termine intendiamo qui ricomprendere tutte quelle tecnologie informatiche denominate anche deep learning, machine learning, deep neural networks, artificial intelligence e/o AI.

[6] Per uno stimolante approccio critico al problema M. GRONDONA, L'intelligenza artificiale di fronte alla dimensione della responsabilità. Una prospettiva ideologica orientata e un inventario di problemi, in Le corti fiorentine, 2021, 3, 3 e ss.

[7] B. STAN, D. PRANAVSINGH e M. BERTALAN, The state of artificial intelligence-based FDA-approved medical devices and algorithms: an online database, in Digital Medicine, 2020, 3.

[8] Sul tema della protezione dei dati personali, prima delle intervenute più recenti modifiche, si rinvia per tutti al volume di C.M. BIANCA, F.D. BUSNELLI (a cura di), La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196 («Codice della privacy»), I e II, Padova, 2007.

della persona[9], non sempre nella piena consapevolezza che ciò stia avvenendo e a quali fini ciò stia avvenendo, lasciando ampi margini di incertezza sulla capacità degli individui di essere coinvolti in modo significativo nel processo decisionale che porta a questa condivisione[10].

A ciò si aggiunge il problema di come gestire il flusso di tali dati tra sistemi pubblici e sistemi privati, dal momento che strumenti di AI-Health di proprietà privata saranno addestrati su dati generati nel sistema pubblico, per essere poi condivisi (legalmente) con aziende private. Un tema da attenzionare, soprattutto quando le società private coinvolte hanno interessi economici anche nell'ambito assicurativo, con un impatto meno significativo in Europa grazie alla presenza di sistemi di assistenza sanitaria pubblica, ma molto significativo in Paesi come gli Stati Uniti, dove nonostante si sia dato vita ad un nuovo sistema di regolamentazione dei dispositivi medici che fanno uso di software di intelligenza artificiale (si veda dopo), sembra essere ancora prestata poca considerazione alla sorveglianza degli strumenti di IA utilizzati dai grandi assicuratori, che non a caso sono stati resi oggetto di attenzione da recenti studi che ne propongono la riconduzione nella definizione di dispositivi medici al fine di sottoporli alla relativa regolamentazione[11].

L'uso crescente di processi decisionali algoritmici in ambito clinico presenta, tuttavia, altre implicazioni negative per l'autonomia individuale: ci riferiamo in particolare alla decisione clinica derivata dall'AI-Health che, nel rispetto del principio della partecipazione del paziente alla relazione di cura, dovrebbe poter essere resa a lui «comprensibile», nel senso che gli debbano essere resi il più possibile espliciti i processi che l'hanno determinata. Sennonché, è di tutta evidenza come la stragrande maggioranza della popolazione non abbia il livello di conoscenze tecniche e scientifiche necessario per comprendere i processi che conducono alla singola decisione clinica automatizzata, e quelli che possono averla - compresi gli operatori sanitari - si trovano comunque ad interfacciarsi con algoritmi dalla natura di black-box.

È questo uno degli aspetti più delicati dei processi condotti dai sistemi di intelligenza artificiale che, mancando di intrinseca «trasparenza», rendono problematica la supervisione umana, richiesta anche al fine di evitare che i risultati ottenuti (i c.d. output) si palesino parziali, discriminatori, finanche errati. Nell'ambito sanitario tale caratteristica incide altresì sulla capacità dell'individuo di comprendere i processi di cura cui egli viene sottoposto,

---

[9] G. VITERBO, Governance and processing of personal data in the Italian healthcare system in the light of UE principles, in Actualidad Jurídica Iberoamericana, 2024, 20, 1052 e ss.;

[10] C. IRTI, L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità delle persone anziane, in Mercato e persona, 2023, 32 e ss.; M. CIANCIMINO, Protezione e controllo dei dati in ambito sanitario e intelligenza artificiale, 2021, Napoli, passim.

[11] R. SIRBU, J. MORLEY e L. FLORIDI, Artificial intelligence for health insurance: A proposed framework for FDA oversight, 2024. Consultabile online: https://ssrn.com/abstract=4702853: il Centers for Medicare & Medicaid Services (CMS) americano ha rilasciato una dichiarazione in tema di uso di algoritmi nel campo dell'assicurazione sanitaria e ha messo in guardia contro i possibili rischi di discriminazioni che possono essere determinate dall'AI. Ha specificato che «le compagnie di assicurazione sanitaria non possono utilizzare l'intelligenza artificiale o gli algoritmi per determinare la copertura o negare l'assistenza agli iscritti ai piani MA (...) Gli assicuratori devono basare le decisioni di copertura sulle circostanze del singolo paziente, per cui un algoritmo che determina la copertura sulla base di un insieme di dati più ampio al posto dell'anamnesi del singolo paziente, delle raccomandazioni del medico o delle note cliniche non può considerarsi sarebbe conforme». La presenza di una revisione umana significativa non è "specificata": cosa si intende per revisione umana significativa?

interferendo sull'autonomia dell'individuo e il suo diritto di essere parte della "relazione di cura", anche al fine di decidere o meno se rifiutare alcuni trattamenti. Non bisogna dimenticare come dal punto di vista etico uno dei risultati più importanti raggiunti nell'ambito medico è stato proprio quello di riconoscere al paziente il diritto di essere coinvolto nella relazione di cura: non più oggetto, ma soggetto coinvolto nel trattamento di cura. L'applicazione della intelligenza artificiale nell'ambito medico può comportare il rischio di un'inversione di marcia.

Altra preoccupazione diffusa che riguarda l'applicazione dei sistemi di AI-Health riposa nel fatto che i dati presenti per l'addestramento algoritmico sono in larga parte provenienti da alcuni gruppi di individui, perlopiù uomini bianchi di età adulta: gli algoritmi addestrati su tali insiemi di dati parziali potrebbero fare previsioni errate per le "minoranze" non presenti[12]. Se gli operatori sanitari vengono lasciati completamente fuori dal giro e i sistemi di apprendimento sanitario si affidano principalmente a decisioni automatizzate, esiste un notevole rischio di esacerbazione delle disuguaglianze esistenti nell'ecosistema della sanità digitale tra coloro che generano abbastanza dati per garantire algoritmi accuratamente addestrati e coloro che non lo fanno.

3. Quali regole per le applicazioni della intelligenza artificiale in ambito sanitario?

Il 2024 è indicato da molti come l'anno cruciale nella regolamentazione dell'IA, con particolare attenzione proprio al settore sanitario: ne è prova l'adozione dell'AI Act in Europa e la regolamentazione federale in atto negli Stati Uniti. La sfida è arrivare ad armonizzare i quadri regolatori per garantire sicurezza e innovazione, riconoscendo le specificità dell'applicazione dell'IA in ambito sanitario.

Negli USA a fine ottobre 2023, il Presidente Biden, con proprio ordine esecutivo, ha chiesto alle agenzie federali di intensificare la loro supervisione riguardo agli strumenti di intelligenza artificiale di loro competenza. Pur non modificando immediatamente il regime normativo, il Presidente Biden ha predisposto una specifica *timeline* per l'adozione di oltre misure volte all'utilizzo responsabile dell'IA, che più di 50 agenzie dovranno seguire, fra cui il Dipartimento della salute e dei servizi umani del Governo e l'Ufficio brevetti e marchi degli Stati Uniti. Già nell'ottobre 2022, la Casa Bianca aveva presentato un "Blueprint for an AI Bill of Rights", ossia un insieme di principi e pratiche finalizzate a guidare la progettazione, l'uso e l'implementazione di sistemi automatizzati garantendo la protezione dei diritti dei cittadini americani. Nel luglio 2023, inoltre, l'amministrazione Biden aveva ottenuto l'impegno da parte di sette grandi aziende di Intelligenza Artificiale (IA) – Amazon, Anthropic, Google, Inflection, Meta, Microsoft e OpenAI – a promuovere uno sviluppo

[12] S. Garattini, Brevettare la salute, Bologna, 2020; F. Rotolo, Le discriminazioni indirette nella ricerca scientifico-farmacologica e il difficile esercizio del diritto di accesso alle cure: quale ruolo per la proprietà intellettuale?, in Familia, 2023; Id., Il diritto alla cura degli anziani tra vulnerabilità, logiche di mercato e brevettabilità della salute: la necessità di un ripensamento della proprietà intellettuale in chiave sostenibile, in Jus Civile, 2023, 4.

responsabile e sicuro dell'IA. La FDA ha altresì pubblicato una serie di linee guida a supporto degli sviluppatori dei dispositivi medici basati sull'IA. L'agenzia richiede che vi sia un attento monitoraggio di questi ultimi anche attraverso meccanismi di valutazione *ex post* la loro distribuzione. Queste iniziative vanno di pari passo con l'attività di aggiornamento del quadro regolatorio dell'agenzia: un sforzo che ha preso avvio nel 2021 con l'Artificial Intelligence/Machine Learning Based Software as a Medical Device Action Plan, e che è proseguito nel 2023 con l'annuncio dell'istituzione di un comitato consultivo per la salute digitale atto a fornirle consulenza sulle tecnologie sanitarie digitali, compresa l'intelligenza artificiale[13].

In Europa è stato approvato l'AI Act, regolamento che dedica specifica attenzione a taluni usi critici della Intelligenza artificiale (come il riconoscimento facciale per scopi di pubblica sicurezza) ma scarsa attenzione è prestata al settore sanitario, dal momento che l'uso della intelligenza artificiale in tale ambito non viene segnalato tra quelli ad alto rischio[14], fatta eccezione per quanto specificato nell'Allegato III del Regolamento, ove si chiarisce che sono considerati sistemi ad alto rischio: «Sistemi di intelligenza artificiale destinati a essere utilizzati da o per conto delle autorità pubbliche per valutare l'idoneità delle persone fisiche a beneficiare di prestazioni e servizi di assistenza pubblica, compresi i servizi sanitari e i servizi essenziali, tra cui, a titolo esemplificativo e non esaustivo, l'alloggio, l'elettricità, il riscaldamento/raffreddamento e internet, nonché per concedere, ridurre, revocare, aumentare o reclamare tali prestazioni e servizi; sistemi di intelligenza artificiale destinati a valutare e classificare le chiamate di emergenza da parte di persone fisiche o a essere utilizzati per l'invio o per stabilire la priorità nell'invio di servizi di primo intervento di emergenza, compresi quelli della polizia e delle forze dell'ordine, dei vigili del fuoco e dei soccorsi medici, nonché dei sistemi di triage dei pazienti di emergenza sanitaria».

Nel corpo del Regolamento il settore è altresì menzionato al considerando 58: «Un altro settore in cui l'utilizzo dei sistemi di IA merita particolare attenzione è l'accesso ad alcuni servizi e prestazioni essenziali, pubblici e privati, necessari affinché le persone possano partecipare pienamente alla vita sociale o migliorare il proprio tenore di vita, e la fruizione di tali servizi. In particolare, le persone fisiche che chiedono o ricevono prestazioni e servizi essenziali di assistenza pubblica dalle autorità pubbliche, vale a dire servizi sanitari, prestazioni di sicurezza sociale, servizi sociali che forniscono protezione in casi quali la maternità, la malattia, gli infortuni sul lavoro, la dipendenza o la vecchiaia e la perdita di occupazione e l'assistenza sociale e abitativa, sono di norma dipendenti da tali prestazioni e servizi e si trovano generalmente in una posizione vulnerabile rispetto alle autorità responsabili. I sistemi di IA, se utilizzati per determinare se tali prestazioni e servizi dovrebbero essere concessi, negati, ridotti, revocati o recuperati dalle autorità,

[13] F. PAOLUCI, O. POLLICINO, F. SACCHI, Regole globali per l'IA in sanità: quali punti di incontro tra norme UE e Usa, 2024. Consultabile online: https://www.agendadigitale.eu/sanita/regole-globali-per-lia-in-sanita-quali-punti-dincontro-tra-norme-ue-e-usa/.

[14] G. COMANDÈ, Tecnologie e metamorfosi del danno e della responsabilità sanitaria, in Danno e responsabilità, 2024, 2, 153 e ss.

compreso se i beneficiari hanno legittimamente diritto a tali prestazioni o servizi, possono avere un impatto significativo sul sostentamento delle persone e violare i loro diritti fondamentali, quali il diritto alla protezione sociale, alla non discriminazione, alla dignità umana o a un ricorso effettivo e dovrebbero pertanto essere classificati come sistemi ad alto rischio. Cionondimeno, il presente regolamento non dovrebbe ostacolare lo sviluppo e l'utilizzo di approcci innovativi nella pubblica amministrazione, che trarrebbero beneficio da un uso più ampio di sistemi di IA conformi e sicuri, a condizione che tali sistemi non comportino un rischio alto per le persone fisiche e giuridiche».

Per il resto il principale riferimento normativo è il Regolamento 2017/745/UE sui dispositivi medici (Medical Device Regulation)[15], che a partire dal 26 maggio 2021 ha sostituito il previgente regime (in particolare, la Direttiva 93/42/CEE) [16] . Detta normativa prevede controlli di conformità preventivi, nonché doveri di sorveglianza post-commercializzazione, simili a quanto accade nel sistema americano.

Nel contesto di questo breve riepilogo del quadro regolativo, non si può, da ultimo, non citare lo «Schema di disegno di legge recante disposizioni e delega al governo in materia di intelligenza artificiale», recentemente approvato dal Consiglio dei ministri del nostro Governo ed ora al vaglio parlamentare, che «reca principi in materia di ricerca, sperimentazione, sviluppo, adozione e applicazione di sistemi e modelli di intelligenza artificiale» e «promuove un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica dell'intelligenza artificiale volto a coglierne le opportunità. Garantisce la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'intelligenza artificiale», ove si rinvengono, in particolare, tre articoli dedicati alle applicazioni della intelligenza artificiale in ambito sanitario: l'art. 7 rubricato «Uso dell'intelligenza artificiale in ambito sanitario e di disabilità», l'art. 8 rubricato «Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario» e l'art. 9 rubricato «Disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale».

Da un punto di vista "politico", quello proposto dal Governo è un primo tentativo di fornire un quadro normativo nazionale di riferimento per l'impiego delle AI nel settore sanitario, mosso dalla volontà di evitare che l'assenza di specifiche previsioni rinvenibili a livello europeo finisca con il rallentare – se non

[15] A norma dell'art. 2 Regolamento 2017/745/UE è considerato dispositivo medico «qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche: - diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie, - diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità, - studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico, - fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere qua giovata da tali mezzi».

[16] I Regolamenti 2017/745/UE e 2017/746/UE (succeduti alle Direttive comunitarie 93/42/CEE sui dispositivi medici, 98/79/CE sui dispositivi medici diagnostici in vitro e 90/385/CEE sui dispositivi medici impiantabili attivi) che regolamentano in modo uniforme in tutti i Paesi della Unione Europea il settore dei dispositivi medici, demandano all'Autorità Competente di ciascun Stato membro la designazione degli Organismi Notificati, che valutano, controllano e verificano i dispositivi medici. Per maggiori approfondimenti sulla disciplina si veda G. Capilli, Diritto Privato sanitario, Pisa, 2022, p. 54 e ss.

compromettere – gli ingenti investimenti dedicati all'impiego di tali tecnologie da parte del PNRR. Da un punto di vista giuridico si rende necessario svolgere nei prossimi mesi un approfondimento circa la portata e la legittimità dei singoli principi in esso enucleati, tenuto conto che lo stesso è destinato a subire emendamenti e modifiche in sede di revisione parlamentare, contesti nei quali sarà opportuno vagliarne la conformità a principi etici e giuridici già consolidati.

Perilla Granados JSA, 'Lineamientos para implementar la inteligencia artificial en el derecho privado' (2024) 1 EJPLT, 42-58.
DOI: https://doi.org/10.57230/EJPLT241JSAPG

EJPLT
ISSN 2704-8012



Lineamientos para implementar la inteligencia artificial en el derecho privado

Guidelines for implementing artificial intelligence in private law

JUAN SEBASTIÁN ALEJANDRO PERILLA GRANADOS
Associate Professor
Universidad Tecnológica de Bolívar

Abstract

El derecho privado encuentra su fundamento en los derechos reales, los cuales están sujetos a procesos que se pueden sistematizar para ser gestionados a través de la inteligencia artificial. Para estos efectos se propone una estructura de cuatro pasos que vincule de manera dinámica las fuentes, los títulos, los modos y los derechos reales. Estos pasos pueden ser estructurados desde una programación tecnológica de flujo, condicional y, generalmente, silogística. Así, en este artículo se presenta una propuesta basada en el enfoque de estructuras de las disciplinas y que permite generar derivaciones tecnológicas en contextos específicos.

Private law finds its foundation in real rights, which are subject to processes that can be systematized to be managed through artificial intelligence. For these purposes, a four-step structure is proposed that dynamically links sources, titles, modes and real rights. These steps can be structured from a technological flow, conditional and, generally, syllogistic programming. Thus, this article presents a proposal based on the approach of discipline structures and that allows generating technological derivations in specific contexts.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: artificial intelligence; real rights; legal systematization; flowcharts; digital right.

Summary: 1. Introducción. – 2. Relación uniforme de las etapas del derecho privado para configurar derechos reales. – 3. Lineamientos de programación para un Desarrollo tecnológico applicable al derecho privado. – 4. Conclusiones.

Introducción.

El uso de la inteligencia artificial se ha implementado en diferentes áreas profesionales. Sin embargo, en el caso del derecho, la implementación aún es limitada y, en consecuencia, la labor humana es la regla general en el ejercicio jurídico. Pese a esta realidad, no es descartable que la inteligencia artificial sea una herramienta aplicable al derecho, programada por la actividad humana, para asumir tareas concretas que optimicen labores tradicionalmente asumidas por el ser humano. Por lo tanto, con la inteligencia artificial aplicada al derecho no se busca reemplazar necesariamente a los operadores jurídicos humanos, pues dependerá en gran medida de la programación que se realice desde las tareas que no requieren la presencia indispensable de una persona humana para su desarrollo; se requiere, entonces, un acuerdo sobre cuáles son aquellas tareas que puede asumir la inteligencia artificial y cuáles debe continuar desarrollando el ser humano.

Sin embargo, el derecho es un campo del conocimiento tan amplio, que difícilmente se podrán establecer postulados generales sobre qué tareas podría asumir la inteligencia artificial en todos los casos. Por lo tanto, se sugiere la necesidad de analizar estas posibilidades por áreas jurídicas y, más específicamente, por regímenes jurídicos propios de cada una de esas áreas[1]. Es en este punto en el cual se puede analizar el área del derecho privado, la cual pretende, de manera específica, regular las relaciones entre particulares. Algunas de estas relaciones particulares tienen incidencia directa en los derechos reales, los cuales pueden ser entendidos, de manera introductoria, como aquellos que ostentan las personas sobre sus bienes. Sobre el particular existe una múltiple cantidad de posibilidades para lograr ostentar derechos reales sobre bienes por parte de las personas. Así, en caso de encontrarse una metodología de análisis que sistematice en categorías generales las etapas de estas posibilidades, podría proponerse como fundamento de la programación tecnológica para que la inteligencia artificial pueda gestionar esta área del derecho.

En consecuencia, este artículo de investigación busca responder la siguiente pregunta: ¿cómo se pueden sistematizar de manera uniforme las etapas para poder ser titular de derechos reales desde una eventual programación

[1] El estudio del derecho como campo del conocimiento se realiza en el marco de las ciencias sociales. En este sentido, se acoge un enfoque iusteórico antiformalista que considera que el derecho tiene una naturaleza abierta y que puede ser complementado por múltiples fuentes desde ejercicios hermenéuticos. Para profundizar en el tema se sugiere leer: JSA Perilla-Granados, 'El Estado retado desde el constructivismo antiformalista: legitimidad y convicción' (2021) 14 Criterios, 21-36.

tecnológica que aporte a la gestión del área del derecho privado a través de la inteligencia artificial? Al respecto de esta pregunta se formula una hipótesis a manera de respuesta anticipada que se validará con la investigación, la cual indica que desde el enfoque de la estructura de las disciplinas es posible conformar un procedimiento basado en cuatro etapas fundamentales, a partir de las cuales se pueden hacer derivaciones en casos concretos. Así, se plantea que la programación tecnológica inicial de esta área del derecho debe realizarse con fundamento en etapas mínimas, las cuales pueden representar toma de decisiones por parte de la inteligencia artificial una vez se enfrente a situaciones específicas que exigen soluciones desde el derecho.

Siendo así, y guardando coherencia con la pregunta y la hipótesis de investigación anteriores, el objetivo general de este artículo consiste en determinar la manera como se pueden sistematizar de manera uniforme las etapas para poder ser titular de derechos reales desde una eventual programación tecnológica que aporte a la gestión del área del derecho privado a través de la inteligencia artificial. Como desarrollo de este objetivo general se formulan los siguientes objetivos específicos a manera de estructura argumentativa del presente artículo: primero, plantear una relación uniforme que agrupe las múltiples posibilidades de consolidación de derechos reales propia del derecho privado; y segundo, formular lineamientos de programación para un desarrollo tecnológico que facilite la gestión del derecho privado desde la inteligencia artificial.

La presente investigación asume un enfoque de estructura de las disciplinas, el cual reconoce que, desde una perspectiva hermenéutico-crítica, el autor está llamado a formular lineamientos mínimos con el fin que el lector pueda generar derivaciones desde su propio contexto; este enfoque se aleja de las pretensiones de normalización absoluta de la ciencia, para otorgar marcos interpretativos que el lector puede ajustar según la realidad en la cual se desempeñe. Para estos efectos se adoptan métodos de investigación cualitativos, cuya recolección y validación de la información está dada por la revisión de documentos científicos. Estos documentos no se refieren de forma íntegra a la propuesta académica que aquí se propone, pues eso implicaría que no es novedosa la formulación del presente artículo. Por el contrario, cada una de las investigaciones se refieren a apartes puntuales de la propuesta académica, que al conjugarlas permite generar una interpretación auténtica[2].

1. Relación uniforme de las etapas del derecho privado para configurar derechos reales.

El derecho privado ha sido entendido tradicionalmente como el conjunto de normas que regulan las relaciones entre particulares, entre las cuales se

[2] La interpretación auténtica responde a un alcance antiformalista de la investigación, la cual permite subsanar vacíos legales desde la interpretación de múltiples fuentes. En la medida en que se conjuguen múltiples fuentes, será posible establecer una propuesta hermenéutica desde y para el contexto del cual se trate. Esta contextualización genera un alcance propio de la investigación, el cual se conceptualiza desde la autenticidad. Para profundizar en el tema de la investigación auténtica se puede consultar: JSA Perilla-Granados, 'Hacia una investigación educativa antiformalista' in JSA Perilla-Granados (ed), *Experiencias de innovación educativa desde investigaciones antiformalistas* (Universidad Sergio Arboleda 2018), 31.

encuentran las relaciones familiares, contractuales, entre otras. Y aunque ha tendido a presentarse como un marco regulatorio mínimo para que en estas relaciones se cuente con cierto nivel de armonía entre los integrantes de la sociedad, existe un propósito marcadamente patrimonial en esta área del derecho; el derecho privado ha buscado garantizar el ejercicio de la propiedad privada de los particulares, sin injerencias o limitaciones externas[3]. Por lo mismo, es importante recordar que el derecho privado ha construido un marco regulatorio suficientemente sólido para proteger, en últimas, la propiedad privada de los particulares. Y es, precisamente, la propiedad privada aquella que, desde la teoría del patrimonio, se relaciona directamente con derechos reales de los cuales trata la presente investigación.

En este sentido, la propiedad privada se materializa en la medida en que el patrimonio de cada persona, natural o jurídica, esté conformado por bienes. Esos bienes son objetos sobre los cuales recaen derechos reales, entre los cuales se encuentran el dominio, el uso, el goce, el disfrute, el usufructo, entre otros[4]. Por lo mismo, una persona particular podrá ser considerada propietaria en la medida en que su patrimonio esté conformado por bienes sobre los cuales ostenta derechos reales[5]. Y la garantía de estos derechos reales que llevan a la consolidación de la propiedad privada es uno de los principales propósitos del derecho privado[6]; los sistemas jurídicos construyen marcos regulatorios para que las personas puedan configurar, ejercer y garantizar los derechos reales que ostentan sobre bienes concretos.

Al respecto, se debe reconocer que tanto la configuración, el ejercicio y la garantía de los derechos reales contienen reglas que pueden ser objeto de sistematización para el desarrollo tecnológico. Esto se justifica al considerar que la configuración se refiere a aquellos requisitos que desde un alcance procedimental se deben cumplir para ser titular de derechos reales, una vez que se tiene tal titularidad será posible ejercerla sobre bienes concretos y, finalmente, a medida que se ejerce la titularidad el derecho debe otorgar garantías tanto sustanciales como procesales para hacerlos oponibles ante

[3] Diferentes investigaciones han sistematizado los debates en torno a los fines del derecho privado y su relación con la armonía entre particulares. Para concoer estos debates desde la perspectiva de la jusrisdicción civil y con una tendencia mundial se recomienda leer: L Galbán-Rodríguez, 'Valores constitucionales: su relación y distinción con los derechos y principios para la resolución de casos en materia civil' (2023) 43 Rev. Derecho Privado, 43-75.

[4] Se presenta una relación dinámica entre bienes, patrimonio y propiedad privada, la cual es secuencial al considerar que los bienes en su conjunto son el patrimonio. Así, toda persona tiene un patrimonio como atributo de la personalidad y en él pueden contenerse bienes (o deudas). Y es el patrimonio aquel que, desde su calidad de atributo de la personalidad, permite configurar la institución jurídica de la propiedad privada. Esto es explicado por recientes investigaciones, las cuales consideran que los bienes hacen parte del patrimonio y el patrimonio hace parte de la propiedad privada. Para profundizar en esta relación se recomienda consultar: JSA Perilla-Granados, *Derecho de Sucesiones* (2 edn, Universidad Sergio Arboleda 2017) 19.

[5] Es común encontrar investigaciones sobre los alcances de la propiedad privada desde la visión jurídica occidental. Un ejemplo reciente que sistematiza los hallazgos en esta área específica es el siguiente: P Guerra-Araya, 'La propiedad privada como canon: notas para su deconstrucción' (2023) 36 Rev. Derecho (Valdivia), 91-111.

[6] Esta concepción en torno al derecho privado se puede profundizar en esta investigación: F Hinestrosa, 'Código Civil y dispersión normativa' (2024) 46 Rev. Derecho Privado, 5-11.

terceros[7]. Se trata de un complejo entramado de acciones que requerirían desarrollos tecnológicos particulares, pero al considerar que la primera de ellas se refiere a la configuración, se adopta en este caso como objeto de investigación.

Ahora bien, el problema de sistematizar los requisitos para la configuración de los derechos reales recae en la multiplicidad de posibilidades que actualmente existen para ello; se tienen desde situaciones naturales hasta jurídicas, vinculando diferentes soportes documentales y requisitos tanto formales como sustanciales diversos. Así, y desde los fundamentos de la estructura de las disciplinas, se propone comprender este asunto desde cuatro etapas concretas: la primera, referente a las fuentes de los derechos reales; la segunda, propia de los títulos que materializan las fuentes en mención; la tercera, que contiene los modos que operativizan al título; y la cuarta, los derechos reales en sí mismos[8]. Se trata de una propuesta aplicable a casi cualquier situación jurídica tendiente a alcanzar derechos reales, en la cual cada una de las etapas es prerrequisito indispensable de la otra o, por lo menos, fundamento necesario para generar continuidad. Esta relación se puede entender gráficamente así:

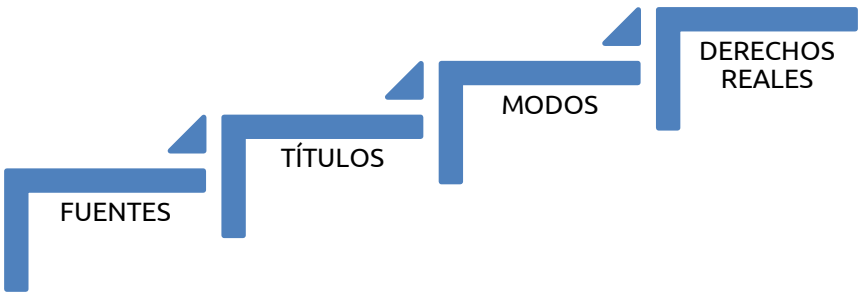


Figura 001. Pasos para la configuración de los derechos reales
Elaboración propia

Este esquema gráfico establece que para adquirir derechos reales se requiere cumplir una serie de pasos, que, en conjunto, llevan a generar una relación causal propia del derecho privado. Esta relación causal no es meramente teórica, pues, al dirigirse a situaciones de personas particulares, requiere materializarse desde sucesos de la realidad. Por lo mismo, cada uno de estos pasos responde a una situación específica a la cual se debe aplicar esta estructura de sistematización[9]; si se llevase a un desarrollo tecnológico, la

[7] El derecho occidental encuentra uniformidad en la reglamentación de los derechos reales que recaen sobre los bienes, dado que son concebidos en el norte global y luego trasplantados al sur global. Este ejercicio jurídico es sistematizado a manera de referente aquí: J Alcalde-Silva, 'Bienes y derechos reales' (2020) 34 RChDP, 315-334.

[8] Una primera aproximación al tema fue realizada por el autor en materiales pedagógicos de clase, a saber: JSA Perilla-Granados, *Derecho de Sucesiones* (2nd edn, Universidad Sergio Arboleda 2017) 36.

[9] Se reconoce que los abogados no están necesariamente formados para desarrollar aplicativos, pero sí para formular estructuras con rigor jurídico que posteriormente serán desarrolladas por técnicos. Esta lógica de

programación que sustente este asunto deberá asumir como estructura estos cuatro pasos concretos. Así, las herramientas de inteligencia artificial aplicables al derecho privado deberán acoger en su programación que las fuentes realizan una lectura de los sucesos para otorgarles una denominación jurídica a través de los títulos y aplicar un procedimiento de los modos para configurar los derechos reales.

De esta forma, las fuentes de los derechos reales, en su calidad de primer paso, están dadas por los sucesos o acontecimientos que se gestan en la realidad cotidiana. Estas fuentes podrán ser o no relevantes para los derechos reales, por lo cual lo primero que se deberá determinar es si son o no jurídicamente importantes; esta relevancia jurídica se determinará si generan consecuencias para la configuración de derechos reales según los pasos siguientes. Por lo mismo, al analizar los sucesos de la realidad se pueden identificar tres tipos de fuentes: los hechos, los actos y los negocios. Cada uno de ellos se debe analizar según qué o quién los genera, así como sus respectivas consecuencias jurídicas. En este sentido, los hechos son generados por la naturaleza y sus consecuencias en relación con los derechos reales están dados por la ley[10]. Por su parte, tanto los actos como los negocios son generados por las personas, pero las consecuencias principales de los actos los da la ley y las consecuencias principales de los negocios los dan las personas.

Una vez se han identificado las fuentes de los derechos reales que pueden tener cierto nivel de relevancia jurídica, es fundamental calificar jurídicamente para configurar un título; esta calificación consiste en otorgarles una denominación según lo disponga la ley o cada persona[11]. Así, por ejemplo, una fuente relevante para los derechos reales puede ser el hecho de que un río se seque por causas naturales y no se sabe en consecuencia a quién corresponde el nuevo terreno que antes ocupaban esas aguas. En este caso se trata de un hecho natural, por lo tanto, la ley determinará como consecuencia principal que se trata de un aluvión y allí se configura el titulo justo para adquirir derechos reales sobre el terreno que se discute. Pero puede darse el caso en el cual la ley no genere denominación al suceso, caso en el cual se podrá acudir a la(s) persona(s) involucradas, como en el contexto de las transacciones trasnacionales con criptomonedas.

Cuando se tiene el título que materializa jurídicamente a la fuente se procede a aplicar una serie de reglas procedimentales para alcanzar finalmente el derecho real; los modos tradicionalmente considerados son la prescripción, la accesión, la ocupación, la tradición y la sucesión. Estas reglas procedimentales son denominadas modos, que responden a una serie de disposiciones que han de seguirse para perfeccionar el contenido del título[12].

---

formulación de estructuras encuentra sus fundamentos en este tipo de investigaciones previas: R Segura, 'Inteligencia artificial y administración de justicia: desafíos derivados del contexto latinoamericano' (2023) 58 Rev. Bioética y Derecho, 45-72.

[10] Se recomienda revisar la siguiente investigación como un aporte reciente a la diferenciación de las fuentes de los derechos reales: F Atria-Lemaitre, 'La noción de poder normativo la distinción entre hechos y actos jurídicos' (2023) 36 Rev. Derecho (Valdivia), 27-48.

[11] Un pertinente estudio exploratorio sobre los títulos, su origen y concepción actual es el siguiente: N Ramírez, M Uribe, 'Título y el modo: definición, evolución y su relación con las fuentes de las obligaciones' (2019) 3 Rev Est de Der Pri Uni Exter de Col, 1-23.

[12] Sobre el particular se recomienda consultar: F Hinestrosa, 'Actualización y unificación del derecho privado' (2018) 35 Rev. Derecho Privado, 5-17.

Así, por ejemplo, puede que se tenga como fuente un negocio jurídico innominado referente a la creación de criptomonedas, caso en el cual la denominación del título bien puede provenir de las personas involucradas. Sin embargo, una vez que son creadas estas criptomonedas deben ser entregadas, como mínimo de manera simbólica, a quienes van a ostentar derechos reales sobre este bien inmaterial. Así, esa entrega hace referencia al modo de la tradición legalmente considerado y que perfecciona el título al permitir que el titular del derecho pueda disponer del bien que adquiere.

Y si se cumple con alguno de los modos típicos y nominados, aunque no se descarta la existencia de otros atípicos e innominados, se alcanzarán en última instancia los derechos reales[13]. Recuérdese que el derecho real por excelencia es el de dominio, el cual tiene alcances que en sí mismos también son derechos reales y que contemplan algunos como el uso, goce, disfrute, usufructo, etc. Se evidencia de esta forma que, al identificar un suceso jurídicamente relevante en el primer paso de la fuente, es posible configurarlo como un título propio del derecho privado y este tiene la posibilidad de exigir la realización de unos procedimientos específicos a manera de modo para alcanzar al final un derecho real en particular[14]. Este esquema tiene la vocación de ser aplicado, por lo menos en su estructura general, a cualquier suceso relacionado con los derechos reales y sistematiza, en últimas, un asunto que generalmente abarca los debates jurídicos de una parte del derecho privado.

Si la configuración de los derechos reales se puede sistematizar de una manera esquemática, los operadores jurídicos podrían tener respuestas sobre la titularidad de un derecho de una manera medianamente automática. Esta tarea optimizaría procesos declarativos, constituyéndose en un apoyo para los operadores jurídicos que puede aportar a la descongestión judicial; en la medida en que se entiendan los requisitos mínimos para adquirir un derecho real y que son comunes para diferentes situaciones, es posible programar un desarrollo tecnológico que lo aplique a partir de información concretamente otorgada por el ser humano. Y es por esta razón que en la sección siguiente se procederá a proponer cuáles deberían ser esos lineamientos mínimos para que se pueda genera un desarrollo tecnológico que permita solucionar conflictos sobre la configuración de derechos reales en cabeza de personas específicas.

2. Lineamientos de programación para un Desarrollo tecnológico applicable al derecho privado.

[13] El contexto actual ha establecido cuestionamientos sobre la aplicación práctica de los modos existentes en la actualidad, dado que responden a dinámicas históricas diferentes a las relaciones contractuales que son mediadas actualmente por la tecnología. Así, se ha abierto la posibilidad para que las partes contratantes establezcan los modos para el cumplimiento de sus obligaciones a través de licencias, amparados en la autonomía de las partes. Esto implica la posibilidad de aplicar modos diferentes a los de la ley y que, en muchas ocasiones, tienen alcances trasnacionales. Sobre los debates de licencias se puede consultar: JSA Perilla-Granados, 'Alineación iusteórica de las licencias creative commons' (2013) 50 Revista de Derecho Privado Universidad de los Andes, 1-29.

[14] Como un ejemplo aplicado de los alcances de los derechos reales que constituyen en conjunto la propiedad privada se recomienda consultar esta investigación: PO Armijos-González, 'El derecho a la propiedad privada frente a los tributos con efectos confiscatorios' (2023) 39 Rev de Dere, 129-148.

La configuración de derechos reales tiende tener múltiples posibilidades, por lo cual tienden a generarse debates jurídicos sobre la titularidad que tienen las personas sobre los bienes y, en últimas, sobre el alcance a la propiedad privada. Siendo así, una proporción importante de los asuntos que conoce la jurisdicción civil, e incluso la comercial, consiste en determinar quiénes ostentan o no derechos reales sobre bienes determinados. Estos procesos implican analizar diferentes pasos que desde pruebas concretas configuran los derechos reales, lo cual es un asunto que puede ser objeto de sistematización para hacer un eventual desarrollo tecnológico que automatice desde la inteligencia artificial esta labor eminentemente humana. Para ello, se establecieron cuatro pasos generales: las fuentes, los títulos, los modos y los derechos reales. Se procede, entonces, a proponer cómo debería ser un lineamiento de programación para que se puedan resolver estos casos con apoyo de la tecnología.

Abordando el primer paso de las fuentes, la programación a desarrollar debería fundamentarse en un modelo dicotómico de respuesta positiva o negativa a partir de preguntas. Así, lo primero que se debería exigir es la narración escrita u oral por parte de una persona de aquello que genera el aparente problema. En esta narración se debe verificar que se respondan a cinco preguntas básicas: quién, qué, cómo, cuándo y dónde[15]. A partir de la narración completa se deberá determinar si alguno de los sucesos conlleva en sí mismo un problema jurídico referente a los derechos reales, para lo cual se determinará si es o no jurídico. Considerando los sucesos jurídicos se tendrá la posibilidad de determinar si son o no hechos, actos o negocios, según sean generados y sus consecuencias determinadas por la naturaleza o las personas. Con fundamento en ello, el desarrollo tecnológico ya tendrá la posibilidad de determinar si es un asunto que sea o no del área del derecho privado referente a los derechos reales. Para comprender esta propuesta diagramada en un flujograma se recomienda consultar el ANEXO 001.

Un ejemplo concreto puede ser la narración que hace una persona natural acerca del fallecimiento de su padre como consecuencia de un infarto. En este caso, el aplicativo debe estar en la capacidad de preguntar las condiciones de tiempo, modo y lugar, así como si, por ejemplo, la persona que falleció tenía o no bienes. Si las respuestas son positivas, se tratará de un hecho con relevancia jurídica para determinar la titularidad de los derechos reales sobre los bienes de quien falleció naturalmente. Allí se podrá preguntar sobre otros asignatarios, al respecto de los cuales se puede indicar que además de quien consulta, sobrevive otro hijo que acordó con un amigo la cesión de sus eventuales derechos a cambio de un pago[16]. En este caso, el aplicativo podrá evidenciar que hay tres sucesos para los derechos reales: primero, un hecho natural referente a la muerte del causante; segundo, el acto jurídico de reconocimiento de paternidad; y tercero, el negocio sobre los eventuales

[15] Recientes investigaciones se han referido a la necesidad de utilizar un lenguaje claro y, por lo tanto, completo en las áreas jurídicas. Se recomienda profundizar con la consulta de las obras aquí referenciadas: R Amaya-González, 'Por el derecho a comprender: lenguaje claro' (2022) 23 EUNOMÍA Rev Cultura Legali, 526-528.

[16] Estos casos resultan frecuentes en el contexto actual, por lo cual se puede encontrar más información en este tipo de investigaciones: H Corral-Talciani, 'Enajenación y transmisión del derecho real de herencia: estudio de la cesión de derechos hereditarios y otras formas de disposición' (2023) 40 RChDP, 9-47.

derechos sucesorales. Así, se deberá evaluar si estas fuentes constituyen en sí mismas un título justo que permita continuar hacia la configuración de derechos reales.

Ahora bien, una vez fue identificada la fuente en el primer paso, se requiere calificar la misma desde el título. La calificación del título exige un ejercicio silogístico, en el cual la premisa mayor del silogismo es el suceso jurídico (hecho, acto o negocio) y la premisa menor lo dispuesto por la ley, a partir de lo cual se puede determinar si se trata de un asunto típico y nominado[17]. Si se trata de un asunto típico y nominado, se analizarán los requisitos para que pueda ser considera un título justo[18]. Pero si se trata de una fuente atípica e innominada, la gestión depende de si las consecuencias son determinadas por la ley o por las personas. Así, si se trata de un hecho o un acto, se acudirá a la analogía o a los principios generales del derecho para asegurar la denominación. Por su parte, si se trata de un negocio atípico e innominado, se respetará lo determinado por las personas. Adviértase que cuando se trata de negocios jurídicos se requiere analizar la teoría de la eficacia del negocio, es decir, si es existente, válido y oponible. Del análisis de estos requisitos se puede concluir si el título es suficiente para aplicar el modo del tercer paso. El flujograma aplicable al título puede ser consultado en el ANEXO 002.

Siguiendo con el caso de ejemplo antes enunciado, una vez se ha identificado el hecho, el acto y el negocio jurídico, se procede a realizar el ejercicio silogístico. En el caso del fallecimiento por causas naturales, la ley determinará que es una muerte que debe contar con una prueba jurídica para ser probada y que, generalmente, es un documento como un registro civil de defunción. Sobre el acto de reconocimiento, se denominará legalmente como filiación y su requisito fundamental se prueba con un documento como el registro civil de nacimiento. Y en el caso del negocio mencionado antes, se puede denominar como venta de derechos herenciales entre vivos y sus requisitos serían: en la existencia, la determinación del derecho y el valor a cambio del mismo, así como la firma ante autoridad competente; en la validez se analizará la capacidad de los contratantes, el consentimiento libre de vicios, la causa lícita y el objeto lícito; y la oponibilidad se verifica con la obligatoriedad que se tenga frente a terceros[19]. Aunque según cada ordenamiento jurídico las denominaciones podrán variar, se configura un esquema que a manera de programación puede ser adaptado según cada realidad.

[17] Téngase en cuenta que la categoría de típico indica que está contemplado expresamente por la ley escrita. Por su parte, el alcance nominado implica que la ley le otorga una denominación concreta. Sobre el particular se puede consultar la aplicación práctica de estos conceptos en investigaciones relacionadas con el uso de la tecnología en derecho: JA Cáceres-Malagón, '¿Sueñan las máquinas con contratar? Un estudio sobre smart contracts y consentimiento algorítmico' (2024) 46 Rev. Derecho Privado, 155-185.

[18] Las sociedades actuales tienden a desbordar en gran medida las normas jurídicas, por lo cual se presentan de manera recurrente fenómenos de atipicidad y, consecuentemente, de falta de nominación legal. Un ejemplo de esta situación lo constituye esta investigación: ME Camacho-López, 'El interés negocial como criterio de distribución del riesgo contractual en el derecho romano y su posible utilidad en contratos atípicos como el leasing financiero' (2024) 46 Rev. Derecho Privado, 187-210.

[19] El cumplimiento de los requisitos de existencia, validez y oponibilidad del negocio jurídico constituyen la teoría de la eficacia del contrato. Una investigación que ilustra este tema es la siguiente: E Pereira-Fredes, 'Ruptura entre promesas, voluntad y autonomía: ¿qué justifica la fuerza obligatoria del contrato?' (2022) 89 Derecho PUCP, 291-323.

En cualquier caso, una vez configurado el justo título se procede a verificar cuál es el modo aplicable[20]. Existen diferentes modos, los cuales pueden resumirse así: la prescripción adquisitiva, la cual se configura por el paso del tiempo según condiciones de buena fe legalmente establecidas, su título es la posesión y la fuente un acto jurídico; la accesión consiste en la unión permanente de diferentes bienes, cuyo título puede ser variado según se trate de muebles, inmuebles y otros que cuentan con fuentes naturales y humanas; la ocupación que se fundamenta en adquirir bienes muebles por el paso del tiempo, cuyos títulos tienden a ser el hallazgo, el tesoro y otros que generalmente son actos jurídicos en calidad de fuentes; la tradición que se materializa en la entrega real o simbólica de los bienes, donde los títulos son múltiples dadas las fuentes naturales y humanas que se presentan; y la sucesión por causa de muerte, cuyos títulos podrán ser la muerte, la filiación o los contratos entre personas, que materializan los tres tipos de fuentes ya mencionados. La sistematización gráfica del modo se encuentra en el ANEXO 003.

Así, el modo es aquel que sigue una serie de pasos para poder perfeccionar el alcance del derecho real. En el caso que se analiza como ejemplo, se tendrá la sucesión por causa de muerte como modo y exige adelantar una serie de requisitos legales expresamente considerados para adquirir los derechos. Así, el aplicativo tendrá la posibilidad de orientar, e incluso preparar, el memorial que conocerá la autoridad, la práctica de pruebas, la liquidación de la masa herencial, la distribución de derecho y hasta la asignación de bienes concretos[21]. Se requiere del cargue de las condiciones legalmente consideradas en cada sistema jurídico, para que a partir del cumplimiento de supuestos legales concretos el aplicativo pueda asumir una compleja labor que tradicionalmente ha demando gran dedicación por el ser humano.

Lo que sí es cierto es que una vez llevado a cabo el modo y validados los requisitos esperables para el mismo, se podrá concluir quién es el titular de determinado derecho real. Para ello se deberán formular supuestos de hechos que determinen el alcance de cada uno de los derechos reales, donde el derecho real de dominio es la potestad plena de usar, gozar y disfrutar del bien, salvo algún límite expresamente considerado por la ley. Por su parte, el uso solo se refiere a la posibilidad de servirse de un bien particular sin que represente un beneficio económico a manera de frutos y de manera individual; el goce implica servirse del bien sin percibir frutos y vinculando a terceras personas; el disfrute consistirá en percibir frutos de manera individual o colectiva; entre otras posibilidades previstas por cada sistema jurídico. En el caso de la sucesión que se analiza como ejemplo, el derecho real que se adquiere es el de dominio pleno sobre los bienes que el causante tenía en su patrimonio al momento de la muerte. La determinación del derecho real se puede comprender gráficamente en el ANEXO 004.

[20] Sobre la relación de los modos y la posibilidad de trascender sus concepciones tradicionales se refiere esta investigación: C Correa-Robles, 'Derecho Privado y proceso civil: más allá del interés individual' (2022) 38 RChDP, 173-225.

[21] Sobre los temas de programación que aquí se sugieren se recomienda consultar: AM Porcelli, 'La inteligencia artificial y la robótica: sus dilemas sociales, éticos y jurídicos' (2020) 6 Derecho glob. Estud. sobre derecho justicia, 49-105.

Se evidencia de esta forma una estructura de cuatro pasos, donde cada paso exige analizar una serie de dicotomías propias de la programación, para resolver en última instancia los debates en torno a la titularidad de los derechos reales. Se trata de una serie de pasos comunes al derecho privado occidental, el cual tendrá desarrollos específicos según cada sistema jurídico en el cual se aplique. Por lo mismo, la propuesta aquí contenida configura una propuesta reguladora de una eventual programación tecnológica, que bien puede, y debe, ser reglamentada según la realidad específica de la cual se trate. Se formula de esta manera una propuesta esquemática que puede fundamentar la estructura de una programación para gestionar debates en torno a la titularidad de derechos reales sobre bienes concretos, que bien puede ser objeto de derivaciones contextualizadas para generar pleno sentido de utilidad.

Conclusiones.

El contexto jurídico actual se enfrenta a la posibilidad de sistematizar sus prácticas para determinar en qué medida se puede vincular la inteligencia artificial. Para ello, es fundamental considerar que difícilmente pueden existir desarrollos tecnológicos capaces de abordar al derecho en conjunto y, por el contrario, se sugiere analizar estas posibilidades por áreas jurídicas concretas. Una de estas áreas es la del derecho privado, la cual ha tendido a presentarse como el conjunto de normas que regulan las relaciones armónicas entre particulares. Entre otros propósitos, muchos de ellos propios de respuestas políticamente correctas, se encuentra aquel encaminado a proteger la propiedad privada de las personas. Esa propiedad privada está dada por el patrimonio que cada sujeto tiene y que se entiende como el conjunto de bienes sobre los cuales se tienen derechos reales.

En torno a estos derechos reales se pueden adelantar diferentes debates, entre los cuales se encuentran aquellos referentes a su configuración, el ejercicio y la garantía. Considerando que el asunto de la configuración es un primer alcance fundamental en torno a los derechos reales, se analizó cómo se pueden sistematizar de manera uniforme las múltiples posibilidades de configuración de derechos reales para poder consolidar una eventual programación tecnológica que aporte a la gestión del área del derecho privado a través de la inteligencia artificial. Para estos efectos se adoptó un enfoque de estructura de las disciplinas, en virtud del cual se formulan lineamientos mínimos comunes a diferentes contextos y que pueden ser adaptados a partir de derivaciones propias del contexto desde y para el cual se interprete la propuesta.

En este sentido, el asunto de la configuración de los derechos reales se sistematizó en cuatro pasos, a saber: primero, las fuentes; segundo, los títulos; tercero, los modos; y cuarto, los derechos reales en sí mismos. Esta propuesta configura un esquema articulado para desarrollar futuros desarrollos tecnológicos, en virtud del cual se pueda emplear la inteligencia artificial para determinar la titularidad de un derecho real en relación con un bien específico. Para ello, lo primero que se debe hacer es contar con una narración que sea clasificada en hechos, actos y/o negocios, según sean generados por la

naturaleza o las personas, y sus consecuencias determinadas por la ley y por las personas. Cada una de esas fuentes deberá ser evaluada desde los requisitos silogísticos de un título justo, para aplicar un modo que permita alcanzar el derecho real en última instancia.

Esta relación dinámica de cuatro pasos puede ser aplicada a cualquier situación del derecho privado tendiente a constituir a favor de alguna persona un derecho real sobre un bien, lo cual dependerá de las condiciones de cada uno de los sistemas jurídicos. Pese a ello, es posible determinar una estructura condicionada de flujo para que la programación cuente con una estructura general para resolver los debates en torno a estos asuntos. Poder resolver estos debates de manera automatizada permite tener un aporte importante para uno de los asuntos que ocupan en gran medida a la jurisdicción civil y comercial, al tiempo que contribuir a la descongestión judicial. Para ello, además de la estructura de flujo condicional y silogística aquí planteada, se requerirá aportar las particularidades jurídicas que la ley establece en cada sistema jurídico en el cual pretenda aplicarse la herramienta.

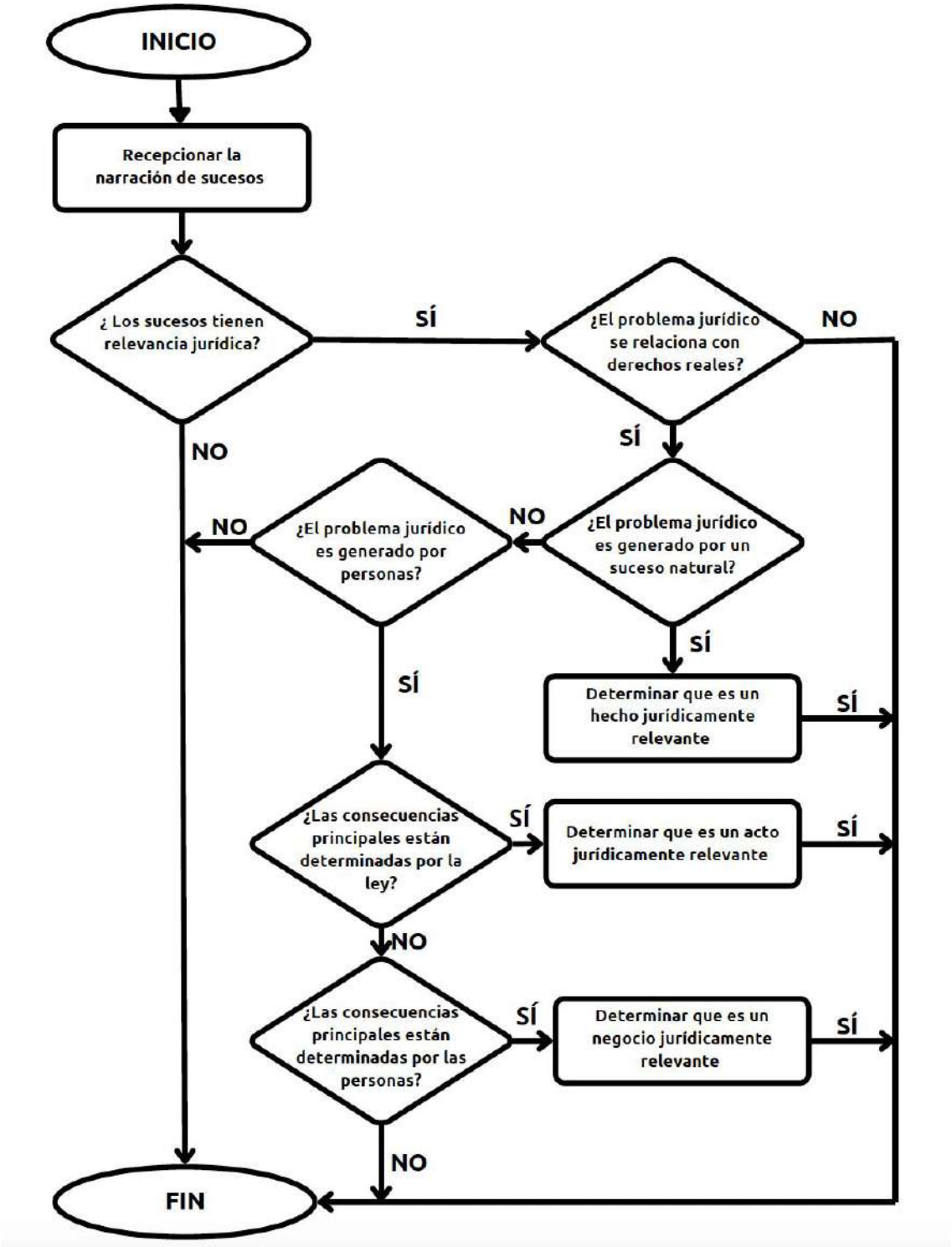
Con fundamento en esta estructura general de flujo, es posible aceptar la hipótesis de investigación del presente artículo y que establece que desde el enfoque de la estructura de las disciplinas es posible conformar un procedimiento basado en cuatro etapas fundamentales, a partir de las cuales se pueden hacer derivaciones en casos concretos. Así, en efecto se planteó que la programación tecnológica inicial de esta área del derecho debe realizarse con fundamento en etapas mínimas, las cuales pueden representar toma de decisiones por parte de la inteligencia artificial una vez se enfrente a situaciones específicas que exigen soluciones desde el derecho. Se trata de una propuesta marco que espera por ser desarrollada desde y para realidades concretas, de tal manera que el reto global de acoger la inteligencia artificial en el derecho pueda ser acogido desde desarrollos tecnológicos auténticos.

ANEXO 001

Flujograma para la programación de las fuentes de los derechos reales

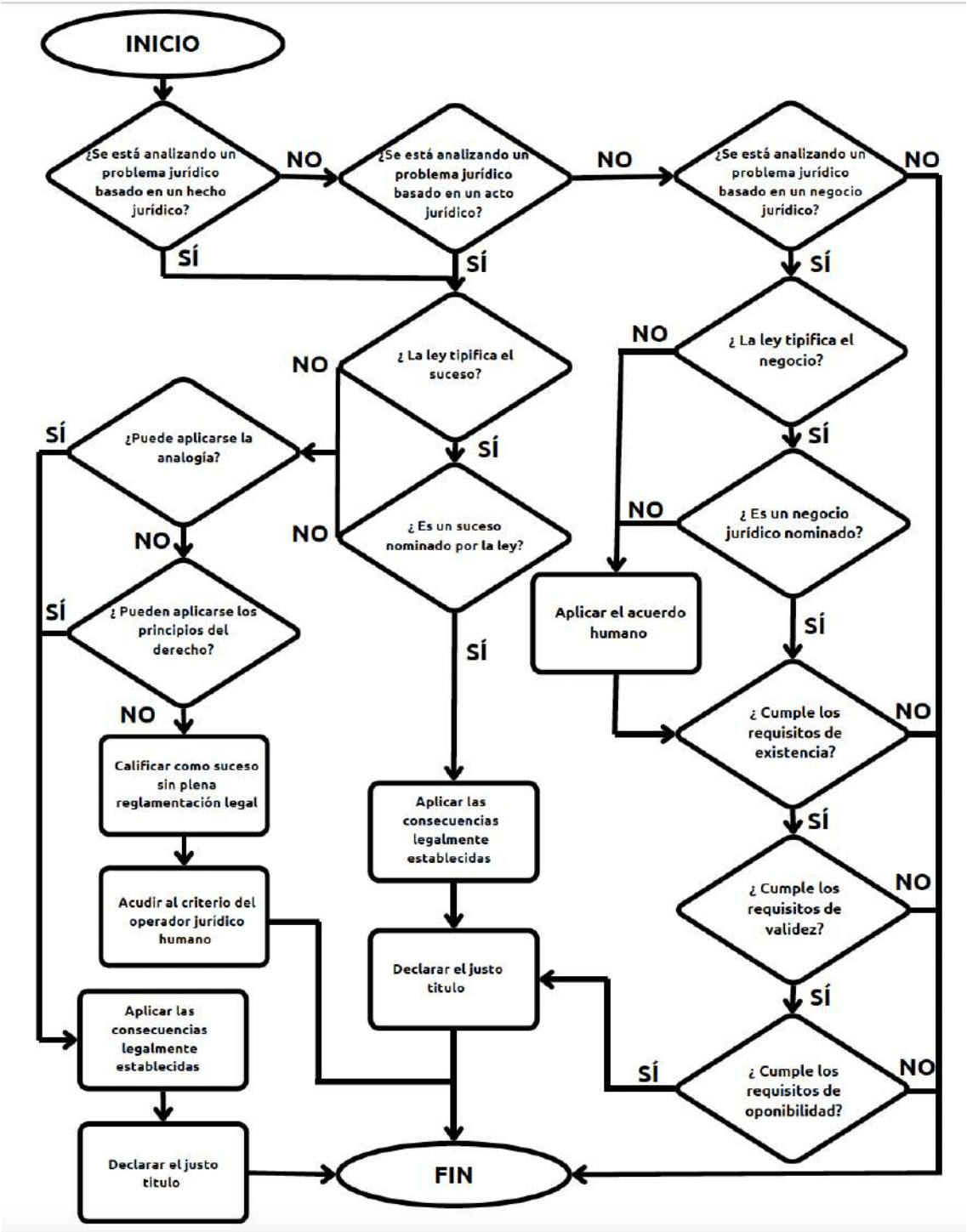
Elaboración propia

ANEXO 002



Flujograma para la programación de los títulos de los derechos reales

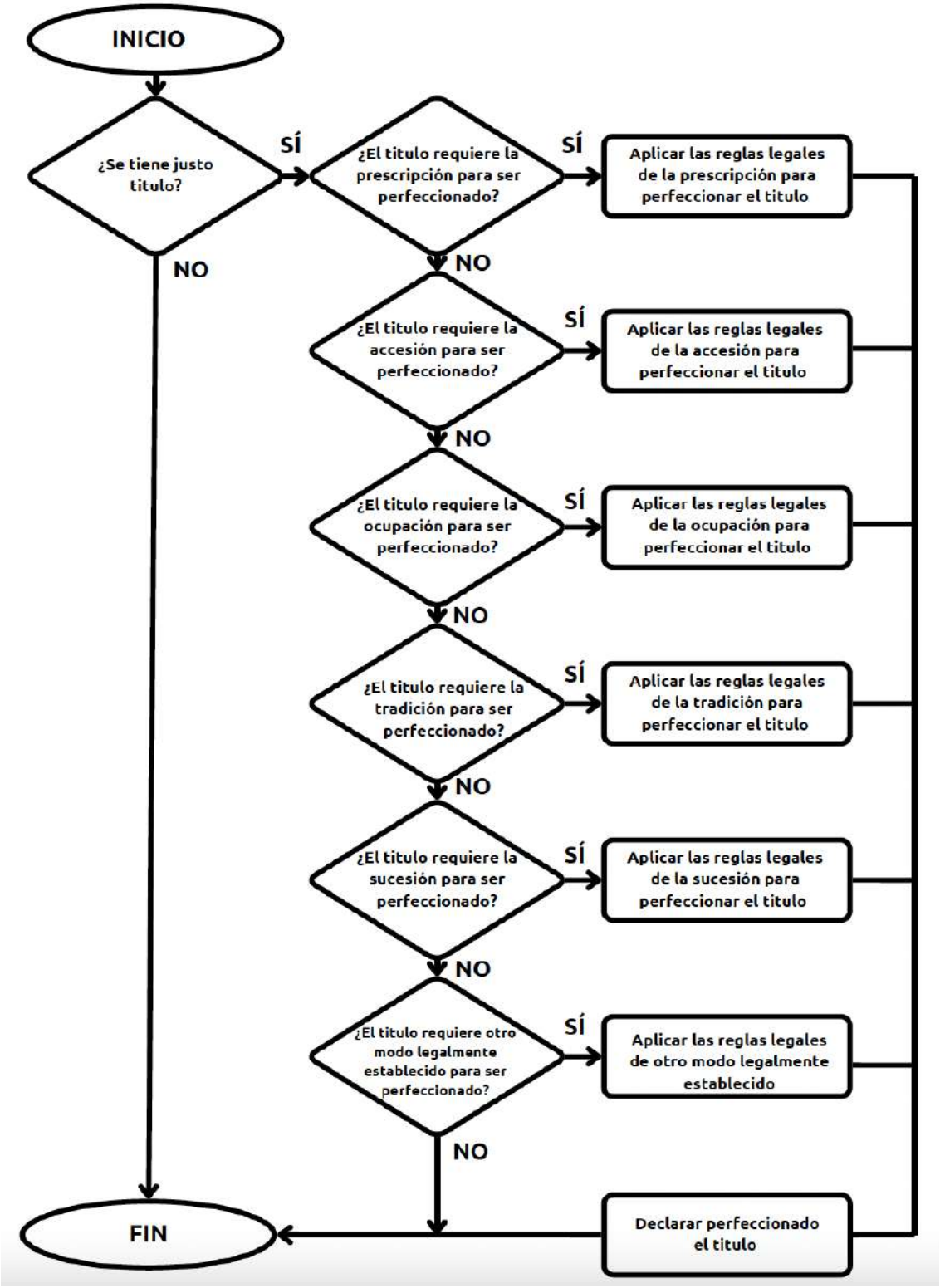
Elaboración propia



ANEXO 003

Flujograma para la programación de los modos para los derechos reales

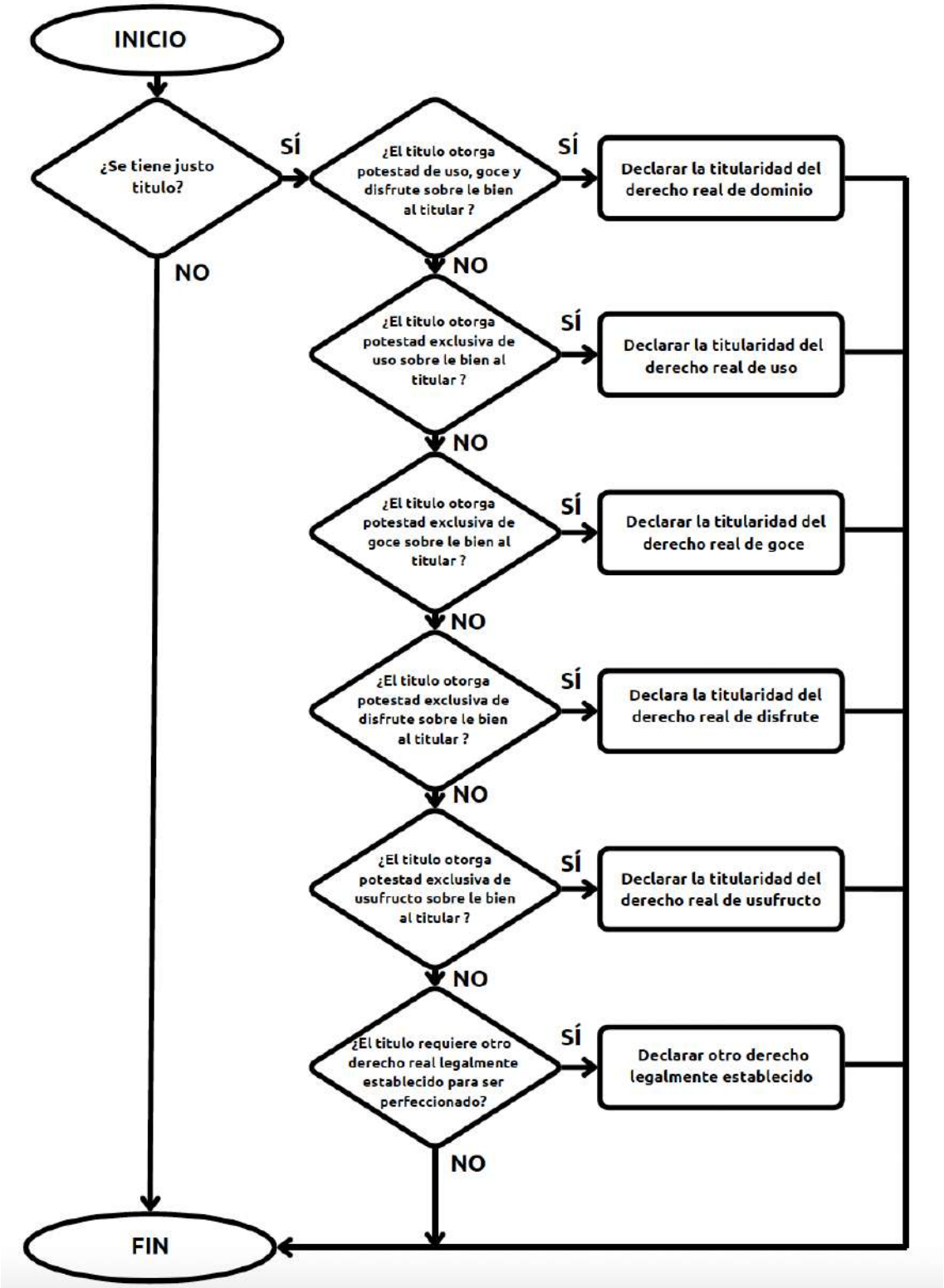
Elaboración propia



ANEXO 004

Flujograma para la programación de los derechos reales

Elaboración propia



Rubio Gimeno G, 'Vulnerabilidad y digitalización en la contratación de consumo : la perspectiva española' (2024) 1 EJPLT, 59-78.
DOI: https://doi.org/10.57230/EJPLT241GRG

EJPLT
ISSN 2704-8012

Vulnerabilidad y digitalización en la contratación de consumo: la perspectiva española

Vulnerability and digitalization in consumer contracting: the Spanish perspective

GEMMA RUBIO GIMENO
Associate Professor of Private Law
Universitat de Barcelona

Abstract

El presente estudio toma en consideración la noción de consumidor medio y de consumidor especialmente vulnerable con el fin de valorar la incidencia del entorno digital de contractación como un factor superpuesto de vulnerabilidad. Se plantean distintos elementos que inciden en la asimetría asociada a la digitalización de la contratación como son la brecha digital, el estado de flow o el scoring crediticio. En cuanto a la digitalización del contexto contractual, dada su incidencia generalizada, se valora si puede dar lugar a un reequilibrio desconectado de la concurrencia de otros factores de debilidad contractual.

The present study considers the notion of the average consumer and the particularly vulnerable consumer to assess the impact of the digital contracting environment as an additional factor of vulnerability. Various elements that contribute to the asymmetry associated with the digitalization of contracting are discussed, such as the digital divide, the state of flow and credit scoring. Concerning the digitization of the contractual context, given its widespread impact, it is considered whether it can lead to a rebalancing disconnected from the presence of other factors of contractual weakness.

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

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Consumidor medio; consumidor especialmente vulnerable; vulnerabilidad multifactorial; digitalización del contexto contractual.

Summary: 1. Introducción. – 2. Del consumidor medio al consumidor vulnerable: ¿una protección superpuesta o un régimen diferenciado? – 2.1. La persistente necesidad de una tuición abstracta general. – 2.2. La vulnerabilidad coyuntural y transitoria. – 2.3. La vulnerabilidad multifactorial. – 3. La digitalización como factor de vulnerabilidad. – 3.1. De la brecha digital al estado de flow: la digitalización del contexto contractual y del objeto del contrato como factores asociados de vulnerabilidad. – 3.2. En particular, la digitalización en el sector financiero y la fragilización resultante. – 4. Planteamiento tuitivo en casos de especial asimetría contractual. – 4.1. De la toma de decisiones con conocimiento de causa a la toma de decisiones óptimas. – 4.2. ¿Cómo se neutraliza o se reequilibra el déficit informativo? – 5. ¿La situación de vulnerabilidad es siempre oponible a la otra parte contractual? – 6. Conclusiones.

1. Introducción.[1]

Cuando incidimos en la protección de la parte débil en la contratación de consumo, se hace preciso distinguir entre la debilidad contractual de carácter abstracto que se predica de los consumidores como agentes del mercado y la fragilidad individual, que, como veremos, puede ser multifactorial, y que afecta a una determinada y concreta contratación de consumo aisladamente calificada [2]. La doctrina se ha referido, además, a las vulnerabilidades interseccionales o agravadas, por confluencia de varios factores -circunstanciales o no- que propician una situación de debilidad contractual[3] y, al hilo de ello, también podemos considerar supuestos de vulnerabilidad combinada por el hecho de añadir a la posición consumidora un solo factor adicional de debilidad contractual, por ejemplo, la edad o la discapacidad.

Llegados al estadio actual de desarrollo del derecho de consumo, cabe plantearse si debe superarse totalmente la protección basada en esa categoría abstracta y uniforme de persona consumidora en su acepción general o en cambio, hay que superponer dicha protección a la que resulte adecuada en función de las circunstancias concretas. Un debate distinto es el de la extensión

[1] Esta publicación forma parte de la ejecución del proyecto I+D+I (PID 2019-107195RB-I009) financiado por el Ministerio de Ciencia e Innovación: *Cumplimiento de los contratos y realidad digital: la adaptación del derecho contractual para la prevención de conflictos transfronterizos*. PID 2019-107195RB-I00.



También es el resultado de las actividades del Grup de Recerca consolidat *Dret civil català i dret privat europeu* (2017 SGR 997).

[2] M. Grochowski, *Does European Contract Law Need a New Concept of Vulnerability?* , en *EuCML*, 2021, 4.

[3] M.P. Palazón Garrido, *¿Existe un Estatuto del consumidor vulnerable tras la reforma del Texto refundido de la Ley general para la defensa de los consumidores y usuarios?*, en *Revista de Derecho Civil,* 2023, vol. X, núm. 4, 202 ss.

que deba darse a la protección dispensada a los consumidores a sujetos distintos, destacadamente micro-empresas y profesionales autónomos.

Seguramente la conclusión más razonable es que no puede prescindirse de un consumidor de referencia al que deba protegerse en todo caso, obviando sus características y circunstancias individuales. Se constata, además, que cuando se asume el rol de consumidor para contratar desde el ámbito privado, el sujeto habitualmente se debilita, pese a la formación o conocimiento del que pueda disponer y, por tanto, se origina una asimetría que podemos considerar de tipo estructural.

En cuanto a las situaciones de especial fragilidad contractual, es labor de la doctrina identificar los focos de vulnerabilidad, así, por ejemplo, el contexto digital de la contratación o la contratación sobre servicios digitales o bienes digitalizados, pero, sobre todo, lo fundamental es concretar las medidas de protección que deben aplicarse en cada caso y que no pueden consistir en una intensificación de los deberes informativos precontractuales.

A continuación, partiremos pues, de una aproximación a la definición de consumidor vulnerable y consideraremos si la digitalización del contexto o del objeto constituye efectivamente un factor debilitante adicional y de qué forma debe afrontarse dicha vulnerabilidad, bien distinta a la que podemos relacionar con factores individuales.

2. Del consumidor medio al consumidor vulnerable: ¿una protección superpuesta o un régimen diferenciado?

La fragmentación del concepto de consumidor ha sido puesta de relieve por la doctrina[4] así como la dificultad de identificar en la jurisprudencia los rasgos que definen al consumidor medio[5], noción que, además, no es sencilla de aplicar cuando se ejercitan acciones colectivas que agrupan en una reclamación sujetos protegidos con perfiles muy distintos o cuando las circunstancias que rodean la contratación pueden incidir en el nivel de atención y perspicacia aplicada por ese consumidor medio en función del planteamiento publicitario utilizado[6]. Ello dificulta el control abstracto en el cumplimiento de la previsión legal y cuestiona la utilidad de la categoría general de consumidor medio definido por

[4] H.W. Micklitz, *Il consumatore: mercatizzato, frammentato, costituzionalizzato*, en *Riv. trim. dir. e proc. civ.* 2016, 3, 874 ss., señala que no existe un único mercado, sino múltiples y todos ampliamente regulados. Ello hace que el consumidor se manifieste continuamente mediante nuevas formas, pasando del consumidor racional al consumidor conductual haciéndose eco de la triple distinción entre el consumidor responsable, el consumidor confiado y el consumidor vulnerable que no excluye la posibilidad de descripciones adicionales combinadas con las necesidades regulatorias. La Comisión europea ya se ha mostrado atenta al fenómeno de la economía conductual y así en la COM (2020) 696 final, p. 21, relativa a la "Nueva Agenda del Consumidor. Reforzar la resiliencia del consumidor para una recuperación sostenible" toma en consideración los riesgos asociados a la explotación de sesgos cognitivos que pueden afectar a todos los consumidores.

[5] S. Pagliantini, In memoriam *del consumatore medio*, en *Europa dir. priv.*, 1/2021, 1 y ss.

[6] En este sentido, el Tribunal Supremo, mediante auto de 29 de junio de 2022, ha planteado una cuestión prejudicial ante el TJUE sobre si es compatible con los arts. 4.2 y 7.3 de la Directiva 93/13/CEE que "pueda hacerse un control abstracto de transparencia desde la perspectiva del consumidor medio cuando varias de las ofertas de contratos están dirigidas a diferentes grupos específicos de consumidores, o cuando son múltiples las entidades predisponentes con ámbitos de negocio económica y geográficamente muy diferentes, durante un periodo de tiempo muy largo en que el conocimiento público sobre tales cláusulas fue evolucionando".

la jurisprudencia como aquel normalmente informado y razonablemente atento y perspicaz[7]. En realidad, en la definición del concepto de consumidor medio ya se ha añadido la necesaria consideración a las circunstancias concretas del caso[8]. Sea como fuere, los dos elementos que definen al consumidor medio -su actitud atenta y diligente- y la información o conocimientos de los que dispone-[9] permiten construir la expectativa con relación al funcionamiento del mercado. Por otro lado, la atención al consumidor especialmente vulnerable plantea dificultades adicionales que derivan principalmente de su caracterización individual.

Hasta la fecha, la contemplación del consumidor vulnerable no ha dado lugar a una protección reforzada de carácter general en fase de ejecución contractual y, por tanto, no ha surgido un estatuto del consumidor vulnerable que se superponga o que absorba el estatuto del consumidor medio. No se ha superado aún la orientación de la Directiva 2011/83/UE (DOUE-L-2011-82312) al atender, en su Considerando 34, a las necesidades informativas especiales de determinados consumidores en la contratación a distancia o fuera de establecimiento, por razón de enfermedad mental, física o psicológica, de edad o de credulidad, sin que ello, se advierte, pueda conducir a niveles distintos de protección. En la previsión actual de la legislación española, si acaso nos pudiésemos referir a ese estatuto, deberíamos circunscribirlo a los deberes

[7] La construcción del concepto ha sido el resultado de la labor del TJUE sobre todo durante la década de los años noventa (STCE, sala Quinta, de 21 de marzo de 1991, asunto Marie Delattre, C-369/88, STCE del Pleno, de 28 de octubre de 1992, asunto J.S.W. Ter Voort, C-219/91 o STCE, Sala Quinta, de 6 de julio de 1995, asunto Verein gegen Unwesen in Handel und Gewerbe Köln e. V., que aludían al "consumidor medianamente informado "o "razonablemente informado"), que cristalizó en la expresión acuñada por la STCE (Sala Quinta), de 16 de julio de 1998, asunto Gut Sprigenheide GmbH, C-210/96, mediante la caracterización del consumidor medio como aquel "normalmente informado y razonablemente atento y perspicaz"; la expresión se normalizó a partir de entonces y fue acogida por los pronunciamientos posteriores: STCE (Sala Quinta), de 28 de enero de 1999, asunto Verbraucherschutzverein, C-303/97, STCE (Pleno) de 22 de junio de 1999, asunto Lloyd Schuhfabrik Meyer and Co. GmbH, C-342/97, STCE (Sala Quinta) de 13 de enero de 2000, asunto Estée Lauder Cosmetics GmbH and Co. OHG, C-220/98, ECLI:EU:C:2000:8 o STCE (Sala Primera) de 4 de abril de 2000, asunto Verein gegen Unwesen in Handel und Gewerbe Köln eV, C-465/98. También halló acogida en textos legales con variaciones leves: así, en el Reglamento núm. 1924/2006 del Parlamento europeo y del Consejo, de 20 de diciembre de 2006, relativo a las declaraciones nutricionales y de propiedades saludables en los alimentos (considerando 15) o en la Directiva 2005/29/CE del Parlamento europeo y del Consejo, de 11 de mayo de 2005 (considerando 18). Podemos hallar pronunciamientos recientes que siguen utilizando esa categoría de referencia: así, en la STJUE (Gran Sala) de 21 diciembre 2023, asuntos acumulados C-38/21, C-47/21 y C-232/21, ECLI:EU:C:2023:1014, acerca de la actuación de un concesionario de vehículos y de si ésta debía considerarse por cuenta de la marca del vehículo, el Auto TJUE de 5 de octubre de 2023 (Sala octava), asunto contra Roller GmbH & Co. KG, C-761/22, ECLI:EU:C:2023:756, acerca de la fácil identificación de la eficiencia energética de una electrodoméstico en función de la información de etiquetado facilitada o la de 12 de enero de 2023 (Sala Segunda), asunto DV contra MA, C-395/2, ECLI:ECLI:EU:C:2023:14 y la STJUE de 13 julio 2023 (Sala Novena), asunto C-265/22, ECLI:EU:C:2023:578, ambas sobre control de cláusulas abusivas.

[8] Así la STJUE (Sala Cuarta) de 2 de mayo de 2019, Asunto C-614/17, ECLI:EU:C:2019:344, en la que se cuestiona si el consumidor medio debe referirse a un consumidor europeo o puede referirse únicamente al consumidor del Estado miembro en el que se plantea el litigio de origen.

[9] L. González Vaqué, *La noción de consumidor medio según la jurisprudencia del Tribunal de Justicia de las Comunidades europeas*, en *Revista de Derecho Comunitario Europeo,* 2004, núm. 17, 63 y ss.

informativos precontractuales[10], siendo su utilidad relativa dada la ausencia de regulación acerca de las sanciones civiles derivadas de su infracción[11].

El consumidor vulnerable se carácteriza como un subtipo de consumidor[12] restringido a las personas físicas -recordemos que la legislación española admite a determinadas personas jurídicas dentro de la categoría general de consumidor-, que tampoco pueda extenderse a otras categorías como los profesionales autónomos o las microempresas y lo que le distingue abstractamente es la situación de desigualdad que padece a la hora de contratar debido a su particular situación o circunstancia/s. Esa desigualdad frente al mercado en relación con los consumidores que no se hallen en la misma situación o circunstancia/s puede afectar a su aptitud para comprender la información o bien, a su capacidad de negociación. En todo caso, si la digitalización es un factor debilitante en general, dicha debilidad no puede enfrentarse desde la perspectiva individual de la fragilidad de un consumidor en una concreta relación de consumo. Esta perspectiva individual solo será relevante en supuestos de combinación de factores (entorno digital sumado a otro factor de vulnerabilidad).

2.1. La persistente necesidad de una tuición abstracta general.

La protección de los consumidores avanza hacia una tuición situacional que acoge factores heterogéneos de eventual fragilidad en la toma de decisiones o en los medios de defensa frente a las pretensiones de la otra parte. Sin embargo, parece claro que la posición consumidora abstracta conlleva, en todo caso, una caracterización asociada e inherente de debilidad contractual y que, pese a las inevitables limitaciones del sujeto de referencia -el consumidor medio-, dicha estandarización tuitiva que da lugar a una protección generalizada, sigue resultando necesaria. Lo es, sobre todo, porque la contemplación de la especial vulnerabilidad del consumidor, salvo la prevista por leyes sectoriales, no ha trascendido, como se ha dicho, a medidas o remedios en fase de ejecución del contrato y así, por ejemplo, no hay ninguna

[10] El Real Decreto-ley 1/2021, de 19 de enero, de protección de los consumidores y usuarios frente a situaciones de vulnerabilidad social y económica (BOE-A-2021-793), posteriormente tramitado como Ley 4/2022, de 25 de enero (BOE-A-2022-3198), además de introducir la definición de consumidor vulnerable en el art. 3 de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, reformó el art. 8 recogiendo como derecho básico de los consumidores y usuarios el de la protección de sus derechos mediante procedimientos eficaces, en especial relación con las personas consumidoras vulnerables (letra f), el art. 17.3 en materia de información, formación y educación de los consumidores y usuarios, el art. 18.1 y 2 en materia de etiquetado y presentación de bienes y servicios, el art. 19 sobre prácticas comerciales, el art. 20.2 y 3 acerca del contenido de las ofertas comerciales, el art. 43.c) sobre cooperación en materia de control de calidad y el art. 60.1 sobre información precontractual. Existe únicamente una previsión que atañe a la fase de ejecución del contrato, la contenida en el art. 72 por el que parece flexibilizarse la carga probatoria del ejercicio de un derecho de desistimiento en casos de que sean personas consumidoras vulnerables las que lo ejerciten.

[11] Es por ello que la doctrina concluye que no existe tal estatuto en la actualidad, M.P. Palazón Garrido, *op.cit.*, 212 y ss., o que solo al margen de las relaciones contractuales se pueden aplicar medidas para proteger al consumidor vulnerable, L. Diéguez Aguilera, *El consumidor vulnerable: en especial, la vulnerabilidad de las personas mayores ante la acusada digitalización del mercado financiero*, en *Diario La Ley,* 2023, núm. 10223, 5 ss.

[12] M.J. Marín López, *El concepto de consumidor vulnerable en el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios*, en *Revista CESCO*, 2021, núm. 37, 115 ss.

previsión respecto de la misma en sede de control la abusividad de las condiciones generales o de conformidad con el contrato. Pero también lo es porque la especial vulnerabilidad de un concreto consumidor no siempre resultará oponible, mientras siempre lo es la asociada a la posición consumidora.

Así, por ejemplo, es clara la distinción entre el régimen de la conformidad del bien con el contrato aplicable a la contratación de consumo y la aplicable en los contratos concluidos entre particulares, pese a la tendencia a la consumerización general del derecho privado, pero no podríamos establecer una diferencia de régimen jurídico entre el régimen de la conformidad aplicable a un consumidor medio y la aplicable a un consumidor especialmente vulnerable. Como señalaremos un poco más adelante, es el derecho privado general y no el derecho de consumo, el que dispone actualmente de normas que pueden servir a esa protección reforzada mediante figuras como la ventaja injusta o la influencia indebida.

En todo caso, el concepto de consumidor, entendido como supraconcepto que delimita dogmáticamente la categoría de las relaciones de consumo[13], solo parece que pueda ir referido a la noción general de consumidor, sin perjuicio de que la aplicación de los estándares reequilibradores de la respectiva posición contractual deba acomodarse o intensificarse en los casos de especial vulnerabilidad o que deban preverse estándares particulares para determinadas situaciones (por ejemplo, la vulnerabilidad económica).

2.2. La vulnerabilidad coyuntural y transitoria.

Uno de los aspectos que se ha planteado en la revisión de la protección que el derecho de consumo debe dispensar a los ciudadanos es la necesidad de contemplar un tipo de vulnerabilidad esencialmente episódico o coyuntural, por definición transitorio y no estructural o vinculado a situaciones endógenas. Es decir, una vulnerabilidad efímera y circunstancial[14] que, sin embargo, condicione decisivamente la capacidad negociadora de un sujeto en relación con una contratación en concreto.

En otros casos, la concreta situación de vulnerabilidad no afectará a la capacidad o habilidad en la negociación del contrato ni a su aptitud para comprender la información facilitada, sino directamente a las circunstancias económicas en la que se halle el consumidor, a su falta de solvencia, que le

[13] C.E. Florensa Tomás, *La delimitación del concepto de consumidor en la reciente jurisprudencia del TJUE*, en AA.VV., *Codificación y reequilibrio de la asimetría negocial,* coord. por M.D. Gramunt Fombuena y C.E. Florensa Tomás, Madrid, 2017, 65 ss., se refiere a él como protoconcepto puesto que la categorización subjetiva de la parte contractual funciona como exigencia dogmática, tanto para calificar la relación jurídica como relación de consumo, como para la aplicación de los estándares reequilibradores de la relación.

[14] E. Lauroba Lacasa, *Consommateur vulnérable et consommateur âgé*, en AA.VV., *Mélanges en l'honneur d'Yves Picod. La loyauté en droit économique*, Paris, 2023, 95, se refiere a la creciente porosidad de las calificaciones categóricas que da lugar a la contemplación de la mencionada vulnerabilidad efímera sin que, en realidad, ello derive necesariamente en la inutilidad de las taxonomías globales, pues éstas tienen la ventaja de identificar inmediatamente las categorías.

impida hacer frente al pago de, por ejemplo, suministros básicos y en ese contexto, hallaremos, además, supuestos de vulnerabilidad severa[15].

La particularidad de la aproximación actual es que la vulnerabilidad no se contempla como una situación permanente asociada a un determinado estado o circunstancia (edad, discapacidad, etc.), sino que puede responder a una realidad puramente coyuntural o puntual del individuo. A su vez, y esa es la mayor dificultad a la que se enfrenta la nueva categorización, se relaciona no solamente con un grupo de consumidores, sino también con la vulnerabildad estrictamente individual. En efecto, mientras la Directiva 2005/29/CE aludía a "un grupo claramente identificable de consumidores vulnerables" (art. 5.3), la Nueva Agenda del Consumidor[16] atiende a una vulnerabilidad que puede estar causada "por circunstancias sociales o características particulares de consumidores individuales o de grupos de consumidores".

Dicha individualización de la vulnerabilidad del consumidor nos llevará a valorar la transcendencia de la misma durante la contratación del bien o servicio y su correlativa oponibilidad a quien haya predispuesto dicha contratación.

Desde esta perspectiva, se distingue entre la vulnerabilidad "class-based", relacionada con características individuales del consumidor (edad, sexo, discapacidad, etc.) y la vulnerabilidad "state-based", que se identifica con el modo como la persona interacciona con el mercado en función de sus características individuales y sus circunstancias personales y por tanto, tiene un incidencia transitoria[17]. La manera como la persona interacciona en el mercado digital y como se dan unas condiciones especialmente propicias para influir en su toma de decisiones sería un ejemplo claro de vulnerabilidad "state- based".

2.3. La vulnerabilidad multifactorial.

A la hora de identificar una concreta situación de debilidad contractual que potencialmente pueda ocasionar una asimetría en el resultado del contrato, pueden tenerse en cuenta indicadores que responden a causas endógenas

[15] Observamos el recurso a definiciones de consumidor vulnerable destinadas exclusivamente a la protección sectorial del mismo. Así, el Real Decreto 897/2017, de 6 de octubre, por el que se regula la figura del consumidor vulnerable, el bono social y otras medidas de protección para los consumidores domésticos de energía eléctrica (BOE-A-2017-11505), precisa una definición, que se contiene en su art. 3, basada en condicionantes de renta anual, a los efectos de bonificar el precio del suministro de energía eléctrica y garantizar la continuidad del suministro. Respecto del ámbito subjetivo de aplicación de la norma, se distingue entre el consumidor vulnerable y el consumidor vulnerable severo, que presenta riesgo de exclusión social (art. 4). También en sede de suspensión de lanzamientos en procedimientos de ejecución hipotecaria se recoge la descripción *ad hoc* de la especial vulnerabilidad que permite aplicar la medida (art. 1 de la Ley 1/2013, de 14 de mayo, de medidas para reforzar la protección a los deudores hipotecarios, reestructuración de deuda y alquiler social (BOE-A-2013-5073). En cambio, otras normas sectoriales, como el art. 14 de la Ley 12/2023, de 24 de mayo, por el derecho a la vivienda (BOE-A-2023-12203) incluyen relaciones de colectivos vulnerables meramente ejemplificativas.

[16] "Nueva Agenda del Consumidor. Reforzar la resiliencia del consumidor para una recuperación sostenible", COM (2020) 696 final,

[17] R. Barceló Compte, *El consumidor especialmente vulnerable. De la protección class-based a la protección state-based*, en *Actualidad Jurídica Iberoamericana,* 2022, núm. 16, 639.

como la edad, la discapacidad[18] o el nivel de formación[19] o exógenas como la situación económica/financiera[20] o geográfica[21]. El carácter multifactorial o multidimensional y a su vez, sectorial[22], de esta nueva mirada sobre la debilidad contractual dificulta su identificación precisa[23] y por tanto, su aplicación reequilibradora, sobre todo cuando la fragilidad se vincula a interacciones individuales con el mercado y no por razón de determinadas características del consumidor.

La atención a la especial vulnerabilidad del consumidor no es nueva. Así, la Directiva 2005/29/CE tipificó como prácticas comerciales desleales (art. 5.3) aquellas susceptibles de distorsionar el comportamiento económico de "un grupo claramente identificable de consumidores especialmente vulnerables a dichas prácticas o al producto al que se refieran, por padecer (…) una dolencia física o un trastorno mental o por su edad o su credulidad", debiendo tomar por referencia la perspectiva del miembro medio de ese grupo. Previamente, la Directiva 2001/95/CE, relativa a la seguridad general de los productos, actualmente derogada por el Reglamento (UE) 2023/988, de 10 de mayo (DOUE-L-2023-80684), ya se refería a determinados colectivos vulnerables, como los menores de edad o las personas mayores, extendiéndose la previsión, en la norma actual, a las personas con discapacidad.

En el caso de España se acuña una previsión de pretendida aplicación general[24] mediante el Real Decreto Ley 1/2021, de 19 de enero, de protección

---

[18] Así el Reglamento (CE) núm. 1107/2006, de 5 de julio, sobre los derechos de las personas con discapacidad o movilidad reducida en el transporte aéreo (DOUE-L-2006-81414).

[19] La Exposición de motivos de la Ley 4/2022, de 25 de febrero, de protección de los consumidores y usuarios frente a situaciones de vulnerabilidad social y económica (BOE-A-2022-3198), se refiere a la incidencia del nivel formativo y cultural del consumidor en las relaciones de consumo y que sitúa en posiciones de vulnerabilidad a aquellas personas que cuentan con menores niveles de estudios, refiriéndose la ley a las circunstancias educativas en el art. 3 al contemplar la consideración de personas consumidoras vulnerables respecto relaciones concretas de consumo.

[20] La transposición de la Directiva (UE) 2021/2067, de 24 de noviembre (DOUE-L-2021-81714) ha de incorporar la previsión de dicha vulnerabilidad y de las medidas en las que se concreta la específica protección, por ejemplo, mediante la obligación de renegociar de la deuda garantizada con la vivienda habitual. Respecto a este tipo de vulnerabilidad, deberán tenerse en cuenta, también, los supuestos en los que proceda la suspensión del lanzamiento ordenado con ocasión de ejecución hipotecaria, prorrogada la medida de suspensión hasta 15 de mayo de 2028 tras la aprobación del Real Decreto-ley 1/2024, de 14 de mayo, por el que se prorrogan las medidas de suspensión de lanzamientos sobre la vivienda habitual para la protección de los colectivos vulnerables.

[21] Se refiere a ello M.L. Palazón Garrido, *op.cit.*, 202 ss.

[22] En el año 2016 un estudio publicado por la UE "Consumer vulnerability across key markets in the European Union" analizaba la vulnerabilidad a partir de abstraer cinco dimensiones de la misma (1ª.- Mayor riesgo de resultados negativos o impactos en el bienestar, 2ª.- Tener características que limitan la capacidad de maximizar el bienestar, 3ª.- Tener dificultad para obtener o asimilar información, 4ª.- Incapacidad o imposibilidad de comprar, elegir o acceder a productos adecuados y 5ª.- Mayor susceptibilidad a las prácticas de marketing, creando desequilibrios en el mercado) en tres sectores distintos: el financiero, el energético y el de la contratación online, señalando que en los dos primeros la incidencia de la vulnerabilidad es notablemente mayor que en el tercero.

[23] S. Pagliantini, *op.cit.,* p. 2 o E. Kaprou, en AA.VV.,*The legal definition of vulnerable consumers in the UCPD: Benefits and limitations of a focus on personal*, Riefa, Christine Riefa y Saintier, Severine (ed.), *Vulnerable consumers and the law*, Routledge, Oxon, 2020, 54.

[24] Las previsiones que hallamos anteriormente se encuentran en normas sectoriales y se relacionan, sobre todo, con la situación económica del consumidor. La doctrina ha sistematizado en dos grupos la normativa que se ocupa de paliar los problemas relacionados con la vulnerabilidad distinguiendo dos dimensiones: la económica y la informativa y ha concluido que ambas dimensiones suelen concurrir en las mismas personas. A. Mut Piña, *La parametrización de la vulnerabilidad en el derecho contactual de consumo. Un estudio empírico sobre el sector financiero*, en *InDret,* 2023, núm. 1, 4 ss. El art. 3.3. del Texto refundido pretende superar, pues, el criterio económico como el único definitorio de una situación de vulnerabilidad. I. Navarro

de los consumidores y usuarios frente a situaciones de vulnerabilidad social y económica (BOE-A-2021-793)[25], que modificó la norma destinada a la definición de consumidor, añadiendo un segundo párrafo destinado a contemplar la categoría de persona consumidora vulnerable (art. 3.2 de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias): «sin perjuicio de la normativa sectorial que en cada caso resulte de aplicación, tienen la consideración de personas consumidoras vulnerables respecto de relaciones concretas de consumo, aquellas personas físicas que, de forma individual o colectiva, por sus carácterísticas, necesidades o circunstancias personales, económicas, educativas o sociales, se encuentran, aunque sea territorial, sectorial o temporalmente, en una especial situación de subordinación, indefensión o desprotección que les impide el ejercicio de sus derechos como personas consumidoras en condiciones de igualdad».

Se ha criticado la inconcreción e imprecisión de la definición que, si bien introduce esa categoría de vulnerabilidad multifactorial, dificulta un tratamiento uniforme y reconocible de la figura[26]. Al margen de estas críticas justificadas, plantearemos a continuación si la digitalización del contexto y del objeto del contrato pueden dar lugar a una vulnerabilidad asociada.

3. La digitalización como factor de vulnerabilidad del consumidor.

Cabe plantear si la digitalización del mercado o incluso, la digitalización del objeto del contrato, acarrean un factor inherente y añadido de vulnerabilidad en la posición consumidora[27]. La respuesta parece ser necesariamente afirmativa. El funcionamiento del mercado en ese concreto contexto, a través de plataformas tecnológicas que controlan la información y se anticipan a la demanda, da lugar a prácticas de segmentación digital que convierten a cualquier consumidor en vulnerable[28] e intensifican la asimetría propia de las relaciones B2C, siendo difícil distinguir en ese contexto las técnicas de incentivación de las de manipulación[29]. Además, la innovación tecnológica

---

Mendizábal, en AA.V.V., *El consentimiento contractual informado de las personas mayores*", S. Adroher Biosca, (dir), *Tratado de derecho de mayores,* Madrid, 2024, 627.

[25] Posteriormente derogado al ser tramitado como ley (Ley 4/2022, de 25 de febrero, BOE-A-2022-3198).

[26] J.A. García Hernando, *La falta de concreción y determinación del concepto de consumidor vulnerable en el RDL 1/2021*, en *Diario La Ley*, 2021, nº9858, 2.

[27] R. Barceló Compte, *op.cit.,* 640. C. Argelich Comelles *Del consumidor vulnerable de la Ley 4/2022 y el Derecho europeo de consumo al "consumidor vulnerable digital" y su protección*, en AA.V.V., *Derecho y colectivos vulnerables,* J. Martín Ostos (dir.), Sevilla, 2022, 17) sostiene la necesidad de hacer evolucionar la categoría de consumidor medio hacia la categoría de consumidor vulnerable digital.

[28] Desde esta perspectiva se habla de la naturaleza arquitectónica de las vulnerabilidades en la sociedad digital, refiriéndose al despliegue de arquitecturas de elección en los mercados digitales que deben ser analizados desde los postulados de la economía conductual. A su vez, se constata que debe superarse el planteamiento de la Directiva sobre prácticas comerciales desleales que yuxtapone el consumidor vulnerable al no vulnerable, como si cada consumidor pudiese asignarse a una categoría u otra N.Helberg, H.W. Micklitz, M. Sax y J.Strycharz, *Digital vulnerability*, en *EU consumer protection 2.0 Structural asymmetries in digital consumer markets*, 2021, 18 y ss.

[29] La ley de servicios digitales (Reglamento (UE) 2022/2065, de 19 de octubre de 2022, DOUE-L-2022-81573), aplicable desde el pasado 17 de febrero de 2024, introdujo, en su art. 25, la prohibición de utilizar los llamados patrones oscuros a través del diseño, organización o gestión de interfaces «que engañen o manipulen a los destinatarios del servicio o de manera que distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas.».

complica la labor legislativa dada la rápida evolución de aquella frente a la lentitud de reacción de esta[30]. Por otro lado, es fácil anticipar que quien se halle en un estado de vulnerabilidad por razón de edad, discapacidad, situación económica, etc., agravará su fragilidad en un contexto digital; todavía más si asociamos un mercado complejo -como el financiero- y lo desarrollamos en un entorno digital. Sin embargo, el planteamiento del legislador europeo no se sitúa, de momento, en esa perspectiva generalizadora de una vulnerabilidad asociada al contexto digital[31].

3.1. De la brecha digital al estado de *flow*: la digitalización del contexto contractual y el objeto del contrato como factores asociados de vulnerabilidad.

El comercio electrónico en España muestra un crecimiento sostenido en la última década. Según pone de relieve el último informe sobre comercio electrónico elaborado con datos de 2022 por el Observatorio Nacional de Tecnología y Sociedad (ONTSI), el 30% de empresas realiza ventas online y el crecimiento desde 2019 se cifra 9,6% para las empresas con más de diez trabajadores. En cuanto a las microempresas se cifra en un 13,2 % el porcentaje de tráfico online y en un 7,4 % el incremento respecto a los datos de 2019.

La relación entre el impacto de la tecnología y la asimetría contractual se ha vinculado, sobre todo, con la llamada brecha digital[32] y a la falta de capacitación digital[33]. La Resolución del Parlamento Europeo, de 13 de diciembre de 2022[34], sobre la brecha digital: diferencias sociales como consecuencia de la digitalización [2022/2810(RSP)][35], tomando la definición de brecha digital acuñada por la Organización de cooperación y desarrollo económicos (OCDE) y

[30] A.B. Veiga Copo, *El consumidor vulnerable,* Navarra, 2021, 339 ss.

[31] Así, la Directiva (UE) 2019/2161 (DOUE-L-2019-81968) que modificó, entre otras, las Directivas 2005/29/CE y 2011/83/UE, señaló la necesidad de adaptar la legislación de la Unión en materia de protección de los consumidores ante el continuo desarrollo de las herramientas digitales (considerando 17) pero siguió asociando la especial vulnerabilidad a una situación subjetiva previa, como la edad avanzada (considerando 54).

[32] Los estudios sociológicos han identificado tres niveles asociados a la brecha digital y que afectan al acceso (distinguiendo entre quienes tienen acceso a internet y quienes no lo tienen), al uso y habilidades de los usuarios (en el que influyen factores como y a los beneficios vinculados a las formas de consumo en entornos digitales (C. Lutz, *Digital inequalities in the age of artificial intelligence and big data*, en *Human Behavior and Emerging Technologies*, 2019, Vol 1, issue 2, apr, 142 ss.) Dichos estudios realizados mediante análisis empíricos ponen de relieve que, pese que la contratación electrónica ha podido favorecer cierta homogeneización de los hábitos adquisitivos de los consumidores españoles respecto a los mantenidos en las economías occidentales más avanzadas, el consumo online da lugar a una nueva forma de fragmentación social en el consumo (M. Barbeta-Viñas y A. Sánchez-Gelabert, *Consumo online y desigualdad en España ¿la emergencia de nuevas formas de fragmentación*, en *Revista española de investigaciones sociológicas*, 2023, núm. 184, octubre-diciembre, 24 ss.; también S.De Marco, *El comercio electrónico en España (2029): un ejemplo de tercera brecha digital*, en *Revista internacional de sociología*, 2022, vol. 80 (2), abril-junio, 4)

[33] M.D. Hernández Díaz-Ambrona, *Consumidor y comerciante*,), en AA.V.V., *Manual de Derecho de consumo*, en Díaz Alabart, Silvia (coord.) 2a ed., Madrid, 2023, 41 ss.

[34] Con anterioridad ya se refería a ella la Resolución del Parlamento Europeo, de 27 de noviembre de 2014, sobre el apoyo a los derechos de los consumidores en el mercado único digital [2014/2973(RSP)], C 289/65, 09.09.2016. También se ha ocupado de la cuestión en un contexto más general, la Decisión (UE) 2022/2481 por la que se establece el programa estratégico de la Década Digital para 2030 [PE/50/2022/REV/1, L323/4, 19.12.2022].

[35] (OJ C, C/177, 17.05.2023, p. 57, CELEX: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022IP0438)

que alude a la distancia existente entre «particulares, hogares, empresas y zonas geográficas en distintos niveles socioeconómicos, tanto en lo que se refiere a sus oportunidades de acceso a las tecnologías de la información y la comunicación (TIC) como a su uso de internet para una amplia gama de actividades», parte de la constatación de que la digitalización tienen una gran repercusión social, económica, política y cultural en la vida cotidiana de los consumidores, generando desigualdades no solo entre zonas urbanas bien conectadas y zonas rurales remotas con niveles bajos de conectividad, sino también «entre las personas que pueden beneficiarse plenamente de un espacio digital enriquecido, accesible y seguro con una amplia gama de servicios, y las que no pueden hacerlo», siendo «que el uso cada vez más extendido de pagos digitales, incluidas tarjetas, carteras digitales o aplicaciones móviles, está dando lugar a que algunos minoristas dejen de aceptar efectivo». Se destaca, asimismo, la necesidad de reforzar la protección de los datos personales y la privacidad de los consumidores, especialmente cuando no están familiarizados con la seguridad de los datos en línea o en relación con interfaces de software que no resulten fáciles de usar.

En cuanto a la brecha digital de género cabe concluir que no tiene impacto en la caracterización de la vulnerabilidad de las personas consumidoras cuando contratan. La brecha se concentra en el dato relativo al número de especialistas digitales y en el número de mujeres que eligen una formación superior en el campo de la informática, pero no afecta al uso regular de internet ni al nivel de competencias digitales, aunque sí se detecta una mayor desconfianza de las mujeres ante lo ciberriesgos[36]. Por el contrario, la brecha digital asociada a las personas de edad avanzada o brecha digital generacional es un dato contrastado[37], que además afecta a la brecha de primer nivel, la del acceso, lo que ya no permite considerar el nivel de capacitación digital, y puede dar lugar a situaciones de exclusión social. Esa deriva ha sido puesta de manifiesto por la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01), de 23 de enero de 2023 que incluye el compromiso de

[36] Ello según los datos del último Informe sobre Brecha digital de género 2023 (Edición 2024 con datos de 2023), publicado por el Observatorio Nacional de Tecnología y Sociedad (ONTSI), dependiente del Ministerio para la transformación digital y de la función pública del Gobierno de España: el 94,6% de las mujeres usan Internet semanalmente frente al 94,3% de los hombres, siendo el sexto país europeo con mayor porcentaje de utilización; el 65,9 % de las mujeres de España tiene un nivel de competencias digitales básicas o por encima de las básicas frente al 66,5% de los hombres; solo el 14,% de las personas egresadas en informática y el 28,3% en ingenierías son mujeres, siendo que las mujeres representan el 18% del total de los especialistas digitales de España. En cuanto al nivel de confianza, el 40,7 % de las mujeres confía poco o nada en Internet frente al 37,7% de los hombres, mientras que el 25,7% de las mujeres se siente preparada para afrontar los problemas derivados de la ciberseguridad ante el 38,7% de los hombres. Respecto al uso concreto de dispositivos para acceder a internet, aspecto que se considerará relevante respecto al estado de flujo mencionado en el texto, la proporción entre hombres y mujeres no arroja diferencias significativas: teléfono móvil (95,6 % mujeres y 95,1 % hombres), ordenador portátil (53,9 % mujeres y 52,5 % hombres), ordenador de sobremesa (25,9 % mujeres y 37,3 % hombres) y tableta (35% mujeres y 34,1 % hombres). Más concretamente, en relación con las actividades desarrolladas en los accesos a internet, se aprecia que las mujeres tienen una ligera dedicación superior a las actividades de contratación online de bienes (1,2% más que los hombres): el 55,2% de las mujeres compran bienes físicos, frente al 54% de los hombres, mientras que los hombres contratan servicios en línea en mayor proporción (30% hombres frente a 23,4% mujeres).

[37] I. Navarro Mendizábal, *op.cit.,* p. 611 y ss. que señala que el uso intensivo de la tecnología sin alternativa genera una brecha digital. Si bien el autor considera que la edad no constituye en sí misma una causa de vulnerabilidad contractual, concluye que puede ser un factor coaduyante cuando concurre con otros factores.

«llevar a cabo una transformación digital que no deje a nadie atrás» y que beneficie «a todos», logrando «el equilibrio de género» e incluyendo, «en particular, a las personas de edad avanzada, las personas que viven en zonas rurales, las personas con discapacidad o marginadas, vulnerables o privadas de derechos, y quienes actúen en su nombre». La forma de lograrlo no es evidente y se señala que solo mediante políticas que permitan la constatación del acceso universal al entorno digital podrá promoverse la capacitación en ese entorno[38]. Desde una perspectiva más realista y centrada en la contratación online, se ha acudido a la categoría de hipervulnerabilidad para caracterizar al consumidor de edad avanzada en el contexto digital[39].

En este sentido, más allá de los indicadores habituales de vulnerabilidad del consumidor (edad, formación, situación económica, discapacidad, etc.) que se planean desde una vertiente subjetiva, se puede concebir una vulnerabilidad asociada al contexto contractual. Entendemos que el entorno digital o incluso, la digitalización del objeto del contrato, incorporan de manera inherente un factor de vulnerabilidad contractual añadido, puesto que la capacitación digital, superada la minoría de edad, no es plena en ninguna franja de edad[40].

Como se ha señalado, la debilidad contractual puede ser multifactorial y sin duda, que un determinado contexto contractual puede ser un factor relevante que la intensifique. Ello se positivizó ya hace ya años en relación con las prácticas comerciales desleales, cuya valoración depende del contexto fáctico y exige tener en cuenta todas las características, circunstancias y limitaciones del medio de comunicación a través del cual se vierte una determinada información (art. 7.1 Directiva 2005/29/CE, de 11 de mayo, relativa a las prácticas comerciales desleales). El contexto digital de contratación puede favorecer una asimetría reforzada [41], asociada a la dificultad de tomar decisiones informadas[42], que lo será aún más en los casos en los que concurra con otros factores de vulnerabilidad, como la edad o la falta de capacitación digital del consumidor[43].

A su vez, la doctrina plantea si existen diferencias de comportamiento en el consumidor en función del dispositivo electrónico empleado para la contratación, refiriéndose al estado de *flow* del usuario que accede a una

---

[38] V. Morente Parra, *Los derechos digitales de las personas mayores. Hacia el fin de la brecha digital generacional*, AA.VV., *Tratado de derecho de mayores*, S. Adroher Biosca (dir.), Madrid, 2024, 667ss.

[39] S. De Salas Murillo, *Hipervulnerabilidad del consumidor mayor en la contratación electrónica*, en AA.VV., *Tratado de derecho de mayores*, S. Adroher Biosca (dir.), Madrid, 2024, 201.

[40] En el apartado 14 de la Resolución se señala que «los factores sociodemográficos influyen significativamente en los niveles de capacidades digitales, ya que, por ejemplo, más de dos tercios de los adultos jóvenes, las personas con altos niveles de educación formal y los estudiantes de educación superior cuentan al menos con capacidades digitales básicas; observa, en cambio, que solo alrededor de un tercio de las personas de entre 55 y 74 años, las personas jubiladas y las personas inactivas tienen al menos capacidades digitales básicas; observa, además, que la brecha entre las capacidades digitales de las personas que viven en zonas rurales y urbanas sigue siendo considerable».

[41] R. Barceló Compte, *op.cit.,* 632.

[42] Según se señala en la "Nueva Agenda del Consumidor. Reforzar la resiliencia del consumidor para una recuperación sostenible", COM (2020) 696 final, p. 11 y ss.

[43] La Comunicación UE sobre la "Nueva Agenda del Consumidor. Reforzar la resiliencia del consumidor para una recuperación sostenible", COM (2020) 696 final, p. 18, remite al Informe BIT (E. Costa y D.Halpern, *The behavioural science of online harm and manipulation, and what to do about it. An exploratory paper to spark ideas and debate*, 2019) sobre los daños y la manipulación en línea, en él se proponen medidas para identificar consumidores vulnerables y poder proveer medidas de apoyo que principalmente se relacionan con una mayor accesibilidad de los datos en beneficio de los consumidores y no de las empresas.

página web de venta y se concluye que, en efecto, la contratación online promueve el hedonismo asociado a la contratación, en detrimento de la toma de decisiones reflexivas o racionales; se dice que ese estado de *flow¸* definido como el estado mental que se alcanza cuando una persona está totalmente involucrada en la actividad que realiza debido al goce que dicha actividad le reporta, encuentra un entorno de desarrollo especialmente propicio en el comercio online[44]. Se ha estudiado, también, el impacto de la digitilalización de la publicidad sobre la actitud del consumidor, determinando que los efectos digitales mejoran la respuesta al incentivo publicitario y por tanto, cumplen un rol moderador sobre el comportamiento del consumidor[45].

Como hemos señalado, con carácter general, el entorno digital de contratación favorece una situación general de vulnerabilidad -del mismo modo que se relacionó la venta fuera de establecimiento con una forma agresiva de ofertar bienes o servicios que podía dar lugar a contrataciones viciadas o que en la actualidad se vincula el sector energético o el financiero a una especial fragilización del consumidor-, puesto que dicho entorno está diseñado para identificar y promover la debilidad del consumidor[46]. Ello puede haber justificado pronunciamientos como el contenido en la STJUE (Sala Sexta) de 10 de diciembre de 2020 (Asunto C-774/1), en el que se califica de consumidor, a los efectos de determinar la competencia judicial internacional, al usuario de una plataforma de apuestas que se dedica a tiempo completo a las apuestas online, siendo estas su medio de vida y contando con amplios conocimientos sobre la actividad desempeñada[47].

Finalmente, debe valorarse también si la digitalización del objeto del contrato conlleva un factor de vulnerabilidad contractual que precise ser reequilibrado. El legislador europeo no ha parecido considerarlo desde esa perspectiva y así, en términos generales, la Directiva (UE) 2019/770, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales (DCD) dispensa una protección menor al contratante de contenidos y servicios digitales respecto del que extiende al comprador de bienes (con elementos digitales y sin ellos[48]) en la Directiva (UE) 2019/771

---

[44] A. V. Ruiz Vega y C. Riaño Gil, *El estado de flow y el comercio electrónico: ¿Existen diferencias en la conducta de los consumidores según el dispositivo electrónico utilizado?*, en AA.VV., *El derecho privado en el nuevo paradigma digital,* E. Arroyo Amayuelas y S. Cámara Lapuente (dirs.), Madrid, 2020, 297 ss.

[45] M. García Torres, *Influencia de los efectos digitales en la actitud del consumidor hacia el anuncio y la marca*, en *Revista Mediterránea de Comunicación,* 2024, vol. 15, núm. 1, 280 ss.

[46] R. Barceló Compte, *op.cit.,* 640.

[47] M. V. Cuartero Rubio, ¿*Puede ser el consumidor un profesional (del póker on-line)? A propósito del asunto Personal Exchange International, C-774/19*, en *Centro de estudios jurídicos,* enero 2021. A este caso se refiere también R. Evangelio Llorca, *El concepto de consumidor en el acervo comunitario a la luz de la jurisprudencia del TJUE*, en *Actualidad Jurídica Iberoamericana*, 2024, núm. 20, febrero, 904, como ejemplo de relajación en la aplicación de los requisitos que debe cumplir la condición de consumidor. De hecho, ya anteriormente el TJUE ha desvinculado el nivel de conocimientos o la elevada competencia técnica con la inclusión/exclusión de la normativa de protección al consumidor; así, en la STJUE (Sala cuarta) de 3 de septiembre de 2015, Asunto C-110/14 (Caso Ovidiu Costea Horace contra SC Volksbank Rumanía SA), puesto que la debilidad de la posición consumidora no se relaciona únicamente con la comprensión de la información suministrada, sino con la limitación del poder de negociación del contrato.

[48] L. Arnau Raventós, *Bienes y elementos digitales: ¿dos mundos aparte?*, en *Revista de educación y derecho*, 2021, núm. 24 *(Relaciones contractuales en la era Digital),* 26 ss, se refiere al distinto tratamiento dispensado y señala que el consumidor que contrata el suministro de elementos digitales formando parte estos de un contrato de compraventa de un bien recibe un trato tendencialmente mejor al consumidor que contrata elementos digitales autónomamente.

(DCV). A su vez, la DCD no toma en consideración la eventualidad de esa vulnerabilidad, ni en su articulado ni en los considerandos previos[49].

3.2. En particular, la digitalización en el sector financiero y la fragilización resultante.

Un ámbito en el que ha resultado evidente la relación entre la digitalización del canal de contratación y de ejecución del contrato y la debilidad reforzada de la posición consumidora es el sector financiero, especialmente en relación a determinados grupos de consumidores. Dicha debilidad se ha relacionado, principalmente, con la edad avanzada. Un segundo aspecto en el que la digitalización tiene un impacto potencialmente debilitante es el del scoring crediticio mediante la utilización de la IA.

En cuanto a la primera cuestión, y pese a los estudios que pretenden desligar la vejez de un estado de vulnerabilidad inherente[50], los datos estadísticos[51] y las previsiones normativas ponen de relieve que es un factor de potencial limitación funcional de acceso al servicio (considerando 4 de la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios (DOUE-L-2019-80999) que menciona como servicio específico con requisitos adicionales de accesibilidad, el bancario). La banca digitalizada, como modelo de gestión de negocio, se ha impuesto de forma abrupta, sin una adecuada implantación progresiva, y pese a que puede haber supuesto un elemento de inclusión financiera de las personas que no tenían acceso físico a las entidades por su localización geográfica, ha expulsado del sistema a un elevado porcentaje del colectivo integrado por las personas mayores[52]. No sirve apuntar ahora, tras la transformación operada, que debe promoverse la inclusión digital de quienes no están capacitados para ello mediante acciones formativas. Seguramente, el único modo de revertir la exclusión financiera de sectores de población para los que la formación no sea una respuesta realista, es garantizar puntos de acceso presencial aunque sea mediante oficinas móviles o agentes financieros que se desplacen puntualmente[53] y, en un futuro, lograr que la capacitación digital

[49] R. Barceló Compte, *op.cit.,* 633 ss.

[50] Precisamente, lo que la digitalización de sectores como el bancario ha propiciado ha sido la movilización en defensa de la dignidad de las personas que, pese a su edad, no tienen habilidades digitales y que por ello no deben ser tratadas como ignorantes o discapacidad, pero tampoco excluidas. I. Navarro Mendizábal, *op.cit.*, 611 ss.

[51] Según los datos relativos al porcentaje de usuarios de la banca online referidos a 2020, y por tanto, post covid, facilitados por la Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares (INE), se estima que en la franja entre 55 y 64 años, la utilización es del 54,1% mientras que en la franja entre 65 y 74 años desciende al 32,6%; por encima de 75 años, solo un 9,1% utiliza los servicios de banca digital.

[52] A.I. Blanco García, *Brecha digital y vulnerabilidad del consumidor financiero. El refuerzo de su protección*, en AA.VV., *Los vulnerables ante el proceso civil*, J.F. Herero Perezagua y J. López Sánchez (dirs.), Barcelona, 2022, 151 ss.

[53] Esa es la respuesta que resulta del Protocolo Estratégico para Reforzar el Compromiso Social y Sostenible de la Banca, suscrito el 23 de julio de 2021 por la Asociación Española de Banca (AEB), la Confederación Española de Cajas de Ahorro (CECA) y la Unión Española de Cooperativas de Crédito (Unacc), que, entre las medidas para la inclusión financiera, incluye la atención presencial en ventanilla en un horario amplio. Sin embargo, según las cifras que arroja el Informe del Banco de España "La accesibilidad presencial a los servicios bancarios en España: informe de seguimiento 2023 (documentos ocasionales núm. 2320) el uso de

mínima de la que dispondrá toda la población, permita el acceso y utilización de servicios que son esenciales[54].

En lo que respecta a la segunda cuestión, sobre la protección del consumidor frente a la toma de decisiones relativas a la solvencia del consumidor y a su capacidad de hacer frente a obligaciones futuras a partir de sistemas automatizados que den lugar a un valor de probabilidad, el TJUE ha tenido ocasión de pronunciarse recientemente sobre la aplicación del art. 22 del Reglamento Reglamento (UE) 2016/679 (RGPD). Dicho precepto establece el derecho de las personas a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de datos, incluidas la elaboración de perfiles; el considerando 71 se refiere concretamente al análisis y predicción de aspectos relacionados con la situación económica o el comportamiento del interesado. El derecho se concreta en poder solicitar la intervención humana por parte del responsable del tratamiento de datos, en poder expresar el punto de vista por parte de quien ha sido objeto de la decisión y en poder impugnar esta. En el caso enjuiciado por el TJUE en Sentencia de 7 de diciembre de 2023 (Schufa Holding, asunto C-634/21, EU: C: 2023:957 y asuntos acumulados C-26/22 y C-64/22, EU: C: 2023:958), se planteó si la protección dispensada por el precepto debía extenderse también a la actividad desarrollada por terceras empresas que finalmente no son las que toman la decisión sobre la denegación de la financiación, sino las que realizan el tratamiento de datos y generan un valor de probabilidad a la entidad financiera, que es quien, finalmente, deniega la concesión del préstamo. Es decir, si la «decisión» a la que se refiere el precepto incluye la actividad de una empresa contratada por la entidad financiera para que proporcione a esta un valor de probabilidad a partir del cual acoger o no la petición de financiación. El tribunal opta por aplicar un concepto amplio de decisión (párrafos 46 a 49), estimando que la decisión de la entidad que deniega el préstamo «está basada de modo determinante en dicho valor» y, por tanto, el interesado se ve significativamente afectado por la actividad de tratamiento desarrollada; el art. 22.1 RGPC «debe interpretarse en el sentido de que la generación automatizada, por una agencia de información comercial, de un valor de probabilidad a partir de los datos personales relativos a una persona y acerca de la capacidad de esta para hecer frente a compromisos de pago en el futuro constituye una "decisión automatizada", en el sentido de la mencionada disposición, cuando de ese valor de probabilidad dependa de manera determinante que un tercero, al que se comunica dicho valor, establezca, ejecute o ponga fina a un relación contractual con esa persona» (párrafo 73)[55].

canales alternativos por parte de las personas mayores (> 65 años) predispuestos para mitigar la exclusión financiera es muy reducido, cifrándolo en menos del 1 % siendo que, a la vez, dicho colectivo utiliza escasamente la banca online (según el Informe "Heterogeneidad en el uso de los Medios de pago y la banca online: Un análisis a partir de la encuesta financiera de las familias (2002-2020). Documentos ocasionales núm. 2308, menos del 20% de los nacidos antes de 1944 lo hace).

[54] J. Hernández López, L. Pascual Hernández y A. Rodríguez González, *El desarrollo de la digitalización y la inclusión financiera. El futuro del dinero y la transformación digital del sector financiero*, en *ICE*, 2022, núm. 926, 133 ss.

[55] L. Cotino Hueso, *La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de Inteligencia artificial,* en *Diario LA LEY,* , 2024, núm. 80, 4, destaca la importancia del pronunciamiento dado el criterio general garantista que introduce en cuanto al tratamiento automatizado de datos y por el hecho de "poner el foco en le peso efectivo que tiene la valoración, perfil o sistema automatizado en la decisión final que se adopte, aunque formalmente sea humana o se adopte incluso por otro sujeto".

Ello es relevante, también, a los efectos de aplicar la previsión del art. 18.8 de la Directiva (UE) 2023/2225 (DOUE-L-2023-81526) y teniendo en cuenta que el Reglamento (RIA) incluye entre los sistemas de IA de alto riesgo (Anexo III, apartado 5, por remisión del art. 6.2) los "sistemas de IA destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su calificación crediticia". Los riesgos asociados al empleo de la IA en los procesos de scoring crediticio se relacionan con el derecho a la privacidad, la opacidad de los sistemas y datos empleados, la eventualidad de que los resultados sean erróneos o, finalmente, de que estén condicionados por factores discriminatorios que, debido a la opacidad mencionada, no trasciendan[56]. La transparencia del sistema y el acceso a los datos que han sido tenidos en cuenta, así como el valor de probabilidad alcanzado, son elementos necesarios para poder ejercer los derechos relativos a la expresión del punto de vista del prestatario y a solicitar una revisión de la toma de decisión.

4. Planteamiento tuitivo en casos de especial asimetría contractual.

La atención a la especial vulnerabilidad del consumidor, descrito por la norma considerando múltiples factores, no ha dado pie a una protección correlativa, salvo la consistente en reforzar las obligaciones informativas previas de la parte profesional. Teniendo en cuenta que el punto de partida es que el consumidor vulnerable puede tener dificultades adicionales, aunque sea por razones meramente transitorias, para comprender la información facilitada, parecería que lo que se exige al profesional es que predisponga una información distinta, más comprensible, de mayor calidad, para un determinado consumidor que contrate con él. Sin embargo, sobredimensionar una vez más la carga informativa del profesional, ni siquiera perfilando más afinadamente su contenido, no constituye un planteamiento realista ni una solución adecuada[57], especialmente en un contexto digital. Por un lado, porque la dificultad de personalizar la información e incluso antes que eso, de identificar la propia vulnerabilidad, llevaran a reforzar la información en todos los casos para su aplicación general -lo cual sería positivo salvo por la inevitable repercusión de los costes derivados de ello- y en segundo lugar, porque seguirán echándose en falta soluciones reequilibradoras aplicables a la fase de ejecución del contrato[58]. Llegados a este punto, parece que volver al derecho general de los contratos, en sus recientes manifestaciones tuitivas, puede ser un camino a explorar.

[56] N. COLLADO-RODRÍGUEZ, *La evaluación de la solvencia mediante el uso de sistemas de IA,* en *Revista CESCO,* 2023, núm. 46, 48 ss.

[57] Acerca de la ineficiencia de la carga informativa como remedio tuitivo y a su persistencia como solución de compromiso que garantice el libre acceso de los consumidores a bienes y servicios, A. Mut Piña, *op.cit.*, p. 27.

[58] M.P. Palazón Garrido, *op.cit.* p. 221. En el mismo sentido, A. Mut Piña (*op.cit.,* p. 28), que señala la inseguridad jurídica asociada a la consideración de un consumidor como vulnerable si ello se parametriza mediante la aplicación de criterios no objetivos.

4.1. De la toma de decisiones con conocimiento de causa a la toma de decisiones óptimas.

En el tránsito hacia el empoderamiento de los consumidores, se introducen ciertas perspectivas cuya concreción, que debe ser compatible con los principios generales de la contratación y más particularmente, con la autonomía privada, puede resultar difícil. Así, al contemplar la caracterización de una oferta comercial dirigida a un consumidor especialmente vulnerable o la carga de información precontractual, el legislador (Exposición de motivos I del Real Decreto Ley 1/2021) establece que la información deberá facilitarse «en términos claros, comprensibles, veraces y en un formato fácilmente accesible, de forma que aseguren su adecuada comprensión y permitan la toma de decisiones óptimas para sus intereses» y para ello, la citada norma modifica los arts. 20 y 60.1 del Real Decreto Legislativo 1/2007.

El planteamiento es distinto al que en sede de prácticas comerciales desleales se relaciona con la toma de decisiones con el debido conocimiento de causa [59] y que lleva a la tipificación como prácticas engañosas de las que distorsionen de manera sustancial el comportamiento económico de los consumidores o que ejerzan una influencia indebida (Considerando 14, arts. 2.d y j, 7.1 Directiva 2005/29/CE).

En efecto, existe un salto evidente entre una toma consciente de decisiones y una toma de decisiones óptimas para el consumidor, puesto que para lograr un resultado económico óptimo podría pensarse que es necesario establecer una comparativa en la oferta del bien o servicio en el mercado y, por tanto, en relación con las ofertas de los competidores y que, además, el empresario ha tenido que desempeñar una labor individualizada de detección de las necesidades de cada consumidor en concreto. En realidad, la norma lo que exige es que pueda hacerse una abstracción de los términos utilizados por el profesional de modo que estos permitan una adopción racional de decisiones que no pueda juzgarse como contraria a sus intereses. Esa valoración, necesariamente, se proyectará sobre las condiciones económicas de la contratación concluida y permitirá revisar, si estas han perjudicado al consumidor, cuál fue y de qué manera se facilitó, la información precontractual (así, por ejemplo, si un consumidor realiza un cambio de comercializadora de electricidad, sector al cual, además, se asocia una particular complejidad, y empeora sus condiciones económicas respecto de las que gozaba antes del nuevo contrato, habrá que valorar sobre qué información el consumidor contrató con un resultado objetivamente desfavorable).

4.2. ¿Cómo se neutraliza o se reequilibra el déficit informativo?

El reequilibrio negocial frente a una asimetría en la posición negociadora de las partes contractuales y en concreto, en relación a la debilidad de una de ellas, ha sido objeto de regulación por el derecho privado general dando lugar a la

[59] Con dicha expresión se alude a una "formación meditada, tranquila, con la posibilidad real de considerar todas las implicaciones del negocio", L. Arnau Raventós, *Formación de la voluntad: riesgos de captación y "decisión con conocimiento de causa*", en AA.VV., *Nuevas orientaciones del derecho civil en Europa,* M. Pereña Vicente y P. Delgado Martín (dirs.), Madrid, 432 y ss.

ineficacia del contrato o a su adaptación (así, en caso de vicios de la voluntad o de ventaja injusta). Más deficiente es la respuesta legal ante los déficits informativos, puesto que no existe una previsión general sobre cómo debe protegerse a la parte desinformada cuando la información omitida o facilitada de forma inexacta o defectuosa ha resultado relevante en la eficacia del contrato[60].

Tampoco en relación con la categoría de consumidor vulnerable no se prevé un remedio concreto a la infracción informativa en relación con el contrato concluido, de modo que la apreciación de la especial vulnerabilidad por aplicación del art. 3.2 del Texto refundido de la Ley general para la defensa de los consumidores y usuarios no parece tener consecuencia alguna. En los casos en los que esa vulnerabilidad haya adquirido relevancia en el contexto del empleo de una práctica comercial desleal, la Directiva 2005/29/CE, de acuerdo con la modificación introducida por la Directiva (UE) 2019/2161, que añadió un art. 11.bis a la disposición, incluye la indemnización, la reducción del precio y la resolución del contrato como medidas correctoras para eliminar los efectos de la práctica utilizada, siendo la reducción del precio un medio particularmente idóneo para reequilibrar el contrato (siguiendo con el ejemplo planteado anteriormente relativo a la contratación de una servicio de suministro eléctrico en condiciones económicas peores que aquellas de las que se disfrutaba antes de la nueva contratación, si se concluye que en la comercialización del suministro se incurrió en deslealtad, la corrección del precio hasta situarlo en los márgenes que dicha comercialización sugería, resultaría un remedio pertinente). No obstante, el legislador español, al transponer la Directiva (UE) 2019/2161, decidió omitir la resolución del contrato y la reducción del precio como medidas correctoras, realizando una deficiente labor de incorporación del derecho europeo y dificultando el acceso a esas medidas siquiera por recurso a los remedios generales del derecho contractual[61].

Más allá de ello, la doctrina reclama que la protección del consumidor vulnerable se desplace de los deberes informativos, que se califican de sobredimensionados[62], a la fase de ejecución del contrato, lo que incluye la simplificación de los medios de reclamación [63] y ello pasa por acarrear consecuencias a la infracción de aquellos deberes adaptando el cumplimiento del contrato.

[60] X. Basozábal Arrue, *En torno a las obligaciones precontractuales de información*, en *Anuario de Derecho Civil,* 2009, tomo LXII, fasc. II, 702, realiza una propuesta en función de los diversos intereses protegidos y atendiendo a la mejor forma de protegerlos.

[61] F. De Elizalde Ibarbia, *La Directiva 2019\2161, de Modernización del Derecho de Consumo, por la que se conceden remedios individuales contra las prácticas comerciales desleales. ¿Un paso más hacia la estandarización del derecho privado de la Unión Europea?*, en *Revista de Derecho Civil,* 2021, vol. 8, núm. 4, 80 y ss.

[62] Y no especialmente idóneos para combatir la vulnerabilidad asociada al contexto digital, R. Barceló Compte, *op.cit.,* 633.

[63] Palazón Garrido, María Luisa, *op.cit.,* p.219.

5. ¿La situación de vulnerabilidad es siempre oponible a la otra parte contractual?

Uno de los aspectos negativos de un enfoque dinámico o *state-based* de la vulnerabilidad del consumidor radica en la excesiva discrecionalidad interpretativa que tal enfoque atribuye al juez cuando deba resolver sobre un litigio planteado en el que dicha vulnerabilidad pueda ser una variable decisiva[64].

La posición de debilidad contractual no parece que pueda oponerse en todo caso a la contraparte profesional. Los elementos que tradicionalmente han caracterizado la vulnerabilidad tomaban en consideración cualidades plenamente identificables por la parte profesional (la edad, la discapacidad, el género, etc.).

La Directiva 2011/83/UE, en su considerando 34, ya se refirió a los consumidores especialmente vulnerables y al deber del comerciante de tener en cuenta sus necesidades especiales, pero solo en la medida en que las circunstancias que dan lugar a esa vulnerabilidad que se manifieste "de una forma que el comerciante pueda razonablemente prever". Nos damos cuenta de que esa previsión o anticipación del comerciante es un elemento que necesario para que se le puedan trasladar las consecuencias negativas que la contratación haya acarreado al consumidor.

Si nos fijamos de nuevo en las normas de derecho general de los contratos orientadas al reequilibrio de asimetrías negociales, advertimos que dicha fragilidad solo puede hacerse valer se haya tipificado y en aquellos casos en los que la otra parte era conocedora de la misma o bien no podía excusablemente ignorarla[65]. El legislador español no ha previsto dicho aspecto a la hora de introducir el concepto de vulnerabilidad del consumidor en el Texto Refundido de la Ley general para la defensa de los consumidores y usuarios, pero sí lo ha hecho de manera puntual al referirse a dicha vulnerabilidad en otros contextos regulatorios y prestando especial atención a un factor concreto de vulnerabilidad, cual es la de la persona consumidora discapacitada. Así, el art. 15 del Proyecto de Ley de atención a la clientela (actualmente en trámite parlamentario), al establecer el acceso universal y no discriminatorio a tales servicios dispone que «para la correcta identificación y atención de la clientela, la empresa podrá solicitar la acreditación de la situación de discapacidad u otras circunstancias que generan una situación de vulnerabilidad para el ejercicio efectivo de los derechos recogidos en esta norma»[66]. Se ha señalado, además,

---

[64] E. Lauroba Lacasa, *op.cit.*, 95.

[65] En el contexto de las propuestas europeas de regulación del derecho de contratos, al abordar la institución de la explotación indebida (II.-7:207 DCFR) o el beneficio excesivo/ventaja injusta (4:109 PECL) se exige expresamente dicho conocimiento como presupuesto de la protección dispensada. Así, se establecen dos presupuestos: el primero, la particular situación de debilidad contractual por razón de las circunstancias concurrentes y/o del contexto negocial -dependencia de la otra parte, relación de confianza, dificultad económica u otra necesidad urgente, incapacidad de previsión, ignorancia, inexperiencia o falta de capacidad negociadora- y el segundo, el conocimiento efectivo o esperable (la ignorancia inexcusable) de la otra parte respecto de la situación de debilidad concurrente, en función de las circunstancias y del objeto del contrato.

[66] También en sede de protección de la vulnerabilidad en el acceso a la vivienda, el art. 10.2 de la Ley 29/1994, de 24 de noviembre, de arrendamientos urbanos, tras la modificación llevada a cabo por la Ley 12/2023, de 24 de mayo, por el derecho a la vivienda, establece que para obtener el beneficio previsto en la norma deberá acreditarse la situación de vulnerabilidad social y económica.

la eventual colisión de la obligación de facilitar información sobre una situación de debilidad contractual y el derecho a la intimidad de la persona.

En definitiva, la vulnerabilidad oponible tendrá que responder:

- o bien a una abstracción posible (vulnerabilidad que afecte a un segmento de la población por el hecho de reunir una condición determinada, como la edad en relación con el nivel de habilidades digitales al interactuar con una entidad financiera que excluye la atención presencial)
- o bien, tratarse de una vulnerabilidad conocida por la parte contractual profesional y que haya transcendido en el resultado económico del contrato dando lugar a unas condiciones económicas (más) perjudiciales para la parte consumidora o que, según una diligencia profesional exigible, hubiesen requerido la prestación de un consentimiento reforzado acerca de la contratación de las mismas o incluso, una adaptación.

En cuanto a la vulnerabilidad asociada a un determinado contexto de contratación, como el digital, no podrá dar lugar a una protección de carácter individualizado, puesto que se ha caracterizado como un supuesto de fragilidad inherente, salvo en aquellos casos en los que el contexto se combine o interseccione con otros factores de vulnerabilidad, ya sean situacionales o resultado de una determinada característica o estado más o menos permanente del consumidor.

6. Conclusiones.

El tratamiento legal de la especial vulnerabilidad del consumidor ha abonado un terreno contratastadamente ineficiente, cual es el de la información precontractual. Entendemos que en este aspecto, el derecho de consumo debe tomar prestadas las soluciones del derecho privado general, en particular, de instituciones como la ventaja injusta, y promover soluciones que favorezcan la adaptación del contrato.

Por otro lado, si consideramos que el contexto digital de contratación da pie a una vulnerabilidad consustancial, dada la asimetría adicional que el medio añade a la contratación que en él se desarrolla, ello iguala la posición de todos los consumidores y, por tanto, la protección vendrá dada por las normas que disciplinen el mercado en relación con un consumidor medio y solo en casos de combinación de factores de debilidad contractual que resulten oponibles al profesional, se podrá lograr una protección adicional.

Dacev N, Ibish M, 'Legal Arrangements of Artificial Intelligence in the European Union and the Republic of North Macedonia' (2024) 1 EJPLT, 79-97.
DOI: https://doi.org/10.57230/EJPLT241DNIM

EJPLT
ISSN 2704-8012



Legal Arrangements of Artificial Intelligence in the European Union and the Republic of North Macedonia

Disposizioni giuridiche sull'intelligenza artificiale nell'Unione europea e nella Repubblica di Macedonia del Nord

Nikola Dacev
Associate Professor of Civil Law
Faculty of Law, International Balkan University

Mevludin Ibish
Associate Professor
Faculty of Law, International Balkan University

Abstract
The article aims to analyze the need to regulate AI, the content of the regulation that needs to be enacted, the content of the regulation adopted in the European Union as well as North Macedonia's positioning on this issue as a country eager to start the negotiations for accession in the EU. The methodology for the article is about the legal arrangements of AI that involve a multi-faceted approach, combining literature review, legal analysis, doctrinal research, empirical research, policy analysis, ethical and normative analysis, and interdisciplinary collaboration. While the rapid development of AI brings convenience to people's lives, it also poses challenges to global changes and the development of human society, social governance, and legal regulation. Many countries have adopted strategic plans and documents related to AI but there are no legal acts adopted until now. The article's discussion on the need for new or updated regulatory frameworks to govern AI is crucial. It may propose specific regulatory measures to address AI's unique challenges, such as transparency, accountability, and fairness, influencing related policy development.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
L'articolo si propone di analizzare la necessità di regolamentare l'IA, il contenuto del regolamento da emanare, il contenuto del regolamento adottato nell'Unione Europea, nonché la posizione della Macedonia del Nord su questo tema come Paese intenzionato ad avviare i negoziati per adesione all'UE. La metodologia dell'articolo riguarda gli accordi giuridici dell'IA che implicano un approccio poliedrico, che combina revisione della letteratura, analisi giuridica, ricerca dottrinale, ricerca empirica, analisi politica, analisi etica e normativa e interazione interdisciplinare. Se da un lato il rapido sviluppo dell'intelligenza artificiale apporta comodità alla vita delle persone, dall'altro pone anche sfide ai cambiamenti globali e allo sviluppo della società umana, della governance sociale e della regolamentazione giuridica. Molti paesi hanno adottato piani strategici e documenti relativi all'intelligenza artificiale, ma fino ad ora non sono stati adottati atti normativi. La discussione dell'articolo sulla necessità di un quadro giuridico nuovi o aggiornati per governare l'intelligenza artificiale è cruciale. Appare opportuno proporre misure normative specifiche per affrontare le particolari sfide dell'IA, come la trasparenza, la responsabilità e l'equità, influenzando lo sviluppo delle relative politiche.

Keywords: AI national strategies; EU legislation; social responsibility; ethics.

Summary: 1. Introduction. – 2. Artificial Intelligence Regulations in the EU. – 3. Artificial Intelligence and the Rule of Law. – 4. Artificial Intelligence in Contract Law. – 5. Artificial Intelligence Liability, Transparency and Future Development. – 6. Artificial Intelligence in the Republic of North Macedonia. – 7. Conclusions.

1. Introduction.

As can be concluded from history, artificial intelligence, which is considered a scientific discipline, appeared shortly after the invention of the first computers. It is attributed to the skills characteristic of intelligent beings, including proving hypotheses, reasoning, and playing games.

About how much importance AI will have in the future some scientists have been aware of for a long time. In 1960, the father of cybernetics, Norbert Wiener, stated that it was 'now generally admitted, over a limited range of operation, machines act far more rapidly than human beings and are far more precise in performing the details of their operations. This being the case, even when machines do not in any way transcend men's intelligence, they very well may, and often do, transcend men in the performance of tasks.[1]

The concept of artificial intelligence cannot be precisely defined. It can be found a large number of definitions of AI in the literature. The first definition of AI presented by John McCarthy referred to the unity of 'science and engineering in the creation of intelligent machine' i.e. creation of especially intelligent computer programs. The definitions, which appeared a little later, can be grouped into four categories taking into account two main criteria. One

[1] N Wiener, 'Some Moral and Technical Consequences of Automation' (1960) 131(3410) Science 1355-1358 <https://doi.org/10.1126/science.131.3410.1355> accessed 12 April 2024; or see AL Samuel, 'Some Moral and Technical Consequences of Automation - A Refutation' (1960) 132(3429) Science 741-742 <https://doi.org/10.1126/science.132.3429.741>; or see M Hauser, 'What's fair? The unconscious calculus of our moral faculty' (2007) 278(41-50) Novartis Foundation symposium discussion 50-55, 89-96, 216-221.

group of definitions relates to the process of thinking and reasoning, while others take into account the factor of behavior. Another difference between the definitions of AI takes into account the category of success.[2]

Over-time, especially in recent years, the rapid growth of AI systems has led to these systems being used in almost every sphere of life. AI can be used in a wide variety of sectors such as healthcare, energy consumption, automotive safety, agriculture, climate change, and financial risk management. It can also help detect fraud and cyber security threats and enable security agencies to effectively fight crime.

Since it is used in several areas, the question of its legal regulation is also logically raised. From 2019 to 2020, scholars paid more attention to the study of AI jurisprudence by scientifically defining the corresponding rights, obligations, responsibilities, and other basic categories, laying solid foundations and providing theoretical support for the sound development of the legal system regulating AI. They also emphasize establishing a regulatory system compatible with the development of AI with a focus on finance, transportation, medical care, and urban construction, building a reasonable and practicable AI law system following statutory procedures to ensure that the development of AI obeys rules and laws. In addition, more research has been conducted on the core of AI law, primarily on theoretical and practical discussions on 'AI' and 'big data', in which scholars analyze legal issues in AI applications from an overall perspective, providing more systematic and in-depth theoretical research on the connotation and the major body of accountability in AI law.

It's worth mentioning that COVID-19 spread throughout the world in 2020 and has taken a heavy toll on human society and the global economy. In the battle against COVID-19, AI has played an extraordinary role in safeguarding the common home of humankind. AI technologies have been widely applied on the frontline, such as health QR codes, whole genome sequencing, CT imaging, and smart medical care. Their presence to provide support in each area, including epidemic monitoring and analysis, virus traceability, prevention, control and treatment, and resource allocation, has significantly improved the capability and efficiency of epidemic prevention and control. With its extraordinary performance in the fight against the virus, AI seems to herald a new period of explosive growth. People have had a deeper understanding of the power and role of AI. As a 'double-edged sword', AI has brought risks and challenges while empowering society. Increasing attention and concern from the public have been aroused for increasingly prominent problems involving

[2] D Prlja, G Gasmi and V Korać, 'The Artificial Intelligence in the EU legal system' (2023) 19 Archaeology and Science <https://doi.org/10.18485/arhe_apn.2023.19.14> accessed 5 march 2024. The authors analyse how the EU institutions approach solving the issue of the safe use of artificial intelligence. The Communication on the European Approach to Artificial Intelligence, of the European Parliament and the Council of Europe, the Coordinated Plans of the European Parliament and the Council of Europe for Artificial Intelligence, and the Proposal for the Regulation on Artificial Intelligence of the European Parliament and the Council of Europe were discussed. The Proposal contains a preamble with 89 points and twelve chapters with 85 articles. In the first title – General Provisions, the subject matter of the Act is specified, as well as the scope of its application, and definitions of 44 terms are given, including the definition of artificial intelligence systems.

security, law, ethics, and other aspects in the rapid development of new-generation AI.[3]

In the war in Ukraine and recent periods of the war in Israel and Palestine where high military technology is used, AI plays a significant role, such as the use of drones, cybertechnologies, etc. Therefore, the issue of protection and prevention in the use of these AI systems is also further emphasized. We were able to see in these war conflicts that the use of AI may lead to a violation of the primary human right – the right to live.

Additionally, the presentation of the Chat GPT robot, which can talk like a human with a high degree of fluency and coherence, drew the world's attention to the use of AI in the service of humans, but also to the possible dangers it can bring. Hence, security and ethics are the two main components that need to be addressed in AI laws.

Related to the work of the courts by 2020 some courts had begun to operate in quite different ways and had integrated Online Dispute Resolution (ODR) features into their activities, digitized records, enabled paperless e-filing systems, and begun to develop new ways of engaging with people that were supported by technology.

Courts adopting such approaches were sometimes referred to as 'online courts' or 'e-courts' to distinguish them from courts that had yet to adopt technologically driven reforms. In some justice systems, these developments were led by courts and Chief Justices (particularly in the USA), and in other places, the developments were supported by organizations that were external to the court by the government or a combination of judicial officers working with the government (for example in the UK and China with the 'smart court' initiatives).

In 2020, as a result of the COVID-19 pandemic, more courts began to change how they operated or enhanced and accelerated technological changes that were already underway. Some courts were not, however, able to rapidly convert court systems to a remote mode of operating and, as a result, delay, postponement, and confusion surrounded court activities, with jurisdictional novelty a feature of 2020 responses to a global pandemic. In some instances, a shift to a remote court operation could not be undertaken because of judicial, court, or societal issues that included a lack of access to technology or an inability to use existing technologies.[4] The abovementioned examples show that the ground for the development and use of AI existed before the pandemic, but the whole process was even more accelerated during COVID-19.

---

[3] C Yudong, *Blue Book on AI and Rule of Law in the World (2020)* (Springer 2022) <https://doi.org/10.1007/978-981-19-3586-2> accessed 10 March 2024. For the COVID-19 impact on AI see H Roberts and others 'The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation' (2021) 36 AI & Soc 59-77 <https://doi.org/10.1007/s00146-020-00992-2> or H Roberts and others (2021) 'The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation' in L Floridi (ed.) *Ethics, Governance, and Policies in Artificial Intelligence. Philosophical Studies Series* (Springer, 2021) vol 144 <https://doi.org/10.1007/978-3-030-81907-1_5>

[4] T Sourdin, *Judges, Technology and Artificial Intelligence* (Edward Elgar Publishing 2021) 1-2, <http://dx.doi.org/10.4337/9781788978262> accessed 7 June 2024. For more see the discussion in Chapter 10 entitled: 'Future Justice' 272-296 of this book and also in WD Heaven, 'OpenAI's New Language Generator GPT-3 is Shockingly Good – and Completely Mindless' (2020) MIT Technology Review <https://www.technologyreview.com/2020/07/20/1005454/openai-machine-learning-language-generator-gpt-3-nlp>.

In the next chapter, we will take a look at the existing legal framework of AI worldwide and the national strategies that the countries have adopted.

2. Artificial Intelligence Regulation in the EU.

In many societies, laws are designed and updated to regulate and follow the changes in the social circumstances between the people. Hence, the base for creating AI regulations is already there in some fields, for example in criminal law, specifically cybercrime. In fact, for at least two decades, (also) European rulers and legislators started turning their attention to new forms of offenses perpetrated in the dematerialized world of IT, trying to set common minimum rules for the harmonization of cybercrime and the consequential issues, such as competence and jurisdiction, also at the international level. The Budapest Convention on Cybercrime signed in 2001 and drafted by the Council of Europe, represented, for a huge number of jurisdictions, the first legally binding instruction to set forth specific legislation tackling such a phenomenon. The first part of the document harmonized the Member States' substantive criminal law, by providing a list of offenses that the High Contracting Parties must introduce in their jurisdictions.[5]

Cryptocurrency crimes may also be mentioned as some of the new types of crimes. They can be identified and prosecuted like any conventional illicit activities, but some of their unique features may not have been covered under existing laws on financial crimes, for example, micropayments, individual activities, and jurisdictions. Since cryptocurrency has been active online, related financial crimes are likely transnational, including individuals and organized criminal groups. Therefore, international coordination and cooperation, as well as data sharing, have become essential for combating cryptocurrency crimes. Moreover, the jurisdictions of prosecutions, law applications, and sentencing standards also vary across countries. This situation makes the proceeding of such crimes more complicated. The micropayments refer to transactions less than the smallest unit of currency; individual cryptocurrency activities are somehow not covered by regulatory rules in many countries, such as in the UK and the US; a standardized scheme for determining jurisdictions is anticipated to facilitate the prosecution processes of international financial crimes.[6]

---

[5] S Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings* (Springer 2020) vol 4. For more details, see A Sachoulidou, 'Going beyond the 'common suspects': to be presumed innocent in the era of algorithms, big data and artificial intelligence' (2023) Artif Intell Law. <https://doi.org/10.1007/s10506-023-09347-w> accessed 20 June 2024 or see LF de Oliveira and others 'Path and future of artificial intelligence in the field of justice: a systematic literature review and a research agenda' (2022) 180 *SN Soc Sci* 2 <https://doi.org/10.1007/s43545-022-00482-w> accessed on 20 June 2024.

[6] A Lui and N Ryder (eds), *FinTech, Artificial Intelligence and the Law: Regulation and Crime Prevention* (Routledge 2021) 125-136. Micropayments in the UK refer to transactions below a penny. The Bank of England deems that enabling micropayments, cryptocurrency could create a new business model: instead of paying monthly subscriptions for digital media, consumers can choose an individual news article to read (Bank of England. With its digital feature, cryptocurrencies can be converted to decimals rather than integer units like normal currencies. However, making small payments that fall below thresholds of reporting requirement has been a method for money laundering. Since using a number of gophers to launder illicit earnings can be costly and risky, small payments may only relate to small illicit earnings. With the aid of cryptocurrencies, offenders can create many pseudonymous accounts online and 24/7 process

Considering that AI development is still in its initial period, the major countries and regions in the world are not eager to introduce regulatory measures but to formulate a framework of governance principles.

If we make a comparative analysis of the most important legal systems in the field of artificial intelligence (USA, EU, China, UN) we can conclude that it represents the subject of strategic documents. In the mentioned countries and international organizations, it is regulated by the adoption of strategic documents that address the social, legal, political, and economic 'background' of AI. AI systems can be partially regulated, primarily in connection with the regulation of certain institutes within the framework of special legal texts on copyright and related rights, protection of personal data, administrative regulations, etc.

The Artificial Intelligence Act is the first comprehensive legal framework in the world that regulates the specific uses of AI, while the Coordinating Plan for Artificial Intelligence offers strategic alignment, policy action, and acceleration of investments. Together, they represent the European approach to AI - an intelligence that puts people first.[7] As part of its digital strategy, the EU wanted to regulate AI to ensure better conditions for the development and use of this innovative technology. AI can create many benefits, such as better healthcare; safer and cleaner transportation; more efficient production; and cheaper and more sustainable energy. Parliament's priority was ensuring that the EU's AI systems are safe, transparent, traceable, non-discriminatory, and environmentally friendly. AI systems should be supervised by humans, rather than automation, to prevent harmful outcomes. The focus of the European Commission in the past period when it comes to regulation of AI was modernizing product liability regulation in the digital age, enabling compensation for damage caused by robots, drones, and smart home systems that are unsafe due to software upgrades, error in AI, or digital services necessary to manage the product, as well as failure to deal with shortcomings and vulnerability to cyber-attacks by manufacturers. As a result, in June 2023, the European Parliament voted on a set of rules for AI, the first of its kind in the world. The law's final text was refined in negotiations with the Council of the European Union. In December 2023, the Council and the Parliament reached an agreement on The Artificial Intelligence Act.[8] In January 2024, the Council published a Draft Regulation of the European Parliament and the Council for establishing harmonized rules for AI and amendments of certain legislative acts of the Union - Analysis of the final compromise text for the agreement.[9] On July 12, 2024, the AI Act was officially published and will come into force on August 1, 2024. The AI Act aims to ensure that AI technologies are safe and transparent and respect fundamental rights while fostering innovation and investment in the AI sector. The new rules establish obligations

micropayments. Although processing such payments may come with fees and expenses, it should be cheaper and less risky than hiring a human.

[7] European Commission website <https://digital-strategy.ec.europa.eu/en/policies/artificialintelligence#:~:text=The%20AI%20Act%20is%20the,AI%20that%20puts%20people%20first> accessed 30.05.2024.

[8] Council of Europe website <www.consilium.europa.eu/en/policies/artificialintelligence/timeline-artificial-intelligence/>accessed 30.05.2024.

[9]<https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf>accessed 10.06.2024.

for providers and users depending on the level of risk from AI. Although many AI systems pose minimal risk, they should be evaluated. Also, the Law bans the use of AI for biometric surveillance, emotion recognition, and predictive policing, while systems like Chat GPT must disclose that content is generated by AI, and AI systems used to influence voters during elections are considered high risk.

Related to the level of risk while using AI we will briefly go through the EU rules for AI. In addition to risk-free or low-risk AI systems, there are also high-risk and unacceptable-risk systems. AI systems with unacceptable risk are systems that are considered a threat to humans and will be banned. They include cognitive behavioral manipulation of people or certain vulnerable groups: for example, voice-activated toys that encourage dangerous behavior in children; social scoring: classifying people based on behavior, socioeconomic status, or personal characteristics; real-time and remote biometric identification systems, such as facial recognition.

Some exceptions may be allowed: for example, 'post' remote biometric identification systems where identification occurs after a significant delay, will be allowed to prosecute serious crimes, but only with court approval.

AI systems that negatively affect security or fundamental rights will be considered high-risk and will be divided into two categories:

1) AI systems used in products covered by EU product safety legislation. This includes toys, aviation, automobiles, medical devices, and elevators.

2) AI systems fall into eight specific areas that will need to be registered in the EU database: Biometric identification and categorization of natural persons; Management and operation of critical infrastructure; Education and vocational training; Employment, management of workers, and access to self-employment; Access and enjoyment of basic private services and public services and benefits; Law enforcement; Management of migration, asylum, and border control; Help with legal interpretation and application of the law.[10]

The field of AL has made tremendous advances in the last few decades, but as smart as AI is now, it is getting exponentially smarter and becoming more autonomous in its actions. This raises a host of challenges to current legal doctrine, including whether the output of AI entities should count as 'speech', the extent to which AI should be regulated under antitrust and criminal law statutes, and whether AI should be considered an independent agent and responsible for its actions under the law of tort or agency.[11] Therefore, it's

[10] European Parliament and Council Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> accessed 18.07.2024.

[11] W Bartfield, U Pagallo, *Research Handbook on the Law of Artificial Intelligence Series* (Edward Elgar Pub 2018) <https://doi.org/10.4337/9781786439055> accessed on 23 June 2024. It is worth noting here author and futurist Ray Kurzweil's predictions for the future given his seminal writings about the future of information technology and AI. Kurzweil lists 2029 as the date in which AI will pass a valid Turing test and therefore be considered to have achieved human levels of intelligence. Additionally, he lists the date 2045 for the "Singularity" which he claims is when we will multiply our effective intelligence a billionfold by merging with the AI we have created. Kurzweil's timetable for the singularity is consistent with other predictions of noted futurists—for example, those of Softbank CEO Masayoshi Son, who predicts that the dawn of super-intelligent machines will happen by 2047.

impossible to predict its development but preventive regulatory measures must be taken.

In some areas, it will be very difficult to implement it without any negative consequences. For example, no simple rule-chaining or pattern-matching algorithm can accurately model judicial decision-making because the judiciary has the task of producing reasonable and acceptable solutions in exactly those cases in which the facts, the rules, or how they fit together are controversial.[12]

Every AI system is different. The use of AI tools by public and private regulators must be guided by a comprehensive technological management strategy grounded in a revised conception of what regulatory responsibility entails. Secondly, the revised understanding, described as a 'new benchmark for legality', must be incorporated into the rules governing the exercise of regulatory power that depend on these technological measures. The revision of these rules requires a 'new coherentism' which focuses on the compatibility, and inter-contingency, of regulatory measures with newly established benchmarks for legality.[13]

3. Artificial Intelligence and the Rule of Law.

What does computable law mean for the legal system's autonomy, authority, and legitimacy? Are we witnessing a shift from the Rule of Law to a new Rule of Technology? Should we even build these things in the first place?[14] Many questions arise from the high level of usage of AL There are 2 essential problems, related to its use and regulation. Ethical and societal dimensions of

[12] G Sartor, LK Branting, 'Introduction', in G Sartor, LK Branting (eds) *Judicial Applications of Artificial Intelligence* (Springer 1998) <https://doi.org/10.1007/978-94-015-9010-5_1> accessed 24 May 2024. See more at RL Canalli, 'Artificial intelligence and the model of rules: better than us?' (2023) 3 AI Ethics , 879-885 <https://doi.org/10.1007/s43681-022-00210-3> accessed 15 July 2024; M Araszkiewicz and others, 'Thirty years of Artificial Intelligence and Law: overviews' (2022) 30 Artif Intell Law, 593-610 <https://doi.org/10.1007/s10506-022-09324-9> accessed 15 July 2024 and T Bench-Capon, 'Thirty years of Artificial Intelligence and Law: Editor's Introduction' (2022) 30 Artif Intell Law , 475-479 <https://doi.org/10.1007/s10506-022-09325-8> accessed 15 July 2024.

[13] S Deakin, C Markou (eds), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence Series* (Hart Publishing 2020) 140-150 <https://doi.org/10.1111/1468-2230.12659> accessed 10 February 2024. In broad terms the chapters in this volume take one of two approaches to the question of law and computation. The first approach asks the theoretical question of whether or not computational reasoning carried out by AI can effectively simulate or replace legal reasoning. The second approach considers pragmatic problems that data driven technologies currently pose to the legal system.

[14] The autonomy of the legal system traditionally relies on the discretion of judges and legal professionals who interpret laws and make judgments based on a mix of statutory guidance, case law, and moral considerations. Computable law can reduce this human discretion by replacing or supplementing it with algorithmic decision-making. As the legal system becomes more dependent on technology, it might lose some of its traditional autonomy. Decisions and processes could become contingent on the functionality and design of technological tools, potentially reducing the ability of human actors to influence outcomes. Computable law promises greater predictability and consistency in legal decision-making, which are key components of the Rule of Law. However, this consistency must be balanced against the need for contextual and nuanced judgments that human actors provide. Technology can enhance access to justice by making legal resources and processes more accessible and efficient. However, it can also create new barriers, particularly for those who lack digital literacy or access to technology. Automating legal processes can lead to increased efficiency, reduced costs, and improved access to justice. It can also help in handling large volumes of data and complex cases more effectively. There are significant risks, including the potential for bias, loss of human judgment, and reduced transparency. Building these systems requires careful consideration of ethical, legal, and social implications.

artificial Intelligence must be taken into consideration which means that if it is used unethically, the consequences can be fatal, and the sphere in which it is used unintentionally can also lead to unwanted consequences. The second problem derives from the inability of the inventors of AI to understand fully what the legal regulation of this area means and how it should be done, to help lawmakers, and the lawmakers cannot understand how these systems work to regulate them accordingly. in this sphere, a lot of work will need to be done to increase the cooperation between the inventors of AI systems and those who will have to regulate them.

Taking into consideration the effects of the AL systems on the whole society and to avoid the shift to the Rule of Technology, we must analyze the possibility to re-work the Rule of Law, as a concept that ensures an orderly and just society that guarantees fundamental rights and values, so that it covers the use of technological tools by both public and private regulators. First, for any community, technological management (just as with rules and standards) mustn't compromise the essential conditions for human social existence (the commons). The Rule of Law should open by emphasizing that the protection and maintenance of the commons is always the primary responsibility of regulators. Moreover, all uses of technological management, whether by public regulators or by private regulators or actors should respect this fundamental responsibility. Secondly, where the aspiration is not simply to be a moral community (a community committed to the primacy of moral reason) but a particular kind of moral community, then it will be a condition of the Rule of Law that the use of technological management (just as with rules and standards) should be consistent with its particular constitutive features – whether those features are, for instance, liberal or communitarian, rights-based or utilitarian, and so on. Such is the nature of the second tier of responsibility. Many modern communities have articulated their constitutive values in terms of respect for human rights and human dignity.[15] This is done through the conscious experience of people in one society. But AI lacks conscious experience, therefore it cannot define its objectives. AI does not appear to be conscious and it cannot formulate its ends. AI's inability to form ends poses difficulties in regulating it. We often assign moral blame and impose legal liability based on intent. But AI cannot form intent. Further, those who adopt AI will often have good intentions. That could allow AI to cause harm that escapes liability in our current legal systems.[16] For example, an employer might rely on AI to award promotions, hoping to make its decisions more objective and less susceptible to improper biases. But the effect may be the opposite. AI may predict future employee success using past employment decisions that

[15] For more details see R Brownsword, H Somsen, 'Law, innovation and technology: fast forward to 2021' (2021) 13(1) Law, Innovation and Technology 1-28 <https://doi.org/10.1080/17579961.2021.1898298> accessed 23 July 2024 or N de Marcellis-Warin and others, 'Artificial intelligence and consumer manipulations: from consumer's counter algorithms to firm's self-regulation tools' (2022) 2 AI and Ethics 259-268 <https://doi.org/10.1007/s43681-022-00149-5> accessed 23 July 2024.

[16] L Di Matteo, C Poncibò and M Cannarsa (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press 2022), 46-74. See more at Part II. AI. Contracting and Corporate Law: AI in negotiating and entering into contracts by Eliza Mik, AI and contract performance by Andre Janssen; and Part III. AI and Liability: Are existing tort theories ready for AI? An American perspective by Robert A. Heverly.

were tainted by improper biases. The outcome could be discrimination against members of protected classes.

Concerning legal cases, since legal rules employ terms and concepts that can be vague and open-ended, a computational model of reasoning with cases would help. Courts often interpret the meaning of legal terms and concepts by drawing analogies across cases illustrating how a term or concept has been applied in the past.

There are computational models of analogical reasoning with legal cases. The models are based on three basic approaches. The first, prototypes and deformations, focus on how to decide a case by constructing a theory based on past cases. The second, dimensions and legal factors, employs stereotypical patterns of fact that strengthen or weaken a side's argument concerning a legal claim or concept. The third, exemplar-based explanations (EBEs), represents legal concepts in terms of prior courts' explanations of why a concept did or did not apply. The models illustrate how to represent legal cases so that a computer program can reason about whether they are analogous to a case to be decided. In particular, they illustrate ways in which a program can compare a problem and cases, select the most relevant cases, and generate legal arguments by analogy for and against a conclusion in a new case.

Legal rules and concepts are promulgated for normative purposes. Teleological arguments (i.e., arguments from the purposes or values served by a rule) play an important role in drawing legal analogies. Computational models that integrate legal rules, intermediate legal concepts (ILCs) from those rules, and cases applying the rules need to take underlying values into account. Therefore, techniques have been introduced for computationally modeling teleological reasoning by integrating values into the measures of case relevance and models of legal analogy.

The integration of text analytics into legal systems marks a significant advancement in the field of cognitive computing. Automated extraction of case facts and legal concepts from natural language texts enhances the efficiency, accuracy, and scalability of legal processes. However, ensuring data quality, addressing bias, and maintaining transparency and interpretability are critical to the successful implementation of these technologies. As text analytics continues to evolve, it will play an increasingly vital role in shaping the future of legal practice and the rule of law.[17]

In this brief analysis of AI and the rule of law, it can be concluded that AI presents both opportunities and challenges for the rule of law. As AI systems become more integrated into legal processes, they have the potential to enhance efficiency, accuracy, and access to justice. However, they also raise concerns about fairness, accountability, transparency, and the potential for bias. To harness the benefits of AI while safeguarding the rule of law, it is essential to develop robust legal and regulatory frameworks, ensure continuous oversight, and foster collaboration between human professionals and AI systems.

[17] KD Ashley, *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*, (Cambridge University Press 2017) 74. Read Part I. Computational models of legal reasoning: Introducing AI and law and its role in future legal practice and Part II. Legal text analytics: representing legal concepts in ontologies and type systems 32-34.

4. Artificial Intelligence in Contract Law.

As we have seen AI technologies can be used in different areas of life and different areas of law as well. Regarding its use in law, for example, AI may be used significantly in some aspects of contract law. It cannot negotiate complex legal terms, or draft clauses that allocate the risks of breach or reason about the mental states of the other party. However, AI can surpass humans in those aspects of the contracting process that involve (or require) real-time analysis of vast amounts of transaction parameters such as prices, delivery terms, product selections, etc.[18] The use of AI in the process of entering into contracts must be distinguished from its much simpler predecessor, namely electronic negotiation systems. The latter term refers to systems facilitating commercial communications, such as the structured exchange of electronic messages or electronic auction models.[19] Although such systems increasingly rely on AI, they are limited to the support of human negotiators and cannot negotiate instead of humans.[20]

In contract law, AI can be helpful in many aspects because of the basic principles on which the contract law relies.

We are witnessing a major revolution in how contracts are initiated, negotiated, concluded, performed, and enforced. One of the most significant trends in the field of contracting and contract law is the use of AI techniques, such as machine learning (ML) and natural language processing (NLP) – deployed by many companies during the whole lifecycle of a contract to make contracting more efficient. At the pre-contractual stage, AI and ML algorithms analyze vast amounts of data to provide insights into customer behavior, preferences, and vulnerabilities. These insights help companies create highly targeted advertising campaigns and tailor products and prices to individual customer profiles. Credit institutions use AI-driven profiling to assess creditworthiness more accurately. AI can analyze historical data and predict future behaviors, improving the accuracy of credit ratings and reducing risk. Insurance companies employ AI to better assess the risk associated with insuring an individual or entity. At the contractual stage, NLP algorithms assist in drafting contracts by pulling in relevant clauses and terms based on the contract type and context. This reduces the time and effort required to create initial contract drafts. Built on blockchain technology, smart contracts automatically execute and enforce the terms of an agreement when predefined conditions are met. They reduce the need for intermediaries and

[18] AI's role in contract law demonstrates its capacity to enhance efficiency, accuracy, and risk management in the contracting process. However, the technology's limitations in negotiating complex terms and understanding human intentions underscore the need for a hybrid approach that leverages both AI and human expertise. By thoughtfully integrating AI into contract law, we can optimize the benefits while maintaining the essential human elements that underpin legal fairness and justice.

[19] M Schoop, A Jertila, T List, 'Negoisst: A Negotiation Support System for Electronic Business-to-Business Negotiations in E-Commerce' (2023) 47(3) Data & Knowledge Engineering 371 <https://doi.org/10.1016/S0169-023X(03)00065-X> accessed on 27 May 2024. The paper is about the second phase of a business transaction and deals with electronic negotiation support.

[20] G Dobrijevic, 'Bargaining Chip: Artificial Intelligence in Negotiation,' in B Christiansen, T Škrinjaric (eds), *Handbook of Research on Applied AI for International Business and Marketing Applications* (IGI Global 2021). See also G Dobrijevic, and F Djokovic, 'E-Negotiation: Can AI Negotiate better deals?' (Sinteza 2020 - International Scientific Conference on Information Technology and Data Related Research, Belgrade, 2020) <10.15308/Sinteza-2020-289-294> accessed on 18 April 2024.

enhance trust and transparency in contractual agreements. AI tools can also simulate various negotiation scenarios and provide strategies to achieve optimal outcomes. NLP can be used to analyze the language and terms proposed by the counterparty, identifying potential risks and opportunities.

AI models can evaluate an applicant's risk based on a comprehensive analysis of personal circumstances, behavioral patterns, and past data. In the post-contractual stage systems continuously monitor the performance of contractual obligations, alerting parties to any deviations or breaches. This ensures timely compliance and helps prevent disputes. AI-driven platforms may also facilitate online dispute resolution by analyzing the contract and relevant communications to provide recommendations. These systems can mediate disputes more efficiently than traditional methods.[21]

Even some characteristics of contract law that at first stance, look like they can be only managed by humans like for example intention in concluding contracts, in contract law AI can deal with it. Although the intention is a human aspect the question is why the product was put on the market to be sold if there was no intention by the seller. AI just needs to inspect if the buyer fulfills all the conditions to conclude the contract for sale.

It is also worth mentioning the importance of the differences in the legal systems when regulating AI.

One of the main questions in contract law is whether the operator of AI systems used to perform a contract can be held liable for damages. For a better understanding of the issue of liability for breach, a few words on contractual liability in common law and civil law are useful. One of the fundamental differences between common and civil laws is the different requirements for awarding damages in contract law. While the common law assumes strict liability of the contracting party in breach of contract (existence of a breach is sufficient), the civil law legal systems also require fault (intent or negligence).[22] Therefore, the use of AI in the common law legal systems would be more helpful in this regard because of the different manner of regulating the liability for damages.

The benefits of using AI are enormous without a doubt. However, regulating AI will not be easy. For example, AI is increasingly important in corporations' internal decision-making. The technology promises increased efficiency, especially for business decisions that are made based on extensive and complex data. AI makes it possible, for instance, to analyze data from customer relationships or production processes on a massive scale, and to prepare it for decision-making processes, such as in the context of algorithmic marketing, algorithmic market research, or algorithmic controlling. Automated decision-making in corporations thus promises key entrepreneurial advantages and

[21] M Ebers, C Poncibò, M Zou, (eds) *Contracting and Contract Law in the Age of Artificial Intelligence* (Hart Publishing 2022),19-23. For a discussion of the use of AI systems in alternative dispute resolution schemes cf M Ebers, 'Automating Due Process – The Promise and Challenges of AI-based techniques in Consumer Online Dispute Resolution', in X Kramer and others (eds), *Frontiers in Civil Justice: Privatisation, Monetisation and Digitisation.* (Edward Elgar Publishing 2022) (forthcoming).

[22] For more details see C Wendehorst, 'Liability for Artificial Intelligence: The Need to Address Both Safety Risks and Fundamental Rights Risks' in S Voeneky and others (eds), *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspective*s (Cambridge University Press 2022) 187-209 <https://doi.org/10.1017/9781009207898.016> accessed 26 July 2024.

efficiency gains. However, automated decision-making also represents the crucial regulatory challenge of this technology.[23] it must be taken into account that an error in the AI system that would contribute to adopting a wrong business decision can lead to big financial losses for the company, but also for customers and other entities on the market depending on the company's activity.

5. Artificial Intelligence Liability, Transparency, and Future Development.

The issue of liability for AI systems is complex and multifaceted, involving questions of accountability, legal responsibility, and ethical considerations. As AI systems become more autonomous and integrated into various aspects of society, addressing liability becomes increasingly crucial.

AI, unlike standard static rules-based software algorithms, is dynamic. It is trained on (often historical) data and continues to learn based on initial parameter rules set from its inputs and its environment. It adapts (whether in a supervised or unsupervised manner) to new situations and new application domains. Based on its 'learning', the AI can recognize patterns, make predictions, make recommendations, and auto-label, helping to speed up processes, thus making them often faster and more efficient than human operations. This raises questions of whether such automatic labeling and/or AI-driven recommendations and predictions are accurate and fair. The output from AI may correctly present the desired end goal, but it is unlikely to understand the context in which that output is to be applied. This can lead to biased or domain-inappropriate results. Furthermore, the efficiencies of AI can also lead to fewer humans being employed in such tasks. This can lead to deskilling or a reduction in human capacity and capability. There are socio-economic effects of AI replacing humans in tasks, such as job losses or role changes, which also have implications for the future of work. This can impact how humans feel valued, feel significance, and experience the fulfillment and joy of a 'job well done' that a paid-for occupation can provide, which also can impact income and ability to earn. A dim picture can be painted of a downward spiral of mankind if ethical and societal impacts even at smaller AI-task levels are not taken seriously at an early stage.[24]

---

[23] While AI offers significant benefits for corporate decision-making, these must be balanced against the need for ethical considerations, accountability, and regulatory compliance. By developing comprehensive legal frameworks, implementing ethical guidelines, ensuring transparency and accountability, and protecting data privacy and security, regulators can address the challenges posed by AI and ensure its responsible use in corporate contexts. This balanced approach will help maximize the benefits of AI while mitigating its potential risks.

[24] C Kerrigan (ed), *Artificial Intelligence Law and Regulation* (Edward Elgar Publishing 2022), 398-399 <http://dx.doi.org/10.4337/9781800371729> accessed 17 June 2024. The author highlights several critical points about the nature and implications of AI: Dynamic Nature of AI (Training and Adaptation: Unlike static rules-based algorithms, AI systems are dynamic, learning from data and adapting to new situations and environments); Accuracy and Fairness Concerns (Bias and Context Understanding): AI's ability to automatically label and make recommendations is powerful but raises questions about accuracy and fairness; Socio-Economic Impacts (Employment and Deskilling): The efficiencies brought by AI can lead to fewer human jobs in certain areas, resulting in deskilling and reduced human capacity (Future of Work): The displacement of human labor by AI has broader implications for the future of work. It can influence how

The importance of liability and AI systems has already been mentioned in several recent documents issued by the European Union (EU). The White Paper on Artificial Intelligence, for instance, stresses that the main risks related to the use of AI concern the application of rules designed to protect fundamental rights as well as safety and liability-related issues. Scholars have also concluded that 'liability certainly represents one of the most relevant and recurring themes' when it comes to AI systems. This emphasis on liability is not surprising considering that AI systems will increasingly cause damage. Reference can be made to recent accidents involving autonomous vehicles. The autopilot of a Tesla car, for instance, was not able to distinguish a white tractor-trailer crossing the road from the bright sky above, leading to a fatal crash. A self-driving Uber car recently hit a pedestrian in Arizona. The woman later died in the hospital. A robot also attacked and injured a man at a tech fair in China. A surgical robot at a hospital in Philadelphia malfunctioned during a prostate surgery, thereby severely injuring the patient. These examples show that accidents may happen despite optimizing national and supranational safety rules for AI. This is when questions of liability become important. Nevertheless, the application of liability regimes for damage caused by AI systems can be challenging. The characteristics of AI systems such as opaqueness, autonomy, connectivity, data dependency, or self-learning abilities make it difficult to trace back potentially problematic decisions made with the involvement of such systems. This in turn may make it challenging for victims to obtain compensation under the current EU and national liability regimes. Moreover, there is also some uncertainty regarding the allocation of responsibilities between different economic operators in the supply chain of AI systems. Several parties can be involved such as the developers of the software/algorithm, the producer of the hardware, owners/keepers of the AI product, suppliers of data, public authorities, and the users of the product. Persons who have suffered harm may not have effective access to the evidence that is necessary to build a case in court and may have less effective redress possibilities compared to situations in which the damage is caused by 'traditional' products. It is, however, important that victims of accidents involving AI systems are not confronted with a lower level of protection compared to other products and services for which they would get compensation under national law. Otherwise, societal acceptance of those AI systems and other emerging technologies could be hampered and a hesitance to use them could be the result.[25]

---

individuals perceive their value and significance, potentially diminishing the fulfillment derived from meaningful employment; Ethical and Societal Considerations (Impact on Human Well-being): The potential for AI to affect human well-being and societal structures underscores the importance of considering ethical and societal impacts early in AI development. Ensuring that AI systems are designed and implemented with these considerations in mind is crucial to prevent negative outcomes.

[25] J De Bruyne, C Vanleenhove (eds), *Artificial Intelligence and The Law* (Intersentia 2021) 360-361. The authors examine whether victims may be successful in claiming recovery for damage caused by AI systems under Belgian tort law. They limit their research to the application of tort or extra-contractual liability regimes in the context of AI. Contractual and criminal liability for damage caused by AI systems are thus not addressed. They restrict their research to tort liability as this is a re-occurring and important topic in several documents that were recently issued by the European Commission. Extra-contractual liability encompasses many of the most fundamental questions and problems that arise in the context of AI and liability. They focus on fault-based liability for damage caused by AI systems, product liability and liability for defective things.

Machine learning and computer processing cannot at this stage be compared with human reasoning and emotional intelligence. If AI eventually acquires the faculty for practical reasoning (and it probably will in the distant future) and agency, then the normal rules of criminal responsibility (whatever they are at the given point in time) will apply. There will be no need for new rules if these machines can make rational choices, but there will be a need for transitional rules for the long period when these AI machines straddle between being able to make fully autonomous choices and partially autonomous choices. At the moment, they can do neither. Civil law such as manufacture liability rules already applies to AI, because at the moment, it is considered no more than an instrument in the hands of human agents.[26]

Artificially intelligent systems should make user lives easier and support them in complex decisions, or even make these decisions completely autonomously. However, at the time of writing, the processes and decisions in an intelligent system are usually not transparent to users. They do not know which data are used, for which purpose, and with what consequences. There is simply a lack of transparency, which is important for trust in intelligent systems. Transparency and traceability of decisions are usually subordinated to performance and accuracy in AI development or sometimes play no role at all. The creation of substantial laws, like the General Data Protection Regulation (GDPR) also referred to as Regulation (EU) 2016/679 (Regulation, 2016), and ethical principles, is intended to remedy this situation and contribute to improving transparency and control. However, legal regulations demand that applications, or more precisely, the socio-technical systems, consider legal aspects and equally consider all stakeholders; e.g., software architects, developers, legal professionals (who check and confirm legal compliance), providers, and users.

In this part, the development of legally compliant software needs a tight collaboration between the different stakeholders must be emphasized. Developing legally compliant software necessitates a multifaceted approach involving close collaboration among software developers, legal experts, end-users, and regulatory bodies. By understanding and integrating legal requirements, providing transparent and accessible information to users, and continuously monitoring and updating the software, providers can ensure that their applications remain compliant with the law. This approach not only protects users but also safeguards the providers from potential legal breaches, contributing to the overall reliability and trustworthiness of the software.[27]

---

[26] DJ Baker, PH Robinson, *Artificial Intelligence and the Law: Cybercrime and Criminal Liability* (Routledge 2020) 3. We often hear the term "autonomous weapon," but this is an oxymoron. Currently, a machine cannot be criminally liable either directly or through the law of complicity for any harm it causes. There is currently no comparison between "machine learning" and "human understanding." Nonetheless, like all machines, AI has capabilities beyond those of a single human. It is true that AI-equipped machines can do many things that humans cannot, but the same can be said of machines generally.

[27] SJ Thomson, *Machine Law, Ethics, and Morality in the Age of Artificial Intelligence* (IGI Global 2021) 13 <10.4018/978-1-7998-4894-3> accessed 24 May 2024. In this chapter the authors describe what intelligent systems are and explain how users can be supported in specific situations using a context-based adaptive system. In this context, the authors describe the challenges and problems of intelligent systems in creating transparency for users and supporting their sovereignty. The authors then show which ethical and legal requirements intelligent systems have to meet and how existing approaches respond to them.

About the future development of AI, we can say that current AI technology, often based on machine learning, is narrow in the sense that it can learn to solve specific problems, such as selecting a job applicant, writing texts, or playing a game. Typically, it cannot solve problems across a wide range of contexts. For instance, an AI system that has learned to drive a car cannot transfer that knowledge into a new domain; it cannot make investment suggestions or write a love letter. AGI is a label often used for future forms of AI that are significantly less limited than current technologies and far more capable of competing with human intelligence than narrow AI. AGI has been defined as a form of AI that 'equals or exceeds human intelligence in a wide variety of cognitive tasks'. So far, it does not exist, but narrow AI can solve many problems without any need to be intelligent. The idea of AGI is based on the hypothesis that progress can be made toward the increased and broad intelligence of artificial agents. Given the speed at which AI has been developed and has taken over on a global scale, some argue that the possibility that AGI may be created cannot be excluded.[28]

6. Artificial Intelligence in the Republic of North Macedonia

The use of artificial intelligence (AI) in the absence of strategy or regulation exposes citizens to the risk of potential abuse. Although many countries have already adopted a national strategy for AI, this is not the case in the Republic of North Macedonia. In September 2021, a working group for the National Strategy for AI was established, consisting of domestic experts, but also successful Macedonians who are globally recognized professionals in this field and work in world-renowned companies and universities. One of the objectives of the National Strategy for Artificial Intelligence is to give a chance to many domestic, innovative startup companies to realize their ideas and projects, respectively education as well as access to modern equipment. Unfortunately, only one meeting has been held since 2021. The strategy is part of the economic development plan of the Republic of North Macedonia and part of the National Strategy for Development 2021-2041. After the elections and establishment of a new Government and taking into account the fact that AI is developing at an enormous speed, and the risks were aforementioned, the Republic of North Macedonia should proceed faster with the adoption of the National Strategy for AI.

About the next steps, the Fund for Innovation and Technological Development in communication with UNDP, the World Bank, as well as other interested parties who have experience and knowledge in the development of a National Strategy AI, will work to provide a leading expert, i.e. a consultant or a team that will help in the process of developing the strategy, with the support of the working group, as well as in the process of developing a financial

[28] B Custers, E Fosch-Villaronga, *Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice* (Springer 2022) 521-522 <https://doi.org/10.1007/978-94-6265-523-2> accessed on 29 June 2024. See also P Księżak, S Wojtczak, 'Consent' in P Księżak, S Wojtczak (eds) *Toward a Conceptual Network for the Private Law of Artificial Intelligence. Law, Governance and Technology* (Springer 2024) vol 51 <https://doi.org/10.1007/978-3-031-19447-4_5> accessed 26 July 2024.

construction for the realization of the whole process. However, it should be taken into account that it is a very extensive process, for which significant resources, time, and humans, are necessary, but if the members of the working group are dedicated to the creation and development of a successful strategy, it will have positive benefits for the ecosystem.[29]

First, the companies need to transform, and all companies need to do that, collect data, adapt processes and systems, and then get the most out of AI. At the moment when the market of the European Union opens, the biggest problem will be Macedonian companies that will not invest on time, because there will be greater competition with companies that are more technologically developed.[30]

The main question is how ready is North Macedonia for the use of AI in the public sector, do we have a relevant digital infrastructure and what are the possible risks of the use of AI in the absence of a National Strategy? For this reason, the communication and cooperation between different entities will enable the country to adopt a relevant and accurate national strategy on AI.[31]

Its worth mentioning that in the field of education and research universities in North Macedonia are increasingly offering programs and courses related to AI, machine learning, and data science to equip students with the necessary skills. Collaborative efforts with international universities and research institutions are fostering a robust academic environment for AI research and development. Research institutions are actively working on AI projects, often in collaboration with EU programs and other international bodies. Key areas of research include AI applications in healthcare, agriculture, and smart cities. The tech industry in North Macedonia is growing, with several companies focusing on AI and related technologies. Startups are emerging in AI-driven software development, fintech, and health tech fields. Innovation hubs and tech incubators are supporting startups and fostering a culture of innovation. These hubs provide resources, mentorship, and funding opportunities for AI-based startups. Therefore, we can say that with supportive government policies, investment in education and infrastructure, and a growing tech industry, AI can significantly contribute to the country's development and global competitiveness.[32]

---

29 Fund for Innovation and Technological Development of North Macedonia, <https://fitr.mk/> accessed on 25 May 2024. The Fund for Innovation and Technological Development is a leading government institution for supporting startups and innovative companies in the Republic of North Macedonia. The main priorities of the Fund are improved access to financial support for innovation and technological development and promotion and encouragement of innovation activity in North Macedonia.

30 In the business sector in the Republic of North Macedonia, companies like Data Masters actively help domestic companies to adapt to new technologies and implement AI solutions in their operations. See some case studies at <https://datamasters.ai/> accessed on 05 September 2024.

31 <https://mk.bloombergadria.com/tehnologija/digitalizacija/61686/vestackata-inteligencija-vo-javniot-sektor-do-kade-e-makedonija/news/> accessed on 05 September 2024. The first digital assistant in North Macedonia was launched in 2023. It was heralded as the first AI-based assistant of its kind in the region. It was made available to citizens and above all to foreign investors in order to receive complete information about the conditions for investing in North Macedonia and about the state aid offered for investments. In reality, it was only a chatbot with data related to foreign investments, and not the use of AI. Its simple use shows that it is more of a PR tool than a real use of machine learning and artificial intelligence for the needs of citizens.

32 Institute for Digitalization, Economy and Innovation IDEI-Skopje, <https://idei.org.mk/category/pub/st/> accessed on 05 September 2024. The Institute is dedicated to improving public policies by building an open,

Although more countries are still limited in regulating AI, the problems that can cause its use and the consequences it can bring are already obvious. The greatest danger to people is the latest military technologies used, drones, cyber-attacks, etc. The Republic of North Macedonia is no exception. Chat GPT is another example of the possible misuse of AI, which is also heavily used by Macedonian students. In practice some students used it to copy seminar papers, master thesis, and doctoral dissertations instead of using it as a benefit, to get more information on how to write a thesis. From the above-mentioned, we can see that AI has positive and negative sides. It's up to human morality which one will be used.

7. Conclusions.

What we can draw as a conclusion is that the benefits of artificial intelligence should be used but only for the benefit of humanity. It would not be advisable for AI to take over the whole control in certain fields. There must be limitations in its use precisely because its unlimited use can cause great dangers leading to harmful consequences, even endangering people's lives.

AI brings with it many benefits for traditional social concepts by helping in the efficiency and success of many business and private activities, faster and better than a human does. The fields of application of AI are numerous and include important sectors such as agriculture, transport, catering, tourism, healthcare, sports, arts, etc.

Further directions of development, should be based on the arrangement of AI systems in special regulations and areas of law, and not exclusively on a single regulation that would regulate the application of AI in an equal way in in all areas. The possibilities of information and communication technologies are enormous, which is also accompanied by a significant risk to the rights and freedoms of citizens, so it is necessary to investigate and arrange it in detail (legal norms) the relationship between the specific form of AI and the area of law in which is applied (administrative law, constitutional law, commercial law, data protection law, etc.). The integration of AI into contracting processes that was analyzed briefly in this article is creating a paradigm shift, enhancing efficiency, accuracy, and customization while also posing challenges related to data privacy and ethical use. As AI technologies continue to advance, they will further transform the way contracts are initiated, negotiated, concluded, performed, and enforced, leading to a more dynamic and responsive contracting environment. In addition, it is necessary to pay more attention to

---

credible socio-economic system through the use of digital tools and innovative solutions. The Institute has published analyses, studies, opinions and reports related to AI. See A Kostadinov, *Artificial inteligence and politics: Comparative analysis of the character of the political debate on Twitter among the leaders of the three biggest Macedonian parties* (Insitute for Digitalization, Economy and Innovation IDEI-Skopje 2023) <https://idei.org.mk/wp-content/uploads/2023/11/%D0%92%D0%B5%D1%88%D1%82%D0%B0%D1%87%D0%BA%D0%B0%D1%82%D0%B0-%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%B8%D0%B3%D0%B5%D0%BD%D1%86%D0%B8%D1%98%D0%B0-%D0%B8-%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B0%D1%82%D0%B0.pdf> accessed on 05 September 2024.

the implementation of new technology opportunities within traditional branches of law and institutes. In that sense, legal systems must adapt to the challenges that usage of AI brings, i.e. they should provide a high level of reliability and safety of the functioning of the AI system. It can be achieved only by adopting new precise regulations, which will define the standards, which they have to fulfill high-risk and low-risk applications that use AI.

Bearing in mind that AI directly affects the lives of citizens and the functioning of society, legal systems and legal science should not remain silent on its appearance and the increasing use of new technologies in everyday life social and business activities.

Gaggero P, Valenza C A, 'Le nuove prassi valutative del merito creditizio tra GDPR, CCD II e AI Act' (2024) 1 EJPLT, 98-116.
DOI: https://doi.org/10.57230/EJPLT241PGCAV

EJPLT
ISSN 2704-8012



Le nuove prassi valutative del merito creditizio tra GDPR, CCD II e AI Act*

*New Creditworthiness assessment practices between GDPR, CCD II and the AI Act**

PAOLO GAGGERO
Professore ordinario di diritto dell'economia
Università degli Studi di Roma "La Sapienza"

CALOGERO ALBERTO VALENZA
Assegnista di ricerca
Università degli Studi di Roma "La Sapienza"

Abstract

La crisi dei mutui subprime ha confermato la centralità della valutazione del cd. "merito creditizio" in ambito bancario. Tale attività, basata sulla raccolta e l'elaborazione di dati, non è stata compiutamente disciplinata dal legislatore, cosicché assumono un ruolo centrale le regole e i principi del GDPR. Quest'ultimo, tuttavia, non risolve efficacemente alcune problematiche, relative principalmente all'uso dei nuovi sistemi di *credit scoring* basati sull'IA. Tali criticità sembrano essere state però meglio affrontate dalla CCD II e dall' AI Act.

The subprime mortgage crisis has confirmed the centrality of the 'creditworthiness' assessment in banking. This activity, based on the collection and processing of data, has not been fully regulated by the legislator, so that the rules and principles of the GDPR assume a central role. The latter, however, does not effectively resolve certain issues, mainly related to the use of the new AI-based credit scoring systems. These critical issues, however, seem to have been better addressed by CCD II and the AI Act.

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

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: credit scoring; merito creditizio; tutela dei dati personali; intelligenza artificiale; attività bancaria; credito al consumo.

Summary: 1. Autonomia contrattuale e impresa bancaria. – 2. GDPR e attività bancaria: premessa. – 3. Sistemi di valutazione del merito creditizio tradizionali e innovativi. – 4. Sistemi di valutazione del merito creditizio e disciplina sul trattamento dei dati personali. – 5. L'insufficienza della disciplina sul trattamento dei dati personali in relazione ai nuovi sistemi di *credit scoring*. – 6. La regolazione del fenomeno nella Direttiva sul credito al consumo (CCD II) e nel nuovo Regolamento UE sull'intelligenza artificiale: il superamento di alcuni problemi lasciati aperti dal GDPR.

1. Autonomia contrattuale e impresa bancaria.*

La *liaison* tra autonomia contrattuale e iniziativa economica privata[1] e, in particolare, tra impresa e contratto, che consegue alla strumentalità del contratto all'impresa, implica la permeabilità del primo alle esigenze della seconda. Con riguardo all'attività bancaria l'interrelazione appare del resto palesata, anche dal punto di vista pratico, dalla non remota crisi dei mercati finanziari che affonda le proprie radici nell'inappropriatezza dei contratti in cui si è suddiviso il corno dell'attività bancaria consistente nell'erogazione del credito[2]. La vicenda è conseguenza, soprattutto, d'una degenerazione dell'impresa bancaria[3] consistita nell'esercizio di quella sua componente rappresentata dall'erogazione in modo svincolato dalla rigorosa valutazione del rischio di credito[4], con particolare riguardo al merito creditizio del

* Pur essendo il presente contributo frutto della riflessione comune dei due autori, i paragrafi vanno così imputati: a Paolo Gaggero il § 1; a Calogero Alberto Valenza i §§ da 2 a 6.

[1] Le collega, a es., A. Zoppini, *Autonomia contrattuale, regolazione del mercato, diritto della concorrenza*, in Aa.Vv., *Contratto e* antitrust, a cura di G. Olivieri e A. Zoppini, Bari-Roma, 2008, 3 ss., e in *Obbligazioni. II. Il contratto in generale*, in *Diritto civile* diretto da N. Lipari e P. Rescigno, coordinato da A. Zoppini, vol. III, t. II, Milano, 2009, 55 ss., per il quale la concorrenza è la manifestazione del pluralismo dell'iniziativa economica privata che si serve dell'autonomia contrattuale che ne è alle origini. Cfr. G. Alpa, *Vendite al consumatore e controllo dei contratti standard nella disciplina del Supply of Good (Implied Term) Act del 1973*, in *Riv. dir. comm.*, 1974, I, 283 ss., F. Galgano, *I contratti d'impresa, i titoli di credito, il fallimento*, Bologna, 1980, 1, e G. Cian, *Diritto civile e commerciale oltre il sistema dei codici*, in *Riv. dir. civ.*, 1974, I, 523 ss., e Id., *Contratti civili, contratti commerciali e contratti d'impresa: valore semantico-ermeneutico delle classificazioni*, *ivi*, 2004, I, 849 ss.

[2] Si allude alla crisi innescata dall'insolvenza di Lehman Brothers Holdings Inc. Sulla vicenda, nell'estesa letteratura, si possono confrontare R.A. Posner, *The Crisis of Capitalist Democracy*, Cambridge, Mass. – London, 2010, anche nella trad. it. a cura di M. Cupellaro, *La crisi della democrazia capitalista*, Milano, 2014; J.E. Stiglitz, *Freefall: America, Free Markets and the Sinking of the World Economy*, New York, 2010, anche nella trad. it. a cura di D. Cavallini, *Bancarotta. L'economia globale in caduta libera*, Torino, 2014; e D. Faber e N. Vermunt (eds.), *Bank Failure: Lessons from Lehman Brothers*, Oxford, 2017.

[3] La ricerca può muovere dall'acuta analisi di F. Capriglione, *Crisi a confronto (1929 e 2009). Il caso italiano*, Padova, 2010.

[4] Si allude non solo al rischio di insolvenza (nel quale talora si esaurisce la nozione di rischio di credito: così, ad es., A. Malinconico, *Rischio di credito e modern portfolio theory. Modelli innovativi per la gestione dei prestiti*, Milano, 2000), ma anche a quello di una variazione negativa inattesa del merito creditizio del sovvenuto, ossia al rischio di migrazione verso una classe di debitori di minore affidabilità, a cui corrisponde una diversa, peggiorativa valutazione del valore del credito e l'inadeguatezza del tasso di interesse (il c.d. rischio di *spread* rispetto al parametro variabile di riferimento) così come originariamente convenuto siccome non più adeguatamente remunerativo del rischio di credito implicato dall'operazione di finanziamento nel suo

sovvenuto che ne esprime la solvibilità e consiste nell'attitudine alla restituzione del finanziamento oltre che al pagamento degli interessi[5].

Sotto quest'ultimo profilo, la c.d. crisi del mercato dei mutui *subprime* è la risultante della migrazione dal modello tradizionale di esercizio dell'attività bancaria verso altri con accentuata caratterizzazione finanziaria. Si allude all'allontanamento dal prototipo classico "*originate-to-hold*" che conserva il credito e il rischio di credito in capo al finanziatore[6]; e al passaggio alla differente pratica "*originate-to-distribute*" caratterizzata dalla dislocazione del credito presso soggetti altri dal sovventore[7]. Quest'ultima è informata all'aspettativa di un miglioramento della *performance* reddituale dell'impresa bancaria[8], ma al prezzo dell'affrancamento delle banche dalla fondamentale funzione economica di selettore di debitori affidabili[9]. In questa prospettiva si possono leggere le disposizioni (così l'art. 116-*bis* t.u.b.[10] e l'art 8 della direttiva del Parlamento europeo e del Consiglio, 23 aprile 2008, n. 2008/48/CE[11], attuato nell'ordinamento interno mediante l'inserimento nel t.u.b. dell'art. 124-*bis*) che appaiono orientate a recuperare l'attività professionale di finanziamento, *massime* bancaria, all'alveo suo proprio, senza giungere a precludere modelli alternativi a quello tradizionale.

La crisi del mercato dei mutui *subprime* rappresenta, quindi, un'esemplare testimonianza della rilevanza che, nella prospettiva della stabilità, assume la

---

divenire (cfr. A. SIRONI, *La misurazione e la gestione del rischio di credito: approcci alternativi, obiettivi e applicazioni*, in AA.VV., *La gestione del rischio di credito*, a cura di P. SAVONA e A. SIRONI, Roma, 2000, 1 ss.).

[5] *Amplius*, sul tema, M. ONADO, *La gestione del rischio di credito nelle banche europee*, Milano, 1995; A. RESTI e A. SIRONI, *Rischio e valore nelle banche. Misura, regolamentazione, gestione*, Milano, 2008; e i volumi collettanei a cura di M. COMANA, *Banca, credito e rischi. Saggi in onore di Tancredi Bianchi*, Roma, 2010, e a cura di A. SIRONI e M. MARSELLA, *La misurazione e la gestione del rischio di credito. Modelli, strumenti, politiche*, Milano, 1998.

[6] Ciò induce alla – e si manifesta nella – cura prestata dal finanziatore nella valutazione *ex ante* del merito creditizio: v., a es., D. DIAMOND e P. DYBVIG, *Bank Runs, Deposit Insurance, and Liquidity*, in *J. of Political Ec.*, 91(1983), 401 ss.; e B. HOLMSTROM e J. TIROLE, *Private and Public Supply of Liquidity*, *ivi*, 106(1998), 1 ss.

[7] Cfr., tra gli altri, G. GORTON e G. PENACCHI, *Banks and loan sales: Marketing nonmarketable assets*, in *J. of Monetary Economics*, 35(1995), 389 ss.; e J. STEIN, *Information Production and Capital Allocation: Decentralized versus Hierarchical Firms*, *ivi*, 57(2002), 1891 ss.

[8] V. A.S. CEBENOYAN e P. STRAHAN, *Risk Management, Capital Structure, and Lending at Banks*, in *J. of Banking & Finance*, 28(2004), 1943 ss., e A. PURNANANDAM, *Interest Rate Derivatives at Commercial Banks: An Empirical Investigation*, in *J. of Monetary Economics*, 54(2007), 1769 ss.

[9] Sotto questo profilo, in prospettiva economica e sociologica, v. A. PARGUEZ, *La dynamique de la monnaie*, in *Economie et Sociétés*, 1984, 83 ss., spec. 99.

[10] Introdotta dall'art. 1, co. 1, lett. n), d.l. 27 dicembre 2006, n. 297, conv. con modificazioni, dalla l. 23 febbraio 2007, n. 15, e poi abrogata dall'art. 4, d.lgs. 13 agosto 2010, n. 141, la disposizione consentiva alla Banca d'Italia di disporre che le banche e gli intermediari finanziari illustrassero agli imprenditori che ne facessero richiesta i principali fattori alla base dei rating che li riguardassero, senza che l'inerente comunicazione potesse dar luogo a oneri per il cliente. In argomento, v. G. MUCCIARONE, *La liceità delle «spese secondarie» nelle operazioni bancarie: l'impatto della direttiva 2007/64/CE sui servizi di pagamento*, in AA.VV., *Armonizzazione europea dei servizi di pagamento e attuazione della direttiva 2007/64/CE*, a cura di M. RISPOLI FARINA, V. SANTORO, A. SCIARRONE ALIBRANDI e O. TROIANO, Milano, 2010, 495 ss. e, ivi, 520, e C. COSTA, *Le regole di Basilea II tra tutela del capitale delle banche e comportamenti virtuosi delle imprese*, in AA.VV., *Le fonti private del diritto commerciale*, a cura di V. DI CATALDO e P.M. SANFILIPPO, Milano, 2008, 209 ss. e, ivi, 212 ss.

[11] La disposizione ha imposto agli Stati membri di introdurre l'obbligo di verificare il merito creditizio del consumatore, prima della conclusione del contratto di credito e sulla base di informazioni adeguate, se del caso fornite dal consumatore stesso e, ove necessario, ottenute consultando la banca dati pertinente; e l'ulteriore obbligo per il creditore di aggiornare le informazioni finanziarie di cui dispone con riguardo al consumatore, nonché di procedere a una nuova valutazione del suo merito creditizio prima di procedere a un aumento significativo dell'importo totale del credito. In tema, v. G. CARRIERO, *Credito ai consumatori*, nel *Testo unico bancario. Commentario. Addenda di aggiornamento ai d.lgs. 141/2010 e 218/2010*, a cura di M. PORZIO, F. BELLI, G. LOSAPPIO, M. RISPOLI FARINA e V. SANTORO, Milano, 2011, 93 ss.

valutazione del merito creditizio, delle tecniche con cui si compie e dei dati di cui si serve.

2. GDPR e attività bancaria: premessa.

Tra i settori in cui le regole contenute nel Regolamento 2016/679/UE (c.d. GDPR) [12] assumono un'importanza particolarmente significativa vi è perciò quello bancario, non foss'altro per l'ingente mole di dati personali, anche sensibili, che viene quotidianamente acquisita e trattata dalle banche nell'esercizio della loro attività tipica.

La raccolta continua e non occasionale di dati attinenti ai clienti è, infatti, connaturale all'attività bancaria e imprescindibile per il suo svolgimento secondo il modello che più conviene alla stabilità dell'intermediario e sistemica[13]. E, del pari, si registra anche al di fuori dell'attività propriamente bancaria degli intermediari in discorso: così, a esempio, nel quadro della semplice prestazione di servizi di pagamento, la quale presuppone l'acquisizione e l'archiviazione di tutti i dati relativi alle operazioni di pagamento del cliente e, di conseguenza, la possibilità di disporre di un articolato quadro delle spese sostenute.

D'altra parte, l'utilizzo di una grande quantità e varietà di informazioni consente anche di contenere alcuni tra i principali rischi connessi all'attività bancaria. Per tale ragione, nell'ottica di assicurare una maggiore stabilità ed efficienza del sistema finanziario, è la stessa legge, talvolta, a imporre agli intermediari la raccolta di certi dati dei clienti e, specie nell'area dei servizi e delle attività di investimento, anche la loro "profilazione"[14].

---

[12] Tale Regolamento, abrogativo della direttiva 95/46/CE, costituisce l'ultimo esito di un lungo processo, la cui fase iniziale è stata accuratamente ricostruita da Cesare Massimo Bianca (*Note introduttive*, in *Tutela della privacy. Commentario alla L. 31 dicembre 1996, n. 676*, a cura di C.M. BIANCA e F.D. BUSNELLI, in *Nuove leggi civ. comm.*, 1999, p. 219). A essa ha fatto poi seguito il d.lgs. 30 giugno 2003, n. 196 (c.d. "Codice in materia di protezione dei dati personali", ancora oggi in vigore, anche se profondamente modificato per adeguarlo al GDPR), che si apriva con un espresso riconoscimento del diritto di chiunque alla protezione dei dati che lo riguardano (art. 1), per la cui qualificazione come autonomo diritto della personalità v. C.M. BIANCA, *Note introduttive*, in *La protezione dei dati personali. Commentario al il d.lgs. 30 giugno 2003*, n. 196, a cura di C.M. BIANCA e F.D. BUSNELLI, Padova, 2007, XIX ss.

[13] Sul punto, più ampiamente, G. LA ROCCA, *Trattamento dei dati personali e impresa bancaria*, in *Riv. dir. banc.*, 2018, 299 ss.

[14] Qui intesa, però, genericamente, come raccolta di dati e informazioni su un soggetto al fine di "categorizzarlo" in base alle sue caratteristiche e non già secondo la specifica accezione accolta nel GDPR che si riferisce invece esclusivamente alla profilazione *automatizzata.* Si pensi, a esempio, alla raccolta di informazioni per la costruzione del profilo finanziario dl cliente che deve essere svolta ai fini della valutazione di adeguatezza o di appropriatezza di un determinato strumento finanziario per uno specifico cliente secondo la disciplina MiFID (cfr. art. 25, par. 3, direttiva 2014/65/UE, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari (MiFID II) nonché artt. 55 e 54, par. 4 e 5, Regolamento delegato 2017/565/UE, del 25 aprile 2016). Per non parlare della disciplina sulla c.d. *product governance* che opera a monte, la quale postula che il distributore di un servizio di investimento effettui un'analisi della propria clientela al fine di identificare *ex ante* i gruppi di clienti di riferimento, a un livello sufficientemente granulare e in base a dei parametri predefiniti, per le cui esigenze, caratteristiche ed obiettivi lo strumento finanziario è o non è compatibile (cfr. art. 16, par. 3 e art. 24, par. 2, direttiva MiFID II; art. 10, direttiva delegata 2017/593/UE, del 7 aprile 2016, nonché gli orientamenti n. 36 e 37 contenuti nella *Linee Guida Esma sugli obblighi di governance dei prodotti ai sensi della MiFID2* del 5 febbraio 2018). Questione diversa è, dunque, quella relativa alla possibilità di svolgere tali attività in modo completamente automatizzato, sfruttando le potenzialità offerte dall'innovazione tecnologica, su cui si vedano, con specifico riferimento alla valutazione

Un ambito nel quale ciò si verifica è quello relativo alla valutazione del merito creditizio del consumatore, atteso che, per svolgere correttamente tale processo, cui è obbligato *ex lege*, il finanziatore deve preventivamente acquisire una serie di informazioni sul soggetto che richiede il prestito, utili ad accertarne la capacità di rimborso del capitale e di pagamento degli interessi.

Le disposizioni normative specificamente dedicate alla valutazione del merito di credito sono però ben poche e non forniscono sufficienti chiarimenti in ordine alle metodologie e ai dati concretamente utilizzabili.

Si tratta di una lacuna di non poco conto, soprattutto in considerazione del progressivo diffondersi di sistemi che consentono di effettuare tale valutazione in modo assai innovativo rispetto al passato, sfruttando le potenzialità offerte dai c.d. *Big Data* [15] e dall'utilizzo di tecniche di c.d. intelligenza artificiale per analizzare e processare tali dati, incluso il *machine learning*[16].

---

di adeguatezza o appropriatezza dello strumento finanziari, le riflessioni di M. DE MARI, *La profilatura finanziaria algoritmica*, in *Orizzonti del Diritto Commerciale*, 2021, 135 ss.

[15] Non esiste una nozione univoca di *Big Data*, ma la maggior parte degli studiosi è concorde nell'attribuire il primo tentativo di definizione a Doug Laney, per il quale si tratta di «*high-volume, high-velocity and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization*» (D. LANEY, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, META Group Report, 2001, file 949; cfr. anche M.A. BAYER e D. LANEY, *The Importance of "Big Data": A Definition*, Analysis Report ID, 2012). Si veda anche la definizione contenuta nel rapporto finale dell'Indagine Conoscitiva sui Big data condotta congiuntamente dall'Autorità Garante della Concorrenza e del Mercato, dall'Autorità per le garanzie nelle telecomunicazioni e dal Garante per la protezione dei dati personali, pubblicato nel febbraio 2020, ove, riprendendo la nozione di Big data di cui alla *Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big data per i diritti fondamentali*, si afferma che «con la locuzione Big data si fa riferimento, in prima approssimazione (nell'assenza di definizioni normativamente vincolanti), alla raccolta, all'analisi e all'accumulo di ingenti quantità di dati, tra i quali possono essere ricompresi dati di natura personale (nell'accezione fornita dall'art. 4 del Regolamento GDPR), in ipotesi provenienti anche da fonti diverse. La natura massiva delle operazioni di trattamento reca con sé la necessità che tali insiemi di informazioni (sia memorizzate, sia in streaming) siano oggetto di trattamento automatizzato, mediante algoritmi informatici e altre tecniche avanzate, al fine di individuare correlazioni di natura (per lo più) probabilistica, tendenze e/o modelli». Sul tema cfr. anche B. BROWN, J. BUGHIN, A. HUNG BYERS, M. CHUI, R. DOBBS, J. MANYIKA, C. ROXBURGH, *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, Washington, 2011 (McKinsey Global Institute), V. MAYER SCHONBERGER e K. CUKIER, *Big Data*, Milano, 2013; H. VARIAN, *Big Data: New Tricks for Econometrics*, in *Journal of Economic Perspectives*, 28, 2014, 3 ss.; A. DE MAURO, M. GRECO e M. GRIMALDI, *A formal definition of Big Data based on its essential features*, in Library Review, 2016, 65(3), 122 ss.; A. GIANNACCARI, *La storia dei Big Data, tra riflessioni teoriche e primi casi applicativi*, in *Merc. conc. Reg.*, 2017, 307 ss.; M. DEL MASTRO e A. NICITA, *Big Data. Come stanno cambiando il nostro mondo*, Bologna, 2019.

[16] La più recente definizione di intelligenza artificiale è fornita dall'art. 3 del Regolamento 2024/1689/UE, del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza (c.d. *AI Act*), secondo cui un sistema di IA è «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali». Per alcune riflessioni sulla definizione di intelligenza artificiale svolte da informatici, si vedano i contributi di M. GABBRIELLI, *Dalla logica al Deep Learning: una breve riflessione sull'intelligenza artificiale*, 21 ss.; di R. ROVATTI, *Il processo di apprendimento algoritmico e le applicazioni nel settore legale*, 31 ss., nonché di L. TOMASSINI, *L'intelligenza artificiale: quali prospettive?*, 43 ss., contenuti nel volume AA.VV., *Lezioni di diritto dell'intelligenza artificiale*, a cura di U. RUFFOLO, Torino, 2021. La letteratura giuridica sull'intelligenza artificiale ha comunque oramai acquisito una sua autonomia, potendosi segnalare, tra gli altri, nella dottrina interna, gli studi pionieristici di G. SARTOR, *Intelligenza artificiale diritto. Un'introduzione*, Milano, 1996; A. SANTOSUOSSO, *Intelligenza artificiale e diritto*, Milano, 2020; G. ALPA, *L'intelligenza Artificiale. Il contesto giuridico*, Modena, 2021; nonché i contributi contenuti in AA.VV., *Intelligenza artificiale e diritto*, numero monografico a cura di E. GABRIELLI e U. RUFFOLO, in *Giur. it.*, 2019.; AA.VV., *Diritto e intelligenza artificiale*, a cura di G. ALPA, Pisa, 2020. Più in generale, sull'incidenza delle nuove tecnologie sui rapporti di diritto privato e di diritto pubblico, già S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, ora riedito a cura di G. ALPA, G. RESTA, M.R. MARELLA, Bologna, 2021.

Come si vedrà, infatti, l'adozione di questo tipo di sistemi, pur potendo presentare rilevanti vantaggi, non è completamente esente da rischi, in termini di possibili ricadute negative sui consumatori e sulla stabilità del sistema.

Ebbene, in questo contesto, oltre alle indicazioni fornite in alcuni atti delle autorità di vigilanza nazionali ed europee[17], finiscono per assumere un rilievo centrale proprio le regole e i principi generali sanciti dal GDPR, i quali, però, non sembrano sufficienti a disciplinare adeguatamente il fenomeno e ad assicurare una piena tutela a chi richiede il prestito.

Una più compiuta analisi delle nuove tecniche di *credit scoring* rivela, infatti, l'esistenza di alcune carenze nella disciplina sul trattamento dei dati personali, in particolare per ciò che concerne i processi decisionali automatizzati, che la rendono inidonea a far fronte ai pericoli derivanti dall'utilizzo dei sistemi di intelligenza artificiale[18].

Le criticità riscontrate sembrano però essere state affrontate efficacemente da due recenti provvedimenti dell'Unione europea: uno è la Direttiva UE n. 2225/2023 sul credito al consumo, contenente regole specifiche sui sistemi di valutazione del merito creditizio; l'altro è il c.d. *Artificial Intelligence Act*, recante invece una disciplina generale volta a regolare, in modo completo e organico, l'immissione nel mercato e l'utilizzo di qualsiasi sistema di intelligenza artificiale.

Con queste premesse, nelle pagine che seguono, si procederà in primo luogo ad analizzare brevemente le diverse tecniche mediante le quali è oggi possibile svolgere la valutazione del merito creditizio. In un secondo momento, invece, si valuterà in che modo le regole contenute nel GDPR incidono sul *credit scoring* e, più in generale, quale sia la loro efficacia in relazione ai sistemi di intelligenza artificiale più complessi. Infine, si darà conto delle novità introdotte dai provvedimenti da ultimo menzionati.

3. Sistemi di valutazione del merito creditizio tradizionali e innovativi.

L'attività di valutazione del merito di credito del consumatore, a cui in passato il legislatore ha riservato scarsa attenzione[19], è da qualche tempo

---

L'impatto dello sviluppo tecnologico sul diritto è stato affrontato di recente anche da G. LEMME, *La transizione giuridica. La crisi del diritto di fronte alla sfida tecnologica*, Torino, 2023.

[17] Di cui si dà più ampio conto in C.A. VALENZA, *Modelli innovativi di valutazione del merito creditizio: contesto normativo e prospettive di regolamentazione*, in AA.VV., *Intelligenza artificiale e rapporti bancari. Umano e non umano nelle relazioni tra intermediari e clienti*, a cura di M. PROTO, Pisa, 2024, 107 ss.

[18] Sul punto, più in generale, cfr. G. SARTOR, *The impact of the general data protection regulation on artificial intelligence* (European Parliament, Directorate-General for Parliamentary Research Services), 2020, 79 ss., consultabile al sito: https://data.europa.eu/doi/10.2861/293; G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *federalismi.it*, 2020, XVI, 266 ss.; A. FEDI, *Big Data and AI: an issue for general law and data protection*, in *Jus civile*, 2020, 169 ss.; C. TABARRINI, *Comprendere la "Big Mind". Il GDPR sana il divario di intelligibilità uomo-macchina?*, in *Dir. inf.*, 2019, 555 ss.; G. FINOCCHIARO, *Considerazioni su intelligenza artificiale e protezione dei dati personali*, in *XXVI lezioni di Diritto dell'Intelligenza Artificiale*, *cit.*, 331 ss.; T.E. FROSINI; *La Privacy nell'era dell'intelligenza artificiale*, in *DPCE Online*, v. 51, n. 1, apr. 2022, consultabile al sito http://dx.doi.org/10.57660/dpceonline.2022.1572; T.M. UBERTAZZI, *Privacy e Intelligenza Artificiale*, in *Comparazione e diritto civile*, 2023, 955 ss..

[19] Lo rilevano anche L. AMMANNATI e G.L. GRECO, *Piattaforme digitali, algoritmi e* big data*: il caso del* credit scoring, in *Riv. trim. dir. econ.*, 2021, 305, per i quali per molto tempo «il legislatore e l'autorità di vigilanza italiana si sono preoccupati di regolare il fine (la sana e prudente gestione dell'ente, nella specifica accezione del rischio di credito) piuttosto che il mezzo (la valutazione del merito creditizio)». La dottrina, invece,

imposta e disciplinata dall'art. 124 *bis* del T.u.b.[20], dettato in materia di credito al consumo, e dall'art. 120 *undecies* del T.u.b.[21], specifico per il credito immobiliare ai consumatori, e consiste in un giudizio prognostico sulla capacità del soggetto finanziato di restituire la somma ricevuta nei termini pattuiti, espresso attraverso l'assegnazione al cliente di un punteggio individuale all'interno di una scala di valori predeterminata.

Tale attività, normalmente collocata nella fase precontrattuale, è volta a stabilire sia *se* il credito può essere concesso, sia, eventualmente, *a quali condizioni*.

In linea generale, gli elementi fondamentali per il calcolo dello *score* sono due: i dati e le modalità con cui essi vengono processati.

I sistemi di valutazione del merito creditizio tradizionali, tutt'oggi utilizzati dagli intermediari creditizi vigilati, si basano generalmente su dati e informazioni relativi al profilo economico-finanziario del consumatore, quali ad esempio l'identità, la passata abilità di ripagare i debiti, il reddito, la movimentazione dei conti, ecc. Si tratta, in altre parole, di c.d. *Hard-Data*, ossia di dati oggettivi, facilmente verificabili e traducibili in un indice numerico, che possono essere acquisiti direttamente dal richiedente, nonché da fonti interne all'intermediario o attraverso le c.d. banche dati creditizie, *in primis* le centrali dei rischi pubbliche.

L'elaborazione di tali dati viene invece fatta mediante il ricorso a modelli tramite i quali si attribuisce a ciascun singolo richiedente un punteggio che, sulla base di una correlazione statistica, esprime in termini predittivi il profilo di rischio, l'affidabilità e la puntualità nei pagamenti.

I sistemi di valutazione tradizionali si basano dunque su algoritmi semplici, il cui schema operativo[22] è determinato in tutto o in parte dagli operatori al momento della creazione per impiegare un numero assai esiguo di dati[23].

---

segnala da tempo la rilevanza di tale fase dell'attività: a es., con particolare riferimento al passaggio «dal prototipo classico "*originate-to-hold*" … alla differente pratica "*originate-to-distribute*"», v. P. GAGGERO, *La trasparenza del contratto. Per un'analisi dei rapporti di intermediazione creditizia*, Milano, 2011, 127 ss. Cfr. pure G. CARRIERO, *Credito ai consumatori*, nel *Testo unico bancario. Commentario. Addenda di aggiornamento ai d.lgs. 141/2010 e 218/2010*, a cura di M. PORZIO, F. BELLI, G. LOSAPPIO, M RISPOLI FARINA e V. SANTORO, Milano, 2011, 93 ss.; R. DE CHIARA, *Verifica del merito creditizio*, nel *Commentario al Testo unico delle leggi in materia bancaria e creditizia*, diretto da F. CAPRIGLIONE, con la collaborazione di M. PELLEGRINI, M. SEPE e V. TROIANO, t. III, Padova, 2012, 1869 ss.; e, a partire dall'accordo sul capitale regolamentare c.d. "Basilea II", F. CAPRIGLIONE, *Crisi a confronto (1929 e 2009). Il caso italiano*, Padova, 2010, 132 ss.; G. BOCCUZZI, *La funzione di* compliance*: il presidio dei rischi aziendali e l'evoluzione della normativa Basilea 2 e Mifid*, in *Bancaria*, 2008, n. 2, 34 ss.; e E. PAOLILLO, *Gestione del capitale bancario e riflessi nei rapporti banca-impresa*, *ivi*, 2002, n. 9, 22 ss. *Amplius*, in tema, M. ONADO, *La gestione del rischio di credito nelle banche europee*, Milano, 1995, e A. MALINCONICO, *Rischio di credito e modern portfolio theory. Modelli innovativi per la gestione dei prestiti*, Milano, 2000.

[20] Che traspone in modo pressoché letterale l'art. 8. della Direttiva 2008/48/CE.

[21] Che dà attuazione a quanto previsto dagli artt. 18-29 8 della Direttiva 3014/17/UE.

[22] Si tratta, in sostanza, di modelli a regressione lineare, che prevedono l'utilizzo di metodologie prettamente statistiche. In tale modo, viene modellata una relazione tra una variabile *target* di cui si voglia prevedere l'esito (normalmente l'insolvenza di un debitore) e altre variabili, i c.d. "predittori", ritenute come statisticamente esplicative.

[23] Tra i sistemi di valutazione tradizionali, è assai noto il *FICO Score*, elaborato da uno storico player statunitense di servizi di data analisi, che impiega una serie di dati di tipo *hard*, raggruppati in 5 categorie che "pesano" diversamente ai fini dell'attribuzione del punteggio: dati sulla storia creditizia del cliente (35%), dati relativi al reddito (30%); dati sulla lunghezza della storia creditizia (15%), dati sulla tipologia di prestiti già richiesti (10%); dati sul nuovo credito per cui è presentata la richiesta (10%). Queste informazioni sono reperibili al seguente indirizzo: https://www.myfico.com/credit-education/whats-in-your-credit-score. Tra gli altri, discorre di tale sistema N. CULLERTON, *Behavioral Credit Scoring*, in *Georgetown Law Journal*, 2013, 807 ss.

Come si è avuto già modo di anticipare, l'innovazione tecnologica, che ha profondamente interessato e interessa in misura crescente anche il settore bancario e finanziario[24], ha finito per incidere pure sull'attività di valutazione del merito creditizio, aprendo la strada a nuove possibilità, sia per quanto riguarda i dati utilizzabili, sia per ciò che concerne le metodologie per processarli

In particolare, l'emersione di nuovi modelli di *credit scoring* è strettamente legata, da un lato, alla già accennata disponibilità dei c.d. *Big Data*, ossia di grandi *dataset* contenenti un elevato volume di informazioni anche non strutturate e, dall'altro, alla diffusione di tecniche sempre più sofisticate di analisi dei dati.

Così, muovendo dal presupposto che «*all data is a credit data*»[25], i nuovi sistemi di valutazione del merito creditizio considerano una serie di dati molto più vasta di quella generalmente analizzata dai modelli tradizionali, assumendo rilievo anche i dati c.d. "alternativi", i quali, si noti, non sono né univoci né numerici.

Tali dati possono essere acquisiti direttamente dal richiedente, ad esempio tramite la compilazione di formulari *on-line*, o in modo indiretto, mediante l'osservazione dell'attività *on-line* ed *off-line* dello stesso (si pensi, ad esempio, ai dati relativi alla navigazione sul web, che possono rivelare abitudini, propensioni di acquisto o altre preferenze personali, o, ancora, a quelli relativi all'interazione sulle piattaforme *social*). Inoltre, altri dati utili per il *credit scoring* possono essere ottenuti da soggetti terzi specializzati nella formazione, vendita e detenzione di profili individuali, che vengono creati attraverso la rielaborazione dei comportamenti e delle informazioni relative ai singoli soggetti.

I modelli più innovativi di *credit scoring* sono dunque in grado di coniugare due categorie di dati: i cd. *Hard-Data*, che si riferiscono al profilo economico e

---

[24] Sull'argomento cfr., *ex multis*, EBA, *Discussion Paper on the EBA's approach to financial technology (FinTech)*, EBA/DP/2017/02, 4 agosto 2017; FSB, *Artificial intelligence and machine learning in financial services*, novembre 2017; BANCA D'ITALIA, *Indagine conoscitiva sull'adozione delle innovazioni tecnologiche applicate ai servizi finanziari*, dicembre 2017; D. MILANESI, *A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States*, TTLF Working Papers n. 29, 2017; C. SCHENA, A. TANDA, C. ARLOTTA e G. POTENZA, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, in *Quaderni Fintech*, Roma, 2018, AA.VV., *Introduzione ai principi giuridici di un mercato unico tecnologico di servizi finanziari*, a cura di M.T. PARACAMPO, Torino, 2017; AA.VV., *Fintech: diritto tecnologia e finanza*, a cura di R. LENER, in *I Quaderni di Minerva Bancaria*, Roma, 2018; AA.VV., *I diversi settori del Fintech. Problemi e prospettive,* a cura di E. CORAPI e R. LENER, Milano, 2019; AA.VV., *La via italiana al fintech: strategie ed esperienze nel settore bancario e finanziario*, a cura di M. GIORGINO, Milano, 2019; AA.VV., *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, a cura di G. FINOCCHIARO e V. FALCE, Bologna, 2019; C. SCHENA, V. STEFANELLI e V. BOSCIA, *Digital banking e FinTech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato*, Roma, 2020; AA.VV., *Banche, intermediari e fintech. Nuovi strumenti digitali in ambito finanziario*, a cura di G. CASSANO, F. DI CIOMMO e M. RUBINO DE RITIS, Milano, 2021; AA.VV., Financial innovation *tra disintermediazione e mercato*, a cura di V. FALCE, Torino, 2021; AA.VV., *Fintech, Smart Technologies e governance dei mercati. L'impatto del digitale sul settore bancario, finanziario e sulla regolazione pubblica*, a cura di A. NUZZO, Roma, 2021; A. NATALE, *Fintech. I confini dell'innovazione nella finanza*, Milano, 2022; AA.VV., *La finanza nell'età degli algoritmi*, a cura di L. AMMANNATI e A. CANEPA, Torino, 2023; AA.VV., *Intelligenza artificiale e rapporti bancari. Umano e non umano nelle relazioni tra intermediari e clienti*, a cura di M. PROTO, *cit.* Si vedano poi, tra gli altri, i contributi di F. CAPRIGLIONE, *Industria finanziaria, innovazione tecnologica, mercato*, in *Riv. trim. dir. econ.*, 2019, 372 ss.; ID., *Diritto ed economia. La sfida dell'Intelligenza Artificiale*, *ivi*, 2021, supplemento al fasc. 3, 4 ss.; G. ALPA, *Fintech: un laboratorio per i giuristi*, in *Contr. impr.*, 2019, 377 ss.; M. PELLEGRINI, *L'intelligenza artificiale nell'organizzazione bancaria: quali sfide per il regolatore?*, in *Riv. trim. dir. econ.*, 2021, 422 ss.

[25] L'espressione è stata utilizzata nel 2021 da Douglas Merrill (ex CIO Google) durante un'intervista al New York Times. Cfr. anche *Big data lends new Zest to banks' credit judgments*, Financial Times, 23 giugno 2014.

finanziario del richiedente e che sono già ora facilmente ricavabili dalle banche dati utilizzate dagli intermediari; e i c.d. *Soft-Data*, che vengono invece estratti dalle tracce digitali extra-finanziarie[26].

Come è stato evidenziato in uno studio promosso dalla Banca d'Italia, nella valutazione del merito di credito si è dunque verificata, a livello globale, «una graduale estensione delle fonti di dati utilizzate […]: dai dati finanziari strutturati (indicatori patrimoniali ed economico-finanziari, sull'andamento dei conti e dei pagamenti, di mercato) a dati non finanziari strutturati (dati di tipo socio-demografico ottenuti anche da fonti terze), dati non strutturati finanziari (analisi delle informazioni transazionali e di quelle derivate da open banking) e dati non strutturati non finanziari (dati di navigazione, digital footprint, informazioni conferite sui social network)»[27].

L'elaborazione di una così grande quantità di informazioni disomogenee è resa possibile dai nuovi sistemi informatici, che si basano su algoritmi particolarmente complessi e, segnatamente, su tecniche di c.d. intelligenza artificiale e di *machine learning* in particolare.

Sono note, ad esempio, le potenzialità del sistema brevettato da un'ex *startup* di *Fintech credit*[28], il cui *software* proprietario fa uso del *machine learning* per processare ed analizzare un'ingente quantità di dati, combinando informazioni tradizionali con altre che sono ricavate dall'attività *on-line* e *off-line* degli utenti. Ad essere presi considerazione, in particolare, sono, tra l'altro, l'attività di ricerca *web*, il tempo impiegato per leggere i termini e le condizioni di utilizzo della piattaforma[29], i luoghi e le modalità delle abitudini di spesa[30], i dati GPS, le informazioni ricavabili *online* tramite le tecniche di *web crawling* e *web scraping*, nonché le attività compiute sui *social network*[31].

Si ritiene, generalmente, che l'utilizzo di sistemi di questo tipo, che ha consentito l'accesso al mercato del credito anche a intermediari non tradizionali (*in primis*, le piattaforme di *lending*), privi del patrimonio

---

[26] M. RABITTI, Credit scoring *via* machine learning *e prestito responsabile*, in *Riv. dir. banc.*, 2023, 182. Sul punto, ampiamente, A. DAVOLA, *Algoritmi decisionali e trasparenza bancaria*, Torino, 2020, 136 SS.

[27] AA.VV., *Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano*, in *Questioni di economia e finanza* (Banca d'Italia), n. 721, 2022, 15. Per un elenco analitico di dati (strutturati e non strutturati) che sono rilasciati in ambito digitale e trattati nella prestazione di servizi finanziari on line si può fare riferimento all'enumerazione contenuta in EBA, *Discussion Paper on innovative uses of consumer data by financial institutions*, DP/2016/01, 4 giugno 2016, 9 ss.

[28] Ci si riferisce a *ZestFinance* (oggi *Zest Ai*), una tra le prime e più note *startup* di *Fintech credit* che ha oramai cessato la propria attività creditizia per concentrarsi esclusivamente sullo sviluppo e la cessione in licenza del *software* proprietario. Si veda, al riguardo, l'analisi condotta da ROBINSON+YU, *Knowing the Score: New Data, Underwriting, and Marketing in the Consumer Credit Marketplace. A Guide for Financial Inclusion Stakeholders*, Ford Foundation, 2014, ove si dà conto anche di altri sistemi di *credit scoring* dotati di caratteristiche simili.

[29] Si ritiene, infatti, che il tempo impiegato da un soggetto per leggere i termini e le condizioni di utilizzo della piattaforma possa essere indicativo del livello di responsabilità del richiedente. Sul punto, si veda l'articolo di Q. HARDY, *Big Data for the Poor*, sul New York Times del 5 luglio 2012, reperibile al sito: https://archive.nytimes.com/bits.blogs.nytimes.com/2012/07/05/big-data-for-the-poor/.

[30] M. HURLEY e J. ADEBAYO, *Credit Scoring in the Era of Big Data*, in *18 Yale J.L. & Tech.*, 148 (2016), 165. Sul punto, efficacemente Q. HARDY, *Big Data for the Poor*, *cit.*, «*paying half of one's income [on rent] in an expensive city like San Francisco might be a sign of conventional spending, while paying the same amount in cheaper Fresno could indicate profligacy*».

[31] J. JIA-XI, *Beyond Free Markets and Consumer Autonomy: Rethinking Consumer Financial Protection in the Age of Artificial Intelligence*, in *13 NYU Journal of Intellectual Property & Entertainment Law*, 56(2023), 87: «*The number of social media connections a person has, the frequency that she deactivates an account, and the number of connections she unfriends are used as proxies to measure risk-taking tendencies*».

informativo delle banche e tendenzialmente esclusi dalle centrali dei rischi pubbliche[32], rechi con sé significativi vantaggi: anzitutto, per i clienti, in termini di inclusione al credito, in quanto permetterebbe di ampliare la platea dei soggetti finanziabili estendendola a includere pure soggetti diversi da quelli c.d. bancabili, ammettendo al credito anche coloro che sono privi di una storia creditizia o che comunque sarebbero esclusi secondo i sistemi di valutazione del merito creditizio tradizionali[33]; ma anche per gli intermediari, che avrebbero la possibilità di operare una maggiore distinzione granulare della clientela e di effettuare una migliore selezione dei soggetti cui concedere il credito, oltre che di adeguare i servizi alle specifiche caratteristiche del singolo cliente[34].

Al contempo, però, è stato da più parti osservato che l'adozione di tali sistemi non è esente da rischi, i quali derivano soprattutto dalla possibilità di utilizzare anche dati non strutturati ed eterogenei, compresi quelli non direttamente correlati alla situazione finanziaria del richiedente ma relativi piuttosto ad altri aspetti della sua vita privata[35].

La possibilità di attingere a un patrimonio informativo così ampio, infatti, non si traduce automaticamente in una valutazione più accurata del merito creditizio, essendo necessaria l'implementazione di sistemi che siano in grado, da un lato, di individuare e selezionare soltanto quei dati realmente utili a definire il livello di affidabilità del richiedente e la sua capacità di restituzione e, dall'altro, di elaborare ed analizzare tali dati correttamente.

In questo senso, non è da escludere che l'utilizzo delle nuove tecniche di *credit scoring* possa condurre, talvolta, a esiti errati, ove faccia difetto la correttezza dei dati o del procedimento algoritmico che li ha elaborati. Di qui, dunque, il rischio di addivenire a "nuove" esclusioni o a forme di discriminazione, anche involontarie, generate da modelli non governati di cui non sono note tutte le determinanti rilevanti ai fini della decisione[36].

---

[32] In questa prospettiva, cfr. L. MODICA, *Peer to Consumer Lending*, in *Osserv. dir. civ. comm.*, 2022, 81 ss.; A. SCIARRONE ALIBRANDI, G. BORELLO, R.G. FERRETTI, F. LENOCI, E. MACCHIAVELLO, F. MATTASSOGLIO, F. PANISI, *Marketplace lending. Verso nuove forme di intermediazione finanziaria?*, *Quaderno FinTech* n. 5 – luglio 2019; G. BIFERALI, Big data *e valutazione del merito creditizio per l'accesso al* peer to peer lending, in *Dir. inf.*, 2018, 487 ss. Quanto al sistema bancario, la ricerca può muovere da M. PELLEGRINI, *Il diritto cybernetico nei riflessi sulla materia bancaria e finanziaria,* in AA.VV., Liber amicorum *Guido Alpa*, a cura di F. CAPRIGLIONE, Milano, 2019, p. 351 ss.

[33] Cfr. G. MATTARELLA, Big *Data e accesso al credito degli immigrati: discriminazioni algoritmiche e tutela del consumatore*, in *Giur. comm.*, 2020, 696 ss.; ID. *L'inclusione finanziaria degli immigrati. La tutela del consumatore vulnerabile nei servizi bancari*, Torino, 2021, 11, ove si esalta il ruolo dell'inclusione *lato sensu* finanziaria quale presupposto dell'inclusione sociale.

[34] F. MATTASSOGLIO, *La valutazione "innovativa" del merito creditizio del consumatore e le sfide per il regolatore*, *cit.*, 704 ss.

[35] Per una più approfondita analisi dei rischi e dei benefici connessi all'adozione dei nuovi sistemi di valutazione del merito creditizio si veda F. MATTASSOGLIO, *La valutazione "innovativa" del merito creditizio del consumatore e le sfide per il regolatore*, in *Dir. banc. merc. fin.*, 2020, 187 ss., spec. 200 ss. Più di recente, sul tema, M. RABITTI, Credit scoring *via* machine learning *e prestito responsabile*, in *Riv. dir. banc.*, 2023, 175 ss. Nella dottrina straniera, oltre ai contributi già richiamati, si veda, in prospettiva critica, D.K. CITRON e F. PASQUALE, *The Scored Society: Due Process for Automated Predictions*, in *Washington Law Review*, 2014, vol. 89, 1 ss.

[36] Si veda ancora G. MATTARELLA, Big *Data e accesso al credito degli immigrati: discriminazioni algoritmiche e tutela del consumatore*, *cit.* 704 ss. Più di recente, sul tema, M. RABITTI, *Discriminazioni tecnologiche e* Fin-tech, in *Riv. dir. impr.*, 2023, 467 ss. In arg. anche L. AMMANNATI, G.L. GRECO, *Il credit scoring "intelligente": esperienze, rischi e nuove regole*, in *Riv. dir. banc.*, 2023, 471 ss.; F. MATTASSOGLIO, *La valutazione "innovativa" del merito creditizio del consumatore e le sfide per il regolatore*, *cit.*, 205 ss. Nella dottrina straniera, K. LANGENBUCHER, *Consumer Credit in The Age of AI – Beyond Anti-Discrimination Law* (December 9, 2022), SAFE Working Paper No. 369, consultabile al sito: https://ssrn.com/abstract=429826; C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, 2016; S. BAROCAS, SELBST, *Big Data's*

4. Sistemi di valutazione del merito creditizio e disciplina sul trattamento dei dati personali.

Nello scenario appena delineato, le indicazioni più significative sui dati utilizzabili ai fini del *credit scoring* e sulle modalità con cui questi possono essere processati si ricavano, come si è già anticipato, dal Regolamento 2016/679/UE (GDPR), il quale contiene una serie di prescrizioni di carattere generale destinate a trovare applicazione ogniqualvolta l'attività praticata implichi il trattamento di dati personali e, dunque, anche in caso di valutazione del merito creditizio.

Anzitutto, come noto, il Regolamento stabilisce che i dati personali devono essere sempre trattati in modo «lecito, corretto e trasparente nei confronti dell'interessato» (art. 5, comma 1, lett. a), prevedendo di norma il consenso del titolare al loro utilizzo (art. 6, comma 1, lett. a), sebbene il legittimo interesse del titolare sia di per sé idoneo a rendere il trattamento lecito (art. 5, comma 1, lett. f). In ogni caso, in applicazione del GDPR, l'intermediario è tenuto ad avvisare il consumatore del fatto che ogni indicazione da lui fornita potrà essere utilizzata ai fini della valutazione del proprio merito creditizio.

Di particolare rilievo sono poi le previsioni relative ai dati che possono essere trattati, atteso che, in applicazione del Regolamento, ciascun finanziatore dovrebbe raccogliere e utilizzare soltanto quei dati dei clienti ritenuti «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (art. 5, comma 1, lett. c). Tali dati, inoltre, dovrebbero in ogni caso essere «esatti» e «aggiornati» (art. 5, comma 1, lett. d) e conservati «in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità» (art. 5, comma 1, lett. e). Si noti, peraltro, che, in linea di principio, la possibilità di trattare dati personali "particolari", come ad esempio quelli relativi alla salute o all'orientamento sessuale o quelli che rivelano l'origine razziale o etnica, è esclusa, sebbene tale divieto sia destinato a cadere in presenza di un esplicito consenso dell'interessato.

Sulle metodologie utilizzabili per processare i dati raccolti assumono, invece, rilevanza soprattutto le disposizioni dettate con riferimento ai processi decisionali automatizzati, quali sono, per l'appunto, i moderni sistemi di *credit scoring*.

Anzitutto, in un'ottica di trasparenza, l'art. 13 del GDPR impone di rendere edotto (*ex ante*) il soggetto interessato dell'esistenza di un processo decisionale automatizzato, fornendo allo stesso tempo informazioni significative sulla logica utilizzata dall'algoritmo, nonché sull'importanza del trattamento e sulle conseguenze che da esso possono derivare[37].

Disparate Impact, in *California Law Review*, vol. 104, n. 3, 671 ss.; C. HAVARD, *"On the Take": The Black Box of Credit Scoring and Mortgage Discrimination*, in *Boston University Public Interest Law Journal*, vol. 20, n. 2, 241 ss.

[37] In questo senso anche l'art. 9 della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (c.d. Convenzione 108+), come modificata dal Protocollo adottato nel 2018 e ratificato dall'Italia nel 2021. Al riguardo, risultano

Il successivo art. 22 prevede poi ulteriori garanzie in relazione ai trattamenti *interamente* automatizzati, sancendo, in particolare, il diritto dell'interessato a non essere sottoposto a una decisione basata su processi che non prevedano il coinvolgimento dell'uomo qualora tale decisione produca effetti giuridici che lo riguardano o incida significativamente sulla sua persona[38].

I sistemi innovativi di valutazione del merito creditizio rientrano, come evidente, nell'ambito di applicazione della disposizione appena menzionata. Il che, peraltro, è stato confermato di recente anche dalla Corte di giustizia[39], la quale ha avuto modo di precisare che il divieto stabilito dall'art. 22 comprende anche quei casi in cui, come accade di frequente, l'attribuzione del *credit scoring* è affidata dall'ente finanziatore a un soggetto terzo[40].

Ciò detto, occorre tuttavia evidenziare che il divieto in discorso subisce una serie di eccezioni che finiscono per renderlo nei fatti una mera declamazione di principio, non trovando applicazione in caso di consenso esplicito dell'interessato o quando la decisione sia necessaria per la conclusione o l'esecuzione di un contratto[41]. Circostanze che potrebbero venire in rilievo proprio in relazione al *credit scoring* automatizzato, in primo luogo per quanto riguarda il consenso dell'interessato[42] e, poi, per la possibilità di ritenere tale

---

significative pure le considerazioni contenute al paragrafo 77 del rapporto esplicativo di tale Convenzione, secondo cui: «gli interessati hanno il diritto di ottenere conoscenza del ragionamento alla base del trattamento dei dati, comprese le conseguenze di tale ragionamento e le conclusioni che ne possono essere state tratte in particolare nel caso di utilizzo di algoritmi al fine dell'adozione di una decisione automatizzata, specialmente nel contesto della profilazione. Per esempio, nel caso di un sistema di valutazione dell'affidabilità creditizia, i mutuatari hanno il diritto di conoscere la logica utilizzata nel trattamento dei loro dati che conduce alla concessione o al rifiuto del prestito, invece di essere semplicemente informati della decisione stessa. La comprensione di questi elementi contribuisce all'esercizio effettivo di altre garanzie fondamentali, come il diritto di opposizione e il diritto di ricorso dinanzi a un'autorità competente».

[38] Così anche l'art. 9 della Convenzione 108+ poc'anzi citata.

[39] Corte di giustizia, 7 dicembre 2023, *Schufa Holding (Scoring)*, causa C-634/21, su cui si vedano i commenti di F. D'Orazio, *Il "credit scoring" e l'art. 22 del GDPR al vaglio della Corte di giustizia,* in *Nuova giur. civ. comm.*, 2024, 410 ss. E. Falletti, *Alcune riflessioni sull'applicabilità dell'art. 22 GDPR in materia di "scoring" creditizio*, in *Dir. inf.*, 2024, 110 ss. Sul punto anche M. Rabitti, *Discriminazioni tecnologiche e* Fin-tech, *cit.*, 478 ss.

[40] La Corte, infatti, ha affermato che il termine "decisione" contenuto nell'art. 22 del GDPR deve essere inteso in senso ampio, in modo da includere tutte le tipologie di atti che, in vario modo, possono incidere sulla persona interessata. Di conseguenza, anche l'attribuzione dello *scoring* effettuata dal soggetto terzo, da cui sostanzialmente dipende la decisione finale dell'ente finanziatore, deve essere considerata come decisione e non come mero "atto preparatorio", evitando in tal modo l'elusione delle tutele previste dal GDPR in tutti quei casi, assai frequenti, in cui la decisione coinvolga tre attori (la banca, la società a cui è affidata la valutazione del merito di credito e il soggetto che richiede il prestito). In questo senso, pertanto, la Corte ha stabilito che «il calcolo automatizzato, da parte di una società che fornisce informazioni commerciali, di un tasso di probabilità basato su dati personali relativi a una persona e riguardanti la capacità di quest'ultima di onorare in futuro gli impegni di pagamento costituisce un "processo decisionale automatizzato relativo alle persone fisiche", ai sensi di tale disposizione, qualora da tale tasso di probabilità dipenda in modo decisivo la stipula, l'esecuzione o la cessazione di un rapporto contrattuale con tale persona da parte di un terzo, al quale è comunicato tale tasso di probabilità».

[41] Un'ulteriore eccezione è rappresentata dall'ipotesi in cui la decisione interamente automatizzata sia autorizzata dal diritto dell'Unione o di uno Stato membro, con la previsione di misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

[42] Sul punto si vedano però le attente riflessioni di D. Imbruglia, *Le presunzioni delle macchine e il consenso dell'interessato*, in *Riv. trim. dir. proc. civ.*, 2023, 941 ss., il quale critica la scelta del legislatore di includere il consenso, sia pure esplicito, dell'interessato tra le basi di giustificazione di una decisione interamente basata sull'*output* determinato dalla previsione automatizzata, in quanto lo strumento in discorso «non risponde[rebbe] al conflitto che tale tipo di tecnologia solleva con i princìpi indisponibili di non discriminazione e di razionalità della decisione personalmente rilevante». L'Autore, infatti, ritiene che il consenso dell'interessato sia idoneo a risolvere principalmente i problemi che si verificano allorquando la tecnologia "incontra" la personalità dei singoli (a es. la propria integrità fisica), non potendo invece essere adoperato qualora, come nel caso di specie, vengano in gioco interessi collettivi indisponibili, relativi alla

trattamento "necessario" per la conclusione del contratto di credito[43]; anche se, va detto, tale ultima possibilità sembra doversi escludersi[44], atteso che, dal punto di vista normativo, l'obbligo di cui all'art. 8. della Direttiva 2008/48/CE riguarda lo svolgimento, prima della conclusione di un contratto di credito, di un'attenta valutazione del merito creditizio e non anche l'automatizzazione di tale attività.

In ogni caso, in presenza di un trattamento automatizzato che rientri nelle eccezioni ora menzionate, il titolare del trattamento è tenuto ad adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato. In particolare, deve essere sempre garantito il diritto di ottenere l'intervento umano, di esprimere la propria opinione e, soprattutto, di contestare la decisione sfavorevole (art. 22, comma 3). E si tratta delle più importanti garanzie di cui potrebbe disporre chi richiede il prestito in caso di decisioni sul finanziamento adottate da sistemi automatizzati di *credit scoring* e ritenute ingiuste.

Le disposizioni contenute nell'art. 22 del GDPR vanno lette, peraltro, alla luce del considerando n. 71, il quale si riferisce ai trattamenti automatizzati prendendo come esempio proprio il caso della «domanda di credito online […] senza interventi umani». Segnatamente, in applicazione dei principi di correttezza e trasparenza, il considerando in discorso richiede agli intermediari bancari di utilizzare procedure matematiche o statistiche "appropriate" per la profilazione, e di adottare misure tecniche e organizzative "adeguate" al fine di consentire la rettifica dei dati inesatti e di impedire possibili effetti discriminatori[45].

---

necessità che il trattamento automatizzato risponda ai principi di razionalità e non discriminazione. Diversamente, per l'Autore, si finirebbe per «trasformare il consenso del singolo in una sorta di "patente illimitata" che lascia i princìpi caratterizzanti quel processo (di non discriminazione e di razionalità della decisione) senza tutela davanti ad atti assunti in palese contrasto» (944). In questa prospettiva, secondo l'Autore, l'interprete potrebbe escludere l'idoneità del consenso *ex* art. 22 a giustificare quelle decisioni che, in quanto basate su inferenze oscure e spurie, risultano in contrasto con i princìpi di non discriminazione e di razionalità della decisione attorno ai quali l'ordinamento articola quel procedimento. Non può non evidenziarsi come la figura del consenso dell'interessato nel trattamento dei dati personali riscontri da sempre un grande interesse da parte della dottrina, a partire da S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 45; ID., *La privacy tra individuo e collettività*, in ID., *Tecnologie e diritti*, *cit.*, 23; ID., *Protezione dei dati e circolazione delle informazioni*, *ivi*, 43. Più di recente, sul tema, A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in *Riv. trim. dir. proc. civ.*, 2022, 701.

[43] F. MATTASSOGLIO, *La valutazione "innovativa" del merito creditizio del consumatore e le sfide per il regolatore*, *cit.*, 211; F. BAGNI, *Uso degli algoritmi nel mercato del credito: dimensione nazionale ed europea*, in *Oss. fonti*, 2021, 915. Anche se, va detto, dal punto di vista normativo, l'obbligo di cui all'art. 18 della dir. 2014/17/UE riguarda lo svolgimento, prima della conclusione di un contratto di credito, di un'attenta valutazione del merito creditizio, e non anche l'automatizzazione di tale attività.

[44] Per lo meno fin quando la nozione di necessità sia interpretata in modo restrittivo. Infatti, anche la circostanza per la quale la profilazione riduca le possibilità di errore umano o consenta di prendere decisioni in tempi brevi o di migliorare l'efficienza non è ritenuta, da sola, condizione sufficiente per dimostrare che tale tipo di trattamento "automatizzato'" sia necessario per la conclusione o l'esecuzione del contratto d'investimento tra il cliente e l'intermediario: v. *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* emanate dal *Gruppo di lavoro Articolo 29 per la protezione dei dati* (17/IT WP 251 rev.01), 14. In questo senso, pertanto, deve ritenersi che, ad oggi, un rapporto di funzionalità necessaria sussiste solo tra la profilatura tradizionale non algoritmica e la conclusione del contratto di finanziamento.

[45] Il considerando, in particolare, fa riferimento a possibili discriminazioni «sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale».

Non va infine trascurato che la declinazione in concreto delle disposizioni contenute nel GDPR è agevolata dalle *Linee Guida sulla profilazione* emanate nel 2017 – e poi emendate nel 2018 – dal *Gruppo di lavoro Articolo 29 per la protezione dei dati* (WP29). Tale documento fa espresso riferimento in diversi passaggi all'attività di *rating* automatizzato degli istituti bancari, fornendo al contempo alcuni esempi pratici di profilazione conforme ai principi del Regolamento. Ad esempio, rispetto agli obblighi di informazione e trasparenza del titolare del trattamento poc'anzi richiamati, è specificato che la logica e i criteri sui quali si basa una decisione dovrebbero essere comunicati con un linguaggio semplice e che le informazioni fornite, pur non implicando la divulgazione dell'algoritmo, dovrebbero essere sufficientemente complete per comprendere appieno i motivi di tale decisione.

5. L'insufficienza della disciplina sul trattamento dei dati personali in relazione ai sistemi più evoluti di *credit scoring*.

La normativa sul trattamento dei dati personali prevede, dunque, una serie di regole particolarmente incisive cui gli intermediari devono necessariamente conformarsi ai fini dello svolgimento dell'attività di valutazione del merito creditizio.

Tuttavia, tali regole non appaiono sufficienti a garantire una piena tutela al consumatore che richiede il credito, lasciando eccessivo spazio all'*accountability* delle singole banche e non elidendo tutti i rischi che possono discendere dai trattamenti basati su *Big Data* e su sistemi di *machine learning* e *deep learning.*

Ciò che manca, in particolare, è l'espressa attribuzione all'interessato di un diritto alla spiegazione della decisione adottata (*ex post*)[46], il che rende possibile l'esistenza di sistemi che si configurano quali vere e proprie *black box*[47], il cui *output* non è spiegabile né interpretabile dall'uomo e dunque, in

[46] Per la verità, il diritto alla "spiegazione" dell'interessato è espressamente menzionato nel considerando n. 71 del GDPR, ove si afferma che: «[i]l trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una *spiegazione* della decisione conseguita dopo tale valutazione e di contestare la decisione». Epperò, come rilevano S. WACHTER, B. MITTELSTADT e L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *IDPL*, vol. 7, n. 2, 2017, 76 ss., è assai significativo che il riferimento al diritto alla spiegazione, originariamente inserito nella Proposta di Regolamento in una disposizione vincolante (nell'attuale art. 22), sia stato poi espunto dal testo sottoposto ad approvazione legislativa e relegato all'area dei considerando. Per una ricostruzione della genesi della disposizione, si veda anche C. DJEFFAL, *The Normative Potential of the European Rule on Automated Decisions: a New Reading for Art. 22 GDPR*, in *ZaöRV*, 80/2020, 847 ss. Secondo alcuni autori, per la verità, un diritto alla spiegazione potrebbe desumersi dall'art. 15 del GDPR sul diritto di accesso dell'interessato (E. TROISI, *Decisione algoritmica, black-box e AI etica: il diritto di accesso come diritto a ottenere una spiegazione*, in *Jus Civile*, 2022, 953 ss.) o comunque dal complessivo quadro normativo (G. CARAPEZZA FIGLIA, *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in *Pers. merc.*, 2023, 638 ss.); altri invece negano una tale interpretazione sulla base del dato letterale della disposizione, non essendovi piena sintonia tra la norma e il considerando n. 71 del Regolamento (S. WACHTER, B. MITTELSTADT e L. FLORIDI, *op. cit.*; G. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, *in Giur. it.*, 2019, 1675). Per un quadro generale sull'argomento v. anche E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della* black box society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *Leggi civ. comm.*, 2018, 1209 ss.

[47] F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge-Londra, 2015.

definitiva, neppure concretamente contestabile[48].

Non può non scorgersi in ciò un grave *vulnus* di tutela per l'interessato, soprattutto in considerazione della crescente diffusione di sistemi basati su algoritmi informatici che, seppur progettati e strutturati secondo determinati criteri, sono in grado di evolvere in modo autonomo con modalità tecniche ed esiti non del tutto prevedibili *a priori*[49].

Un'effettiva tutela dell'interessato richiederebbe, pertanto, di adottare un approccio sostanziale e non meramente formale per la *compliance* con la normativa sulla *privacy*, assicurando l'effettiva spiegabilità e interpretabilità delle decisioni fornite dai modelli. Il che vorrebbe dire, in concreto, vietare gli algoritmi che producono essi stessi criteri di inferenza non identificabili neppure dai programmatori o strutturati secondo logiche di natura non deterministica[50], i quali si comportano, per l'appunto, come delle *black box*[51]. Solo in questo modo, infatti, può essere garantita la possibilità di contestare le modalità con cui la valutazione viene condotta, espressamente prevista dal GDPR[52].

Deve rilevarsi, inoltre, che le regole e i principi fondamentali stabiliti dal Regolamento lasciano aperti alcuni dubbi anche sulle tipologie di dati che possono essere utilizzati ai fini dello *scoring*.

In particolare, se certamente risolutiva è la previsione che esclude il ricorso ai dati "particolari", in quanto facilmente discriminatori, o quella relativa alla possibilità di rettificare i dati erronei, non è invece semplice comprendere in che modo debba darsi attuazione ai principi di minimizzazione e pertinenza, atteso che in astratto (quasi) qualsiasi dato relativo al cliente, in quanto indicativo di un comportamento, può essere utilizzato per valutarne l'affidabilità. Il che sembra lasciare aperta la possibilità di prendere in considerazione dati non strutturati e non finanziari, come ad esempio i dati di navigazione, *digital footprint*, e le informazioni conferite sui *social network*[53], la cui qualità non è assicurata da alcuna fase di verifica o validazione e la cui capacità predittiva è tutt'altro che certa.

Si noti, infine, che nei sistemi di *machine learning*, i quali si perfezionano in

---

[48] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 2019, 83.

[49] F: BAGNI, *op. cit.*, 924.

[50] Si pensi alla diffusione di algoritmi elaborati sulla base di reti di apprendimento "neurali", ovvero di algoritmi basati su logiche cosiddette *fuzzy* – o di logica sfumata – cioè algoritmi non vincolati al solo criterio di verità/falsità, ma anche a criteri di parziale verità-parziale falsità. Come rileva A. SIMONCINI, *op. cit.*, 79, in tutti questi casi «la stessa pretesa di "avere informazioni rilevanti sulla logica" delle decisioni potrebbe non avere senso».

[51] Su un possibile divieto all'utilizzo di tali tipi di algoritmi cfr. R. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. impr.*, 2019, 889; E. TROISI, *op. cit.*, 953 ss., spec. pp. 974-975.

[52] Anche se, per la verità, talvolta è possibile studiarne il comportamento analizzando le risposte che esso produce a fronte delle sollecitazioni che riceve. I c.d. "*explanatory tools*" (o "*post-hoc explanation techniques*", cfr. J. ZHONG e E. NEGRE, *AI: To interpret or to explain?*, Congrès Inforsid, 2021, https://hal.science/hal-03529203) sono in grado di ricostruire *ex-post* il funzionamento di taluni modelli decisionali "opachi", trovando i collegamenti tra le caratteristiche dei dati di *input* e i risultati o costruendo un modello più semplice per approssimare il modello originale. Critico sull'affidabilità delle "spiegazioni" così ottenute è C. RUDIN, *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead*, in *Nature Machine Intelligence*, vol. 1, n. 5, 2019, 206 ss.

[53] Cfr. T. BERG, V. BURG, A. GOMBOVIC, M. PURI, *On the Rise of Fintech:* Credit *Scoring using Digital Footprint*, in *RFS,* 2020. Sul punto, v. anche M. RABITTI, Credit scoring *via* machine learning *e prestito responsabile*, cit., 181 ss.

modo autonomo, le variabili predefinite non sono le uniche a rilevare, divenendo determinanti anche i dati desunti o inferiti dal sistema sulla base di correlazioni statistico probabilistiche[54]. Pertanto, anche laddove siano stati correttamente individuati i dati da utilizzare, è possibile che il sistema crei poi correlazioni di dati errate o che conducono a decisioni discriminatorie.

6. La regolazione del fenomeno nella Direttiva sul credito al consumo (CCD II) e nel nuovo Regolamento UE sull'intelligenza artificiale: il superamento di alcuni problemi lasciati aperti dal GDPR.

Le problematiche e le criticità emerse in relazione ai nuovi sistemi di *credit scoring* trovano adesso alcune risposte in due recenti provvedimenti dell'Unione europea: la nuova Direttiva sul credito al consumo e il Regolamento sull'Intelligenza Artificiale.

La prima[55] prevede opportunamente una serie di garanzie per il consumatore per il caso in cui la valutazione del merito creditizio comporti il ricorso al trattamento automatizzato di dati personali. In particolare, risulta di assoluto rilievo l'espressa previsione del diritto di chiedere e ottenere dal creditore una spiegazione chiara e comprensibile della valutazione del merito creditizio, potendosi così superare le incertezze lasciate aperte dal GDPR di cui si è dato conto nelle pagine precedenti. A ciò si aggiunge la possibilità di esprimere al creditore la propria opinione e di chiedere un riesame della valutazione del merito creditizio e della decisione relativa alla concessione del credito[56].

Con la direttiva in discorso, inoltre, il legislatore ha operato una vera e propria scelta di campo, escludendo espressamente la possibilità di utilizzare le informazioni ottenute tramite i *social network* ai fini della valutazione del merito creditizio[57] e richiedendo, in linea di principio, l'esistenza di una

[54] Ecco perché non ha convinto l'argomentazione utilizzata da Apple-Card, nel 2019, per far fronte allo scandalo sorto negli USA in relazione al caso di un uomo che aveva ricevuto una linea di credito di molto superiore a quella offerta alla moglie, sebbene i due avessero presentato dichiarazioni dei redditi comuni, vivessero nella stessa casa e possedessero lo stesso immobile. La difesa della società emittente di Apple-Card aveva infatti facilmente dimostrato che i suoi algoritmi «non usano nemmeno il genere come input» e «non prendono decisioni basate su fattori come il genere». Tuttavia, tale argomentazione è apparsa inadeguata ai giudici, proprio per il fatto che un algoritmo cieco al genere potrebbe comunque essere pregiudizievole fintanto che trae inferenza statistica da *input* che sono correlati al genere, come la cronologia degli acquisti e l'utilizzo del credito. Sul punto, efficacemente, M. RABITTI, *Discriminazioni tecnologiche e* Fin-tech, *cit.*, 482, la quale afferma che linea difensiva di Apple-Card «non ha convinto perché finisce per riflettere l'errata opinione diffusa secondo cui la rimozione di *input* e *proxy* algoritmici difettosi su caratteristiche protette è di per sé idonea e sufficiente ad eliminare i pregiudizi dell'IA».

[55] Direttiva 2023/2225/UE del Parlamento europeo e del Consiglio del 18 ottobre 2023 relativa ai contratti di credito ai consumatori e che abroga la direttiva 2008/48/CE.

[56] Art. 18, par. 8, lett. a), b) e c), Direttiva 2023/2225/UE.

[57] All'art. 18, rubricato «Obbligo di valutazione del merito creditizio del consumatore» la direttiva stabilisce che «La valutazione del merito creditizio è effettuata sulla base di informazioni pertinenti e accurate sul reddito e sulle spese del consumatore e su altre informazioni sulla situazione economica e finanziaria, che siano necessarie e proporzionate rispetto alla natura, alla durata, al valore e ai rischi del credito per il consumatore. […] Dette informazioni non includono le categorie particolari di dati di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679. Le informazioni sono ottenute da pertinenti fonti interne o esterne, incluso il consumatore e, ove necessario, sulla base di una consultazione di una banca dati di cui all'articolo 19 della presente direttiva. *I social network non sono considerati una fonte esterna ai fini della presente direttiva*» (corsivo aggiunto). A sua volta, l'art. 19, rubricato «Banche dati» prevede: «I creditori e gli

correlazione tra la situazione economico-finanziaria del singolo e le informazioni da processare. In questo contesto, si noti, i *dati social* vengono equiparati ai dati personali particolari di cui all'art. 9, par. 1, del GDPR, il cui utilizzo è pure espressamente vietato dalla direttiva, a prescindere da un eventuale consenso del consumatore.

Regole più specifiche sulla strutturazione e l'utilizzo dei sistemi di *credit scoring* si rinvengono, poi, nel nuovo Regolamento sull'intelligenza artificiale[58], il quale si propone di creare le condizioni per far sì che l'innovazione tecnologica possa svilupparsi in condizioni di sicurezza, assicurando il rispetto dei valori, dei diritti fondamentali e dei principi dell'UE[59]. Tutto ciò, mettendo al centro la tutela della persona e promuovendo l'idea che le attività basate su sistemi di IA siano affidabili, etiche e sicure[60].

L'approccio adottato con il Regolamento è dichiaratamente *risk oriented*, con la previsione di misure graduate in ragione del livello di rischio connesso allo specifico utilizzo dell'intelligenza artificiale. In particolare, alcune applicazioni o pratiche basate sulle tecnologie di IA sono considerate inaccettabili e dunque esplicitamente vietate (ad esempio, sistemi che adottano tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche manipolative aventi lo scopo o l'effetto di distorcere il comportamento umano[61]); altri utilizzi dell'IA sono considerati ad alto rischio e dunque sottoposti alla previsione di una serie di verifiche e presidi volti ad escludere o quantomeno minimizzare i potenziali danni[62]; altri ancora sono ritenuti a "basso rischio" e per tale motivo è rimessa alla discrezione dei produttori e degli utilizzatori l'eventuale adozione, su base volontaria, delle precauzioni previste per gli usi dell'IA classificati come "ad alto rischio"[63].

---

intermediari del credito non trattano le categorie particolari di dati di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 e i dati personali trattati dai social network che potrebbero essere contenuti nelle banche dati di cui al paragrafo 1 del presente articolo».

[58] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828. L'interesse della dottrina si è manifestato sin da subito con la Proposta di Regolamento, potendosi segnalare, tra le prime riflessioni, quelle di G. ALPA, *Quale modello normativo per l'intelligenza artificiale*, in *Contr. impr*., 2021, 1003 ss.; V. LEMMA, *Intelligenza artificiale e sistemi di controllo: quali prospettive regolamentari?*, in *Riv. trim. dir. econ*., suppl. n. 2 al n. 3, 2021, 319 ss.; C. CASONATO e B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, 2021, 415 ss.; G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf*., 2022, 303 ss.; G. RESTA, *Cosa c'è di "europeo" nella Proposta di Regolamento UE sull'intelligenza artificiale?*, ivi, 2022, 323 ss. Analizzano la Proposta con specifico riguardo alla regolamentazione del *credit scoring*, L. AMMANNATI e G.L. GRECO, *op. cit*., 501 ss., M. RABITTI, Credit scoring *via* machine learning *e prestito responsabile*, 192 ss.; D. DI SABATO e G. ALFANO, *L'impiego dell'IA per condizionare e valutare le persone tra limitazioni e divieti: qualche considerazione critica sulla proposta di Regolamento sull'IA elaborata dalla Commissione europea*, in *Riv. dir. impr*., 2022, 281 ss.

[59] Cfr. considerando n. 1. del Regolamento 2024/1689/UE.

[60] In questo senso, all'art. 1 si precisa che l'obiettivo Regolamento è quello di promuovere la diffusione di un'intelligenza artificiale « antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione».

[61] Art. 5, par. 1, lett. a) del Regolamento 2024/1689/UE.

[62] Ai sistemi ad alto rischio è dedicato l'intero Capo III del Regolamento 2024/1689/UE.

[63] In particolare, all'art. 95 del Regolamento 2024/1689/UE è previsto che la l'ufficio per l'IA e gli Stati membri incoraggino e agevolino l'elaborazione di codici di condotta volti a promuovere l'applicazione volontaria dei requisiti stabiliti per i sistemi ad alto rischio anche agli altri sistemi di IA.

I sistemi di intelligenza artificiale utilizzati per il *credit scoring* delle persone fisiche rientrano tra quelli considerati "ad alto rischio" [64] in ragione del loro impatto su alcuni interessi fondamentali degli individui e del pericolo relativo all'introduzione o perpetuazione di dinamiche di discriminazione nella valutazione della loro affidabilità creditizia. Per tale motivo, è previsto il rispetto di specifici requisiti di liceità, la cui sussistenza è verificata nell'ambito di una apposita valutazione di conformità e dimostrata nella documentazione tecnica redatta dal fornitore.

Più precisamente, affinché l'utilizzo dell'intelligenza artificiale per la valutazione del merito creditizio sia conforme ai valori etici e di affidabilità perseguiti dal legislatore europeo – e dunque per l'immissione di tali applicativi nel mercato – è richiesta la predisposizione di un sistema di gestione dei rischi che consenta l'identificazione, la stima e la valutazione dei rischi che possono emergere in relazione a tale utilizzo, in modo tale da permetterne l'eliminazione o l'attenuazione attraverso un'adeguata progettazione del sistema[65]. Inoltre, al fine di garantire la tracciabilità del loro funzionamento, è previsto che i sistemi di intelligenza artificiale ad alto rischio siano progettati e sviluppati con capacità che consentano la registrazione automatica degli eventi (c.d. "*log*")[66].

Di centrale rilievo è, poi, la previsione secondo cui ciascun sistema di IA deve essere progettato e sviluppato in maniera tale da garantire che il suo funzionamento sia sufficientemente trasparente da consentire al soggetto che lo utilizza (c.d. *deployer*) di interpretare l'*output* del sistema e utilizzarlo adeguatamente[67]. Ciò anche al fine di poter spiegare le decisioni adottate alla persona interessata, e permetterne l'eventuale contestazione dinanzi all'autorità nazionale competente.

Occorre evidenziare, infatti, che il Regolamento sull'intelligenza artificiale sancisce espressamente il diritto dell'interessato alla spiegazione dei processi decisionali [68], colmando perciò definitivamente uno dei principali limiti del GDPR[69].

---

[64] Cfr. l'Allegato III, punto. 5, lett. b) del Regolamento 2024/1689/UE. Sono escluse dall'elenco dei sistemi ad alto rischio le pratiche di *credit scoring* algoritmico volte a verificare il merito di credito delle imprese. D'altra parte, rispetto a queste ultime non si ripropongano le medesime preoccupazioni che i nuovi modelli di valutazione del merito creditizio destano con riferimento alle persone fisiche. Anzi, soprattutto in relazione alle PMI e alle imprese innovative di recente costituzione (prive, dunque, di una significativa storia creditizia), l'utilizzo di dati alternativi può essere un importante strumento per l'accesso al credito, permettendo al contempo all'ente finanziatore di effettuare una migliore valutazione circa l'effettiva messa in atto di condotte socialmente responsabili (secondo i c.d. parametri ESG).

[65] Art. 9 del Regolamento 2024/1689/UE.

[66] Art. 12 del Regolamento 2024/1689/UE.

[67] Art. 13 del Regolamento 2024/1689/UE.

[68] Art. 86 del Regolamento 2024/1689/UE, rubricato «Diritto alla spiegazione dei singoli processi decisionali», il cui par. 1 stabilisce che «Qualsiasi persona interessata oggetto di una decisione adottata dal deployer sulla base dell'output di un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi elencati al punto 2 dello stesso, e che produca effetti giuridici o in modo analogo incida significativamente su tale persona in un modo che essa ritenga avere un impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali ha il diritto di ottenere dal deployer spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata».

[69] In generale, sui rapporti tra il GDPR e il nuovo Regolamento sull'intelligenza artificiale, si veda A. LOMBARDI, *Disciplina della tutela dei dati personali e regolazione dell'intelligenza artificiale: rapporti, analogie e differenze tra* GDPR *e* AI Act, in *EJPLT*, 240 ss.; P. FALLETTA e A. MARSANO, *Intelligenza artificiale e protezione dei dati*

L'*AI Act* detta, inoltre, alcune regole specifiche sui dati e sulla loro *governance*, stabilendo, in particolare, che i sistemi di intelligenza artificiale ad alto rischio siano sviluppati sulla base di *set* di dati di addestramento, convalida e prova pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista[70]. Tali *set* di dati devono possedere le proprietà statistiche appropriate per quanto riguarda le persone o i gruppi di persone in relazione ai quali il sistema di IA ad alto rischio è destinato a essere usato[71]. Essi, poi, devono essere soggetti a misure di *governance* adeguate, che comprendono la valutazione delle possibili distorsioni[72] nonché le misure idonee per individuare, prevenire e attenuare tali possibili distorsioni[73].

Si noti, infine, che allo scopo di prevenire o ridurre al minimo i pericoli legati all'utilizzo dell'intelligenza artificiale è previsto che i sistemi ad alto rischio siano progettati e sviluppati in modo tale da poter essere efficacemente supervisionati, durante il periodo in cui sono in uso, da persone fisiche[74], le quali oltre ad essere in grado di comprendere appieno le capacità e i limiti del sistema, devono monitorarne il funzionamento (anche al fine di individuare e affrontare anomalie o disfunzioni) ed eventualmente intervenire sul sistema medesimo, interpretarne correttamente gli *output* e, se necessario, decidere di «ignorare, annullare o ribaltare» le indicazioni da esso fornite [75]. In questo modo, si attribuisce agli interessati una tutela più ampia e incisiva rispetto a quella sancita dall'art. 22 del GDPR, ove – riprendendo quanto si è già accennato – il «diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato» risulta depotenziato da una serie di significative eccezioni e «il diritto di ottenere l'intervento umano» non è assistito da misure che ne assistano concretamente l'effettività[76].

Alla luce di quanto sin qui detto, non possono non accogliersi positivamente le novità introdotte dal legislatore europeo, le quali, per quanto qui di interesse, consentono di sfruttare le potenzialità e i benefici della c.d. intelligenza artificiale applicata alla valutazione del merito di credito, riducendo al contempo al minimo il rischio di decisioni errate o distorte, in una prospettiva che mette al centro la persona e la tutela dei suoi diritti fondamentali.

---

personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR, in *Riv. it. inf. dir.*, 2024, 119 ss.

[70] Art. 10 par. 3 del Regolamento 2024/1689/UE

[71] Art. 10 par. 3 del Regolamento 2024/1689/UE.

[72] Art. 10 par. 2 lett. f) del Regolamento 2024/1689/UE.

[73] Art. 10 par. 2 lett. g) del Regolamento 2024/1689/UE.

[74] Si vedano al riguardo le considerazioni di D. ROSSANO, *L'intelligenza artificiale: ruolo e responsabilità dell'uomo*, in *Riv. trim. dir. econ.*, suppl. al n. 3, 2021, 222 ss.

[75] Art. 14 del Regolamento 2024/1689/UE, rubricato «Sorveglianza umana».

[76] Sul punto, cfr. C. CASONATO e B. MARCHETTI, *op. cit.*, 428.

Giacalone M, Arnone G, 'Dispute Resolutions for Digital Assets in a Decentralized Virtual World' (2024) 1 EJPLT, 117-135.
DOI: https://doi.org/10.57230/EJPLT241MGGA

EJPLT
ISSN 2704-8012



Dispute Resolutions for Digital Assets in a Decentralized Virtual World

La risoluzione delle controversie per i beni digitali in un mondo virtuale decentralizzato

MARCO GIACALONE
Research Professor and Co-Director of the Digitalisation and Access to justice Research Group (DIKE)
Private and Economic Law Department (PREC), Vrije Universiteit Brussel

GIOIA ARNONE
Ph.D., Researcher of the Digitalisation and Access to justice Research Group (DIKE)
Private and Economic Law Department (PREC), Vrije Universiteit Brussel

Abstract
Digital assets and the Metaverse have transformed our interactions and business practices. This dynamic environment, comprising virtual worlds and online communities, facilitates the creation, sharing, and consumption of digital information. As the Metaverse grows, disputes over digital assets pose challenges for traditional dispute resolution. Thus, this study explores the need for effective dispute resolution, focusing on digital assets, decentralization, digital evidence, and proposing a structure for decentralized resolution.

Gli asset digitali e il Metaverso hanno trasformato le nostre interazioni e le pratiche commerciali. Con la crescita di questo ambiente dinamico, composto da mondi virtuali e comunità online, le controversie sugli asset digitali pongono sfide per la risoluzione tradizionale delle dispute. Pertanto, questo studio esplora la necessità di una risoluzione efficace delle controversie, concentrandosi sugli asset digitali, la decentralizzazione, le prove digitali e proponendo una struttura per la risoluzione decentralizzata.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Digital assets, Metaverse, Blockchain technology, Decentralization, Dispute resolution.

Summary: 1. The Role of Digital Assets within virtual realms. - 2.Understanding Digital Assets in virtual realms. - 3. Legal Frameworks for Digital Assets in the Metaverse. - 3.1 Challenges in Resolving Disputes on digital assets in virtual realms. - 3.2 LegalTech Challenges in the Metaverse. - 4. The future of digital assets in the Metaverse. – 4.1. Key Findings. – 4.1. Future Research Directions.

1. The Role of Digital Assets within virtual realms.

Computer science innovations significantly impact daily life by improving and transforming social interactions, communication, and human contact. Three significant waves of technical progress have been identified from the perspective of end users, and they are based on the arrival of desktop computers, the Internet, and mobile devices, in that order. Immersive technologies like augmented reality (AR) and virtual reality (VR) are at the centre of the fourth wave of computer innovation. This wave is expected to create the next paradigm in ubiquitous computing, potentially revolutionizing remote labour, business, education, and entertainment - especially for online learners. This new paradigm is called the Metaverse. The closed compound word metaverse comprises the Greek prefix meta, which means beyond, or after, and universe. Stated in various ways, the Metaverse is an everlasting, multiuser post-reality setting that blends virtual and physical reality. The fundamental flaws of web-based 2D e-learning tools can be addressed by metaverse in the context of distance learning through the internet.

Metaverse is a multiuser and post-reality environment that combines both physical reality and digital virtuality and is based on the convergence of Augmented and Virtual Reality that allows multimodal interaction with digital data, individuals and virtual environment. As a result, Metaverse refers to a multiuser platform connected to another network of social engagement settings to facilitate dynamic interaction with smooth embodied user communication and digital objects in real-time. It comprises an immersive and social VR system that engages and works with open game worlds, AR spaces and parallel computing networks.[1] There is fierce competition to develop the standards, protocols and infrastructure for the Metaverse. Big companies are putting a lot of effort into developing their closed, proprietary hardware and software ecosystems in an effort to entice customers and position themselves as the de facto Metaverse destination.

The scientific community has recently given the metaverse a great deal of attention, and much research was previously done on this technology's principles, architecture, and uses. Since this technology is still in its infancy, we must manage any potential issues that may arise from the qualities of the metaverse, such as virtual worlds, scaling, perseverance, synchronization, financial flexibility, decentralization, privacy, and interoperability.

[1] Y Aouidef, F Ast, B Deffains, 'Decentralized justice: A comparative analysis of blockchain online dispute resolution projects' (2021) 4 Frontiers in Blockchain, 3.

Neal Stephenson coined the term 'metaverse' 1992 while writing 'Snow Crash', a science fiction novel. According to Stephenson,[2] the prefix 'meta' denotes 'far off', and the suffix 'verse' denotes 'universe'. The founder of Facebook, Mark Zuckerberg, later validated this by declaring in October 2021 that his digital platform would now be referred to as 'meta'. The term 'metaverse' refers, in general, to a fifth-generation of technology and everything that exists outside of the Internet, where individuals can utilize software and avatars to portray themselves as members in an interactive three-dimensional world[3]. However, because many scholars have defined the phrase differently, there isn't a single, widely acknowledged definition. Some academics describe it as an immersive three-dimensional collaborative setting where users can engage in cultural, social, and economic activities while communicating via avatar[4]. The main objective asserts that the Metaverse is seen as a thriving component of the next-generation internet, having emerged with the emergence of the web and mobile internet.[5]

Several significant IT giants have declared participation in the Metaverse, including Microsoft, Facebook, Tencent, NVIDIA, Unity, and Bytedance. Facebook has gone even so far as to adopt the moniker "meta" for itself. Microsoft purchased Activision Blizzard for an astounding $68.7 billion to increase its presence in the Metaverse gaming industry. This represents a significant investment in the Metaverse for the firm. These technology industry titans are keen to lead this new and exciting frontier because they believe the Metaverse can completely transform the digital world m.[6] Metaverse Seoul is building a virtual ecosystem to facilitate communication amongst several municipal administrative domains, such as culture, tourism, commerce, education, and public service. These developments offer a glimpse into the expanding Metaverse universe that draws the attention of various social network platforms, online gaming giants, financial and business companies, and more. It can also expand to other aspects of human life, such as healthcare, education, simulation, and transportation.[7]

Thus, the main objective of this article is to examine and emphasize the critical need for effective dispute resolution processes in the rapidly expanding Metaverse, with a specific focus on challenges related to digital assets. The article aims to address the unique complexities arising from the advent of digital assets, including virtual products, currencies, NFTs, and cryptocurrencies, within the immersive and decentralized environment of the Metaverse. It seeks to explore the impact of decentralization and blockchain

[2] JG Allen, 'Wrapped and stacked:'smart contracts' and the interaction of natural and formal language', (2018) 14(4) European Review of Contract Law, 307-343.
[3] J Allen, P Hunn. (Eds.), *Smart Legal Contracts: Computable Law in Theory and Practice* (Oxford University Press 2022).
[4] E Androulaki, A Barger, V Bortnikov, C Cachin, K Christidis, A De Caro, J Yellick, 'Hyperledger fabric: a distributed operating system for permissioned blockchains, (2018, April) In Proceedings of the thirteenth EuroSys conference, pp. 1-15)
[5] P Bacaksiz, 'Criminal Law against Metaverse and Virtual Reality Environments', (2023) 14 Inonu UL Rev., 289.
[6] R Belk, M Humayun, M Brouard, 'Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and Wild Markets', (2022) 153 Journal of Business Research, 198-205.
[7] G Benton, 'Cost Is the Top Tech Litigation Problem, Survey Shows', (2017) 2 Silicon Valley Arbitration, Mediation Center, available at https://svamc.org/wp-content/uploads/SVAMC-2017-Survey-Report.pdf

technology on conflict resolution, analyze the intricate nature of digital assets, and propose a structured approach for decentralized dispute resolution.

Digital assets are distributed ledger or blockchain-based assets that may be issued and transferred. Several names, such as cryptocurrency, digital tokens, and crypto assets, refer to them. Digital assets include commodities, real estate, securities, and money. One of the main issues with the Metaverse is how personal information is handled. The requirement to protect user information is reflected in the laws that apply to the Metaverse, such as the EU's General Data Protection Regulation (GDPR).[8] The Metaverse's immersive quality makes it possible to gather previously unheard-of volumes of data, such as biometric psychography, which discloses users' mental, emotional, and physical conditions. In decentralized Metaverse systems, disagreements may emerge about data protection principles, the appropriate use of such data, and who is ultimately responsible.

Identity theft must be avoided by making sure people in the Metaverse are who they say they are: existing criminal laws will probably be referenced in legal responses to identity theft in the Metaverse. Still, there are also practical issues to be resolved, such as tracking down offenders across countries. Resolving disputes in the Metaverse entails manoeuvring through intricate matters about jurisdiction, choice of law, and the characteristics of non-formal dispute resolution procedures. Although an intra-metaverse conflict resolution mechanism might develop, it is challenging to implement such decisions in the actual world. A possible answer is arbitration, as a hybrid method of resolving conflicts while maintaining anonymity.

2. Understanding Digital Assets in virtual realms

For decades, people have debated and conjectured about the idea of a Metaverse: a shared virtual world where people can communicate with one another in a computer-generated setting. But it wasn't until recently that technological advances have enabled the development of a Metaverse a plausible prospect.[9]

The concept of a virtual world was first proposed by scientists and futurists in the 1960s when they imagined a society where people might interact in a computer-generated environment. Ivan Sutherland, a computer scientist, invented the Sword of Damocles, the first head-mounted display (HMD), in the late 1960s. He named it "the ultimate display," allowing individuals to surround themselves with a virtual world.[10]

As virtual reality developed in the 1980s and 1990s, the idea of a Metaverse gathered increasing traction. Science fiction author Neal Stephenson defined a Metaverse as an online setting created by computers where individuals might

[8] P Bhattacharya, MS Obaidat, D Savaliya, S Sanghavi, S Tanwar, B Sadaun, 'Metaverse assisted telesurgery in healthcare 5.0: An interplay of blockchain and explainable AI', (2022, July), In *2022 IEEE International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1-5.

[9] LH Lee, and Others, 'All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda', (2021), *arXiv preprint arXiv:2110.05352*.

[10] D Buhalis, MS Lin, D Leung, 'Metaverse as a driver for customer experience and value co-creation: implications for hospitality and tourism management and marketing', (2022) 35(2) International Journal of Contemporary Hospitality Management, 701-716.

interact with one another in his 1986 book "Snow Crash." Many in the computing sector were drawn to the book, which became a cult classic.[11]

In the early 2000s, virtual worlds like World of Warcraft and Second Life were released, allowing users to create and interact with one another in an online environment. These virtual worlds were the first genuine attempts to establish a Metaverse. Still, they could not provide users with the desired level of immersion and involvement at the time due to technology limitations.[12]

Virtual Reality (VR) is a technique that uses hardware and software to create a digitally created perspective of the natural world to replace the user's perspective. The most popular virtual reality applications on the market today leverage all of the user's senses to produce a fully immersive experience that immerses the viewer in an incredibly realistic virtual environment. Augmented Reality (AR) is a technology that combines the virtual and physical worlds. Recognizing surfaces and things in the real world makes use of a range of technologies, including recognition of facial features, movement tracking, identifying objects, and plane detection. Augmented reality can potentially replace the present-day ecosystem of phones and other gadgets as our primary means of interacting with digital assets and as our primary portal to the metaverse.

Milgram and Kishino[13] defined Mixed Reality as a hybrid of augmented and virtual reality that exists in one of these contexts. Uses of mixed reality can improve the metaverse in the robotics, entertainment, military, and healthcare sectors. Van Niekerk[14] (2006) defines a digital asset precisely as "any item of text or medium that has been translated into a binary source which includes the right to use it". According to this perspective, the idea of a digital asset evolved due to implementing the digital citizenship concept rather than the effect of the Internet itself:[15] the strength of digital assets drives ongoing development in the metaverse's economic framework.

Given its magnitude and continual expansion, calling the metaverse the next great thing in the digital space wouldn't be an enormous exaggeration. and the projected counterpart to the online world.[16] Significant IT giants like Microsoft, Facebook, Tencent, NVIDIA, Unity, and Bytedance have declared their presence in the metaverse. Facebook has even gone so far as to call itself "meta." Microsoft acquired Activision Blizzard for an astounding $68.7 billion to bolster its standing in the metaverse game business. This represents a significant metaverse investment for the corporation. These titans of industry from the technology sector are eager to steer this exciting new future because they

[11]V Buterin, 'A next-generation smart contract and decentralized application platform', (2014) 3(37) 3(37) white paper, 2.

[12] E Chan, E Hay, Something Borrowed, Something Blue: 'The Best of Both Worlds in Metaverse-Related Disputes', (2022) 15 Contemp. Asia Arb. J., 205.

[13] K Cornelius, 'Responsibility under criminal law in virtual worlds', in *Virtual worlds and criminality* (Heidelberg: Springer Berlin Heidelberg, 2011), pp. 95-119.

[14] H Duan, J Li, S Fan, Z Lin, X Wu, W Cai, 'Metaverse for social good: A university campus prototype', (2021, October), In Proceedings of the 29th ACM international conference on multimedia, pp. 153-161.

[15] YK Dwivedi, L Hughes, AM Baabdullah, S Ribeiro-Navarrete, M Giannakis, MM Al-Debei, SF Wamba, 'Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy'(2022) 66 International Journal of Information Management, 102542.

[16] G Freeman, D Maloney, 'Body, avatar, and me: The presentation and perception of self in social virtual reality', (2021) 4(CSCW3) Proceedings of the ACM on human-computer interaction, pp. 1-27.

think the metaverse has the potential to transform the digital media landscape altogether. [17] These developments offer a glimpse into the expanding metaverse environment grabbing the attention of big online gaming corporations, social media networks, financial and commercial organizations, and more. In addition, it can be applied to various areas of human life, such as transportation, simulation, healthcare, and education.[18]

The world is increasingly transitioning into a digital economy with the advancement of digital technology. The digital economy is the primary economic form following the industrial and agricultural economies. According to Li and Jia,[19] this new economy combines efficiency and fairness. Its main components are data resources, modern information networks that serve as the primary carrier, technology for communication and information integration and application, and digital transformation factors that are significant driving forces. The digital economy is driving significant changes in manufacturing, lifestyle, and democracy. It is significantly impacted by reducing resources, reorganizing the world economy, and reshaping the global competitive environment.

Any digital content produced by metaverse users, including images, music, videos, and so on, is referred to as user-generated content (UGC). According to Lee et al., [20] the generated material has potential commercial value and contains personal private data. UGC is a good stand-in technique to assess user demand. Common user-generated content, produced by users for users, serves as its central pillar. Anyone can upload content to the website. The content has either automatic or manual approval before being viewed by the public on the platform. Similar to the idea behind We Media, users can create a wide variety of personalized digital media, including blogs, podcasts, audio recordings, videos, and news.

There is a rising requirement for UGC property because UGC in the realm of the metaverse is typically diverse.[21] However, because artistic ability is not required, the standard of user-generated content varies. With so much informal and repetitive digital content, many UGCs cannot be effectively captured by the current approaches. Timoshenko et al.[22] use a deep learning-based method to weed out irrelevant material so they don't sample the same things twice. Even though several scholars have focused on essential study issues for user-generated content (UGC) in the metaverse, there are still specific challenges, including ownership control, payment framework, and incentive system.

Professional Generated Content (PGC) indicates that the content was produced by field experts or institutions with specialized training in content development. The competency of the content can be ensured in this way. PGC is, therefore, usually validated by the platform. It typically pays more attention

[17] JM aron, 'Legal implications of a ubiquitous Metaverse and a Web3 future', (2022), Marq. L. Rev., p.p. 106-163.
[18] A Gatt, E Krahmer, 'Survey of the state of the art in natural language generation: Core tasks, applications and evaluation', (2018) 61 Journal of Artificial Intelligence Research, pp. 65-170.
[19] M Georgantzidou, 'Arbitration of Disputes involving Smart Contracts and Blockchain Technology', [2023].
[20] D Grider, M Maximo, 'The Metaverse: Web 3.0 virtual cloud economies', (2021), *Grayscale Research*, *1*, 18.
[21] M Gupta, D Gupta, 'Investigating Role of Blockchain in Making your Greetings Valuable' (2023) 10(4) Universal Research Reports, 69-74.
[22] BE Howell, PH Potgieter, Uncertainty and dispute resolution for blockchain and smart contract institutions', (2021) 17(4) Journal of Institutional Economics, 545-559.

to copyrights and contains original content. PGC can attest to the importance and effectiveness of the content. For instance, PGC video services offer capabilities related to specialisation and revenue in an environment that is easy to utilize for advertisements.[23]

One popular kind of blockchain-based digital asset is non-fungible tokens (NFTs), digital tokens that are linked to specific digital or physical assets and are recorded on a blockchain. NFTs are used in the Metaverse to conduct transactions with digital assets like virtual land, artwork in a virtual museum, and shoes that avatars might wear. Legal systems worldwide are investigating the legal standing and property rights granted by different digital assets.[24] By archiving past encrypted transactions on the linked blockchain indefinitely, NFTs ensure the distinctive qualities of digital assets.[25] NFT provides a futuristic option for art trade as a blockchain-based digital token as evidence of ownership and authenticity for crypto assets. For example, Niemeyer and Gerber[26] have developed a sophisticated economic framework that allows users to amass virtual currency in Axie Infinity, an NFT-driven Ethereum game. To provide uniqueness and authentication, NFT may tokenize various digital assets, including music, film, art, collectables, and in-game objects.[27] When defining legitimate rights for metaverse games, NFT is a significant factor. NFTs are distinguished by their cultural solid and interactive traits. When a user purchases an NFT, they will become the only owners of that asset. This purchasing activity has a lot of social significance because it enables users to display their unique preferences, purchasing prowess, and even social standing in the online community. Therefore, to recognize the ownership and worth of the NFT based on the technological blockchain, a certain number of participants must agree and engage in rich social activity. Using digital collections to materialize digital assets into tradeable entities is the primary goal of NFT.

3. Legal Frameworks for Digital Assets in the Metaverse.

3.1 Challenges in Resolving Disputes on digital assets in virtual realms.

Digital assets include many items, such as self-executing smart contracts, tokenized stocks, NFTs, cryptocurrencies like Ethereum and Bitcoin, and digital tokens representing ownership rights. Several factors make these assets challenging, chief among them being the technological intricacy of blockchain, dispersed networks, and cryptography.

Regulatory issues result in additional complexity since legislation varies

[23] T Huynh-The, QV Pham, XQ Pham, TT Nguyen, Z Han, DS Kim. 'Artificial intelligence for the Metaverse: A survey', (2023) Engineering Applications of Artificial Intelligence, 117, 105581.
[24] HJ Jeon, HC Youn, SM Ko, TH Kim, 'Blockchain and AI Meet in the Metaverse' (2022) Advances in the Convergence of Blockchain and Artificial Intelligence, 73 (10.5772).
[25] A Joy, Y Zhu, C Peña, M Brouard, 'Digital future of luxury brands: Metaverse, digital fashion, and non-fungible tokens' (2022) 31(3) Strategic change, 337-343.
[26] M Kalyvaki, 'Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction' (2023) 3(1) Journal of Metaverse, 87-92.
[27] K Kamenov, 'Immersive experience—The 4th wave in tech: Learning the ropes', (2017), Retrieved from Accenture: https://www.accenture.com/gb-en/blogs/blogs-immersive-experience-wave-learning-ropes.

throughout jurisdictions. Security is crucial since there is a chance of fraud and hacking due to the digital nature of these assets. Interoperability issues arise from protocol differences, and market dynamics are influenced by sentiment, technology advancements, and legal changes. Determining ownership responsibilities and rights in the digital domain is a challenging governance and legal matter. Scalability becomes a problem when acceptability rises; therefore, it's essential to be informed about how things change. A multidisciplinary approach combining finance, technology, legal, and regulatory expertise is required to negotiate this challenging environment successfully.

Thus far, the metaverse hasn't directly caused many commercial problems.[28] Numerous potentials use for VR, MR, AR, and metaverse platforms are either unconsidered or in the theoretical stages of study. However, there are currently a lot of cases of disputes involving technological assets.[29] More disputes of this kind are expected to arise because digital assets will be central to the metaverse. Few business issues have resulted directly from the Metaverse thus far.[30] Many possible applications for VR, MR, AR, and platforms in the Metaverse are still in the theoretical research stage or have not yet been considered. On the other hand, there are already many instances of conflicts concerning technology asset.[31] Given that digital assets will play a significant role in the Metaverse, additional disagreements of this nature are expected to occur.

Although the decentralized structure of various metaverse systems allows users to transact freely with each other, it also increases the risk of user disputes mimicking contracts over any aspect of a transaction or agreement, such as a sale, license, or service. Users themselves will choose the terms under which these transactions are done.[32] Contractual arrangements for the industry and technological know-how necessary to establish and maintain a presence in the metaverse will be made by commercial entities. As new products and services, as well as new partnerships, are established, new disputes will undoubtedly surface.

There is currently little control in the metaverse area, even though state authorities have begun examining the regulatory implications of digital assets.[33] Governments will certainly wish to exercise control over the metaverse by applying existing rules and regulations or passing new ones. This could include following the law on taxes, banking regulations, competition, money laundering prevention, criminal offences, video games, and rules

[28] O Kanevskaia, 'Regulation (EU) No 1025/2012 of the European Parliament and of the Council, (14th November 2012) [2012] OJ L316/12).
[29] S Kasiyanto, MR Kilinc, 'The legal conundrums of the Metaverse', (2022) 1(2) Journal of Central Banking Law and Institutions, 299-322.
[30] C Kerdvibulvech, 'Exploring the impacts of COVID-19 on digital and metaverse games', (2022, June) In International conference on human-computer interaction, Cham: Springer International Publishing, pp. 561-565.
[31] SN Khan, F Loukil, C Ghedira-Guegan, E Benkhelifa, A Bani-Hani, 'Blockchain smart contracts: Applications, challenges, and future trends', (2021) 14, Peer-to-peer Networking and Applications, 2901-2925.
[32] J Kim, 'The institutionalization of YouTube: From user-generated content to professionally generated content', (2012)' 34(1) Media, culture society, 53-67.
[33] O Kostenko, V Furashev, D Zhuravlov, O Dniprov, 'Genesis of legal regulation web and the model of the electronic jurisdiction of the metaverse', (2022) 6(2) Bratislava Law Review, 21-36.

protecting consumer privacy and data.[34] This regulatory action may give rise to conflicts other than those already stated, including disputes with other regulators. Some metaverse platforms have included taxation disclaimers in their use conditions, implying that they have thought about possible tax-related difficulties.[35]

When negotiating the legal environment of the metaverse, there are several other ethical and legal considerations, such as cybercrime. The metaverse is becoming a target for cybercriminals as it develops. This may involve problems like fraud, hacking, and selling illicit products and services. Furthermore, online worlds can foster discrimination and harassment, and the metaverse's anonymity may make it harder to hold individuals accountable.[36]

In the metaverse, "digital identity" refers to how a person's identity is portrayed in virtual spaces such as social media platforms, online forums, and virtual worlds.[37]

Cybercrimes are also handled internationally through treaties and contracts like the Council of Europe Convention on Cybercrime or the Budapest Convention, ratified by 57 nations, including the US, Canada, Japan, and many European nations.[38]

Several businesses have teams of moderators that watch for infractions in the virtual world and take appropriate action. Additionally, some VR companies employ third-party technologies, including anti-cheat tools, to identify and stop hacking and cheating in virtual environments.

3.2 LegalTech Challenges in the Metaverse.

Enforcing intellectual property laws, like trademark and copyright regulations, in the Metaverse could prove difficult due to its decentralized and virtual nature. Additionally, determining ownership and authorization to use virtual assets in the Metaverse may present challenges. In addition to the existing intellectual property regulations, it is crucial to acknowledge that resolving disputes arising from digital assets within the Metaverse requires considerations beyond mere copyright infringement. The intricate nature of this virtual realm introduces a plethora of complex issues, including but not limited to ownership disputes, instances of fraud, and the enforcement of contractual agreements. Consequently, as the Metaverse continues to evolve, it becomes imperative for legal frameworks to adapt and address these multifaceted challenges effectively. By doing so, a robust and comprehensive

[34] LH Lee, Z Lin, R Hu, Z Gong, A Kumar, T Li, P Hui, 'When creators meet the Metaverse: A survey on computational arts', (2021), arXiv preprint arXiv:2111.13486.
[35] V Lehdonvirta, 'Real-money trade of virtual assets: ten different user perceptions', (2005), Proceedings of Digital Arts and Culture (DAC 2005), IT University of Copenhagen, Denmark, 52-58.
[36] L Li, H Jia, 'Analysis of Metaverse Development in the Context of Digital Economy', (2023, August), In 2023 2nd International Conference on Artificial Intelligence, Internet and Digital Economy (ICAID 2023) (pp. 481-490). Atlantis Press.
[37] X Li, X Wang, T Kong, J Zheng, M Luo, 'From bitcoin to solana–innovating blockchain towards enterprise applications', (2021, December), In International Conference on Blockchain, Cham: Springer International Publishing (pp. 74-100).
[38] WYB Lim, Z Xiong, D Niyato, X Cao, C Miao, S Sun, Q Yang, 'Realizing the Metaverse with edge intelligence: A match made in heaven' (2022) IEEE Wireless Communications.

system can be established to safeguard the rights and interests of all participants engaging with digital assets within this virtual world. Since users may require greater authority over their personal information and how it is gathered, used, and shared, privacy is a significant concern in the Metaverse. Data protection regulations, including the EU General Data Protection Regulation (GDPR), may be broken.[39]

Blockchain technology and smart contracts also lay the foundation of Bitcoin, a digital money with fungible (interchangeable) tokens that will be utilized for transactions in the Metaverse. Blockchain is a term for a decentralized digital ledger that uses cryptography to record assets and transactions in a safe network. This ledger provides quick, shared, and open access to data stored in an unchangeable, unbreakable format only accessible by network users with permission. However, a lot of data, including digital content and movies taken by VR devices, are frequently transferred and stored in data centres without the necessary security and privacy protections, leaving them vulnerable to cyberattacks within the virtual universe known as the Metaverse. In light of these privacy and security issues, blockchain technology, with its unique features, offers a workable solution for data protection in the Metaverse. Several innovative methods for gathering, storing, and dispersing data have been proposed during the past ten years by combining blockchain technology with artificial intelligence in various industries to provide the highest level of data security and privacy. These techniques have shown great promise for use in the Metaverse.[40]

Prospective buyers can now "visit" a house virtually instead of only seeing images or videos, giving them a more significant idea of the property's design, features, and general atmosphere. Luxury real estate developers also utilise the Metaverse to build virtual showrooms to present their assets to a worldwide clientele. This enables them to market their real estate in a more dynamic and captivating manner and to connect with a larger spectrum of prospective purchasers.[41] Furthermore, the development of virtual rights to ownership and the capacity to exchange virtual assets is made possible by applying blockchain and smart contract technology. This creates a new business benchmark and expands the luxury real estate market in the Metaverse.[42]

Different nations have different legal and regulatory frameworks. This diversity encompasses consumer protection legislation, privacy laws, and intellectual property rights. Conflicts may occur when users from different countries are subject to contradictory rules or when disparate legal systems collide in the need for a standard legal structure for the Metaverse. The Metaverse frequently lacks a single governing body, unlike conventional legal systems, where a centralized governing body or government organization offers a framework for dispute resolution. Although decentralized platforms

[39] K Lippert, MNR Khan, MM Rabbi, A Dutta, and R Cloutier, 'A framework of Metaverse for systems engineering', 2021 December, In 2021 IEEE International Conference on Signal Processing, Information, Communication Systems (SPICSCON) (pp. 50-54). IEEE.
[40] A Singh, RM Parizi, Q Zhang, KKR Choo, A Dehghantanha, 'Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities', (2020), Computers Security, 88, 101654.
[41] N Stephenson, 'Snow crash: A novel', (2003), Spectra.
[42] G Stobbs, *The Digital Millennium Copyright Act. In Multimedia Security Technologies for Digital Rights Management* (Academic Pres, 2006), pp. 457-482.

and virtual worlds might have proper regulations and governance processes, they need to be compatible with conventional legal frameworks. Although decentralization might support user autonomy, it makes it challenging to enforce uniform regulations.[43]

The meta-universe is neither novel nor lawless; it is not above the laws of the real world. The difficulty lies in comprehending how legislation might operate at several levels to control various facets of an online experience as technology advances (Aydin, 2023). It is crucial to remember that the regulations that govern the actual world and the internet now will largely govern the Metaverse: the meta-universe order is already subject to existing laws covering topics like contracts, data protection, anti-money laundering, defamation, torts, gaming and gambling, intellectual property, taxation, and financial regulations.[44]

Contracts are also necessary to determine intellectual property rights, the validity of terms and conditions, user usage of the software, and any constraints. It is also feasible for legal professionals to mediate contractual disputes online. In the virtual world today, smart contracts are widely used. The practice of activating embedded codes in contract terms with data to enable honest transaction execution without intermediaries and virtually eliminate the possibility of outside intervention is known as smart contracting. "Buying food or drinks from food machines after an individual's instruction in return for a given amount" is the most famous example of a fundamental overview of this notion. Because copyright laws grant authors the exclusive right to reproduce, share, and exhibit their creations, they can protect artists in the metaverse. Examples include avatars, virtual worlds, 3D models, and other digital content produced in the metaverse. The U.S. Copyright Act of 1976 provides a framework for protecting creative works of authorship, including literary, dramatic, musical, and artistic works, including those that might be produced in the metaverse, according to the United States Copyright Office (2020): the law states that when a work is created in a fixed form, its copyright protection is applied and remains in effect for several years following the author's death. The Digital Millennium Copyright Act (DMCA) and the Copyright Act safeguard works secured by copyright in digital contexts. It has provisions for the safe harbour for internet service providers and the notice-and-takedown process for removing unlawful content.[45]

Since collecting and sharing vast amounts of personal data can occur in virtual worlds and online communities, protecting privacy in the metaverse can be difficult. A mix of organizational, legal, and technical protections could be required to preserve privacy. Although rules pertaining to privacy in the metaverse are still being developed, a number of them already in place can serve as a foundation for safeguarding privacy in virtual environments. For example, under the General Data Protection Regulation (GDPR) in the EU and

[43] DP Sheldon, 'Claiming ownership, but getting owned: contractual limitations on asserting property interests in virtual goods' (2006) 54 UCLA L. Rev., p. 751.
[44] P Shrivastava, M Damle, 'Investment decision in cloud gaming-based businesses opportunities: An analysis of the cloud gaming industry,' (2022, March), In 2022 International Conference on Decision Aid Sciences and Applications (DASA), pp. 1224-1228.
[45] P Si, J Zhao, H Han, KY Lam, Y Liu, 'Resource allocation and resolution control in the metaverse with mobile augmented reality,' In GLOBECOM 2022-2022 IEEE Global Communications Conference, pp. 3265-3271.

the California Consumer Privacy Act (CCPA) in the US, individuals have rights to their data, including the opportunity to view, modify, and erase personal information. Sensitive personal data, including health information, is further protected by the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada and the Health Insurance Portability and Accountability Act (HIPAA) in the United States. One specific example of legislation protecting privacy in the metaverse is the Children's Online Privacy Protection Act (COPPA) in the United States, which regulates the gathering of personal information from children under the age of thirteen. This law requires that websites and online services geared at minors seek verifiable parental consent before acquiring, using, or disclosing private data from children. Virtual private network (VPN) technology is another way to safeguard privacy in the metaverse. By encrypting data as it is transferred between a user's device and the virtual environment, VPNs can increase the difficulty of third parties intercepting or accessing personal data.[46]

In the Metaverse, NFTs are governed by customary financial laws, including those about securities, banking, and commodities. These assets might be classified as investment contracts depending on how they are made and traded, putting them under the purview of securities law. Banking, money transfer, and other financial regulations will probably be applied to the system as a result of the issue, lending, and trading of cryptocurrencies on the Metaverse.[47] The blockchain has been known for more than ten years as a technology in which every transaction that has ever occurred in a peer-to-peer network is recorded in a distributed database. It is considered a distributed computing model that effectively resolves the problem of centralized party trust. As a result, multiple nodes work together in a blockchain network to maintain a set of shared transaction records securely and independently. Executable scripts running on top of the blockchain are called smart contracts, and they are used to allow, carry out, and maintain agreements between untrustworthy parties without the help of a trustworthy third party[48]. Network automation and the conversion of paper agreements into digital contracts were made possible by smart contracts. Smart contracts, being replicated to every blockchain node to guard against contract manipulation, are opposed to traditional contracts and allow users to automate transactions under the oversight of a central authority, thereby codifying agreements and trust relationships[49]. Human error might be decreased to prevent conflicts about such contracts by allowing the operations to be carried out by computers and the services offered by blockchain platforms: without the help of a central server or trusted authority, smart contracts' decentralisation, auto-enforcement capability, and verifiability allow their encoded business

[46] H Snee, C Hine, Y Morey, S Roberts, H Watson, 'Digital methods as mainstream methodology: An introduction', (2016) In Digital methods for social science: An interdisciplinary guide to research innovation. London, Palgrave Macmillan UK, pp. 1-11.
[47] JH Tan, 'Blockchain "Arbitration" for NFT-Related Disputes,' (2023) 16(1) Contemporary Asia Arbitration Journal, pp. 145-186.
[48] Y Zhu, C Peña, A Joy, and M Brouard, 'Digital future of luxury brands: Metaverse, digital fashion, and non-fungible tokens', 2022 31(3) Strategic change, pp.337-343.
[49] A Timoshenko, JR Hauser, 'Identifying customer needs from user-generated content,' (2019) 38(1) Marketing Science, pp. 1-20.

regulations to be carried out in a peer-to-peer network where every node is "equal" and lacks special authority. Therefore, smart contracts are anticipated to completely transform several established industries, including banking, healthcare, and energy. We thoroughly analysed blockchain-enabled smart contracts in this study, covering their use and technical aspects.[50]

Courts adhere to certain norms and criteria when determining whether digital evidence can be admitted and considered during legal procedures. The admissibility of digital evidence is a dynamic field influenced by technological advancements and evolving legal standards. Here are some future trends and policy considerations that may shape the admissibility of digital evidence. Transparency and tamper-proof transaction recording are provided by blockchain technology. It might be essential in guaranteeing the validity and integrity of digital evidence.[51] Courts may need to consider the admissibility of evidence kept on blockchains and the legal standing of blockchain records. Courts will have to decide whether evidence produced by AI and machine learning systems is admissible as these systems gather and analyze more data. One possible policy issue is to set up standards for certifying the correctness and dependability of evidence produced by AI. Provenance, or the details surrounding the creation and history of digital files, can play a significant role in verifying digital evidence's legitimacy and custody chain. Policy frameworks may be created to ensure that metadata is handled and preserved correctly. Policy frameworks may be created to ensure that metadata is handled and preserved correctly.[52]

As the metaverse continues to evolve and expand at an unprecedented rate, the complexity of legal disputes within this virtual realm is bound to escalate. With the convergence of diverse individuals, businesses, and entities in this digital landscape, the question of jurisdictional laws looms large, presenting a challenging maze for legal professionals and stakeholders alike. Delving into the intricacies of the metaverse's legal framework, one realizes that traditional approaches to conflict resolution may prove inadequate in this tech-driven, alternative reality. As traditional court systems grapple with the concept of jurisdiction over virtual spaces, a more agile and innovative method is poised to assume dominance: arbitration. Arbitration, a recognized form of dispute resolution deeply rooted in legal principles, stands poised to play a central role in resolving conflicts within the metaverse. Offering an efficient and authoritative means of settling disputes, it provides metaverse inhabitants with a reliable mechanism for justice in an otherwise uncertain environment. The allure of arbitration lies in its ability to transcend conventional jurisdictional boundaries, allowing for the resolution of metaverse conflicts on an international scale. As digital content intertwines with global audiences, this method presents a universally recognized platform for fair and enforceable rulings. Complex questions surrounding intellectual property, virtual asset ownership, and contractual agreements can find resolution through the

[50] HC Youn, SM Ko, TH Kim, and HJ Jeon, 'Blockchain and AI Meet in the Metaverse,' 2022, Advances in the Convergence of Blockchain and Artificial Intelligence, 73(10.5772).
[51] A Toygar, CE Rohm Jr, J Zhu, 'A new asset type: digital assets', (2013) 22(4) Journal of International Technology and Information Management, p. 7.
[52] S Yong, HY Moon, Y Sohn, M Fernandes, 'A survey of security issues in collaborative virtual environment', (2008) 8(1) Ijcsns, pp. 14-19.

impartiality and expertise of arbitrators specialized in the metaverse domain. By harnessing their knowledge of emerging technologies and legal nuances, arbitrators can navigate the intricate web of virtual disputes, ensuring a balanced and equitable outcome for all parties involved. With the metaverse heralding a new era of interaction and commerce, it is essential to establish a robust and adaptable system for conflict resolution. The incorporation of arbitration as the preferred method in metaverse conflicts not only safeguards the interests of digital content creators and users but also fosters an environment of trust and stability. This approach reflects the growing recognition of digital assets as legitimate forms of property and the need for specialized dispute resolution mechanisms. Thus, through its legally binding rulings, arbitration holds the potential to harmonize, protect, and propel the metaverse towards a future defined by fairness, innovation, and digital progress.[53]

Notwithstanding, it is important to highlight the significant impact the current rules have on the arbitration process. They have not only streamlined and enhanced the efficiency of resolving digital disputes but have also paved the way for greater trust and confidence among parties involved. The provisions allowing parties to maintain their anonymity during proceedings have proven to be particularly valuable in ensuring a level playing field and avoiding any bias. This level of confidentiality ensures that parties can present their cases without fear of repercussion or prejudice. Moreover, the establishment of clear timelines within the rules has had a tremendous impact on the efficiency of dispute resolution. By implementing specific timeframes for each stage of the process, parties are able to anticipate and plan accordingly, reducing unnecessary delays. This expeditious approach to resolving disputes avoids prolonged periods of uncertainty, providing a quicker resolution while still maintaining the necessary thoroughness and integrity. In addition, the authority granted to arbitrators to adapt, revise, or revoke digital assets has been instrumental in ensuring the effectiveness of the resolution mechanism. In the rapidly changing digital landscape, where the value and nature of assets can evolve rapidly, this flexibility is crucial. By empowering arbitrators to make swift decisions regarding digital assets, the resolution process remains up-to-date and capable of addressing emerging issues effectively. This adaptability ensures that the rules remain relevant in the ever-evolving realm of digital disputes.

Looking beyond the UK Jurisdiction Taskforce's Digital Dispute Resolution Rules, the 2018 JAMS Draft Rules Governing Disputes Arising out of Smart Contracts further demonstrate the flexibility and adaptability of dispute resolution in the digital realm. These tailored rules specifically address the unique challenges posed by smart contracts, allowing for a more comprehensive and effective resolution process. By acknowledging and accommodating the intricacies of smart contracts, parties involved in such disputes can have confidence in the ability of arbitration to navigate through complex contractual arrangements. In conclusion, the Digital Dispute Resolution Rules and the JAMS Draft Rules prove that dispute resolution in the

[53] M Turdialiev, 'Legal Discussion of Metaverse Law,' (2023), International Journal of Cyber Law, 1(3).

digital realm is not only possible but can be efficient, fair, and reliable. These rules exemplify the ongoing efforts to keep pace with the ever-changing world of technology and its impact on legal processes. By embracing innovative ideas, maintaining confidentiality, establishing clear timelines, and providing flexibility, these rules ensure that the resolution of digital disputes remains effective and satisfactory for all parties involved. One aspect of these regulations designed for digital disputes is that the arbitrator will only consider the conditions of the smart contract to the degree that they are converted to the English language if there is ambiguity or logical conflict in code.[54]

The strong attraction of cross-border applicability under the New York Convention is a feature of conventional international arbitration. However, due in part to the due process procedural requirements, determining small claims is not adequately time and cost-economical. An arbitral award's enforcement may be a drawn-out, complex, and expensive procedure. Given the nature of the case, a standard arbitral procedure may be too expensive for some types of disputes that occur in the metaverse, such as conflicts between users or between users and platforms.

In a fully immersive three-dimensional environment where products and services are easily accessible online, there is an expectation for efficient conflict resolution processes. Online dispute resolution (ODR), such as decentralized justice platforms like Kleros, Jur, and Aragon, is gaining traction as an alternative to traditional arbitration methods. These dispute-resolution methods are at various stages of development and have yet to be widely adopted.[55] ODR tools included in the platform is probably the best choice if a large amount of trade happens within the metaverse among users or through platforms. Smart contracts used for on-chain decisions come with restrictions that require a lot of confidence in the potential risks and situations, and they are also susceptible to mistakes or misuse. The significance and relevance of utilizing ODR platforms to resolve disputes of low monetary value cannot be overstated. ODR platforms serve as effective and efficient mechanisms for resolving conflicts at a diminished cost, saving both time and resources for all parties involved. By leveraging the power of technology, ODR platforms enable individuals and businesses to navigate and address legal issues in a simplified and accessible manner. Similarly, the evolution of cryptocurrency and NFTs has revolutionized the way we perceive and engage with digital assets: in today's fast-paced and interconnected world, the adoption of ODR platforms empowers disputants to seek timely resolutions without the need for traditional, in-person court proceedings. These platforms offer a variety of tailored features and tools that facilitate communication, negotiation, and the overall dispute resolution process. From online mediation and arbitration to facilitated settlement discussions, ODR platforms provide a comprehensive range of dispute resolution methods.[56]

One of the key advantages is their accessibility: by eliminating the need for

[54] AJ van Niekerk, 'The strategic management of media assets: A methodological approach' (2006) In Allied Academies, New Orleans Congress.

[55] Q Wang, R Li, Q Wang, S Chen, 'Non-fungible token (NFT): Overview, evaluation, opportunities and challenges', (2021) arXiv preprint arXiv:2105.07447.

[56] W Wang, DT Hoang, P Hu, Z Xiong, D Niyato, P Wang, DI Kim, 'A survey on consensus mechanisms and mining strategy management in blockchain networks,' (2019) Ieee Access, 7, 22328-22370.

physical presence, individuals are able to engage in resolving low-value disputes irrespective of geographical constraints. This opens up opportunities for parties who may find it challenging to attend in-person hearings due to location, time constraints, or financial limitations. ODR platforms create a level playing field, ensuring equal access to justice for all, regardless of their circumstances. In the world of cryptocurrency and NFTs, these platforms are revolutionizing the way legal disputes are resolved. Moreover, ODR platforms offer flexibility and convenience, allowing disputants to engage in the process at their own pace and choose the most appropriate time for their discussions. This flexibility enables individuals and businesses to juggle their personal and professional commitments while actively participating in dispute resolution procedures. Another crucial aspect of ODR platforms is the transparency they bring to the dispute resolution process. Through clear communication channels and document sharing capabilities, all parties involved can access relevant information, track progress, and maintain a record of their discussions. This transparency promotes accountability and assists in fostering trust among the disputing parties. In addition to these benefits, ODR platforms contribute to reducing the burden on traditional court systems by diverting low-value disputes to alternative channels, freeing up valuable resources for more complex cases. This efficient allocation of resources allows courts to focus on cases that require their specialized attention, ultimately strengthening the overall justice system [57]. Smart agreements are executable software that operate on top of the blockchain to facilitate, carry out, and maintain a contract between unreliable parties without the involvement of an unbiased third party[58]. Smart contracts enabled network automation and the transfer of paper obligations into digital contracts. Unlike traditional contracts, smart contracts let users automate transactions with a central authority monitoring them, helping formalise agreements and trust relationships. rom enhanced accessibility and convenience to increased transparency and reduced burden on traditional courts, ODR platforms offer a multitude of advantages for individuals and businesses seeking swift and cost-effective resolutions. By harnessing the potential of technology-driven solutions, we can revolutionize the way we approach dispute resolution and ensure justice for all.[59]

Nevertheless, much data, like movies and digital content captured by VR equipment, are often moved and kept in data centres without the required privacy and security safeguards, making them open to cyberattacks inside the Metaverse, a virtual reality. Given these concerns about security and privacy, blockchain technology, with its particular characteristics, provides a practical way to protect data in the Metaverse. [60] The development of safe and transparent methods for registering and transferring ownership is facilitated by blockchain and smart contract technologies, opening the door for the

[57] Y Wang, Z Su, N Zhang, R Xing, D Liu, TH Luan, X Shen, 'A survey on Metaverse: Fundamentals, security, and privacy', (2022) IEEE Communications Surveys Tutorials.
[58] Q Yang, Y Zhao, H Huang, Z Xiong, J Kang, and Z Zheng, 'Fusing blockchain and AI with metaverse: A survey,' 2022 'IEEE Open Journal of the Computer Society", 3, pp.122-136.
[59] AD Yemenici, 'Entrepreneurship in the world of Metaverse: virtual or real?,' (2022) 2(2) Journal of Metaverse, 71-82.
[60] A Schmitz, C Rule, 'Online dispute resolution for smart contracts' [2019] J. Disp. Resol, p. 103.

emergence of virtual property rights and the trading of virtual assets.[61]

With the development of technology, it is now feasible to create more realistic and immersive virtual environments, which creates new and exciting opportunities for exhibiting luxury properties. Instead of only seeing pictures or videos, prospective buyers may now "visit" a house virtually, which helps them get a better sense of the property's layout, amenities, and overall feel.[62] Furthermore, the development of virtual ownership rights and the exchange of virtual assets are made possible by applying blockchain and smart contract technology. As a result, the market for opulent real estate in the metaverse is expanding, and the industry norm is being raised.[63]

Algorithms based on artificial intelligence (AI) can be used to execute smart contracts, handle digital evidence automatically, and even predict future disputes through predictive modelling. As a result, resolution processes might become more proactive and efficient. [64] Another pivotal facet involves fostering cross-platform cooperation, advocating collaboration among diverse metaverse platforms, and establishing standardized procedures for resolving disputes that traverse multiple virtual worlds. Common standards and interoperability mechanisms must be developed to facilitate dispute resolution across several platforms.[65]

Integrating oracles capable of real-time data retrieval in smart contracts further contributes to resolving disputes arising from unforeseen events. Legal frameworks recognizing and safeguarding virtual property rights, particularly concerning digital assets like NFTs and virtual currencies, are essential to clarify ownership and transaction disputes. Lastly, international cooperation in addressing jurisdictional concerns within the metaverse is advocated, promoting the establishment of clear legal frameworks through treaties or agreements for a standardized and globally recognized dispute resolution procedure.[66]

4. The future of digital assets in the Metaverse.

4.1. 4.1 Key Findings.

The study concludes that it is essential to set up a user-centred, open conflict settlement framework, including blockchain for transparency, dealing with issues of authority, and encouraging people from different fields to work together. This method ensures disagreements about digital assets are settled quickly and fairly in the Metaverse. It also keeps the Metaverse's open nature and encourages growth and wealth. Resolving Metaverse disputes requires

[61] R Schroeder, A Huxor, A Smith, 'Activeworlds: geography and social interaction in virtual reality', (2001) 33(7)Futures, pp. 569-587.
[62] M Xu, WC Ng, WYB Lim, J Kang, Z Xiong, D Niyato C Miao, 'A full dive into realizing the edge-enabled Metaverse: Visions, enabling technologies, and challenges,' (2022), IEEE Communications Surveys Tutorials.
[63] P Ortolani, P Wolters, A Janssen, 'International Arbitration and Technology,' (2022) International Arbitration and Technology, 1-264.
[64] SM Park, YG Kim, 'A Metaverse: Taxonomy, components, applications, and open challenges', (2022) 10 IEEE access, 4209-4251.
[65] PG Watts, KF Low, The Case for Cryptoassets as Property', (2022), *Available at SSRN 4354364*.
[66] I Nikolaidis, 'Networking the metaverses', (2007) 21(5) IEEE Network.

close cooperation between engineers, legal experts, and business players. Formulating practical and fair solutions requires an interdisciplinary approach that combines legal knowledge with technical insights and corporate viewpoints. Legal experts contribute their knowledge of jurisdictional concerns, legal frameworks, and user rights to the table, helping to build a regulatory framework that protects people in the Metaverse.[67]

Frameworks for jurisdiction, data protection, and the legal acceptance of digital evidence depend heavily on the junction of legal and technological expertise. Second, the Metaverse is a quickly changing environment where user behaviour, business models, and technology standards constantly change. Working with company stakeholders guarantees that dispute resolution procedures comply with industry standards and are flexible enough to accommodate new developments. This proactive strategy contributes to the general stability of the Metaverse by anticipating and resolving possible conflicts. Third, interdisciplinary approaches encourage the development of novel dispute-resolution techniques. Conventional legal frameworks might not meet the unique difficulties presented by the Metaverse. New and creative solutions, including decentralized management models, smart contract-based resolution of disputes, or industry-specific standards for digital evidence, can be developed by fusing legal, technological, and business viewpoints. In the end, cooperation between technologists, business stakeholders, and legal experts guarantees that Metaverse conflict resolution processes are thorough, equitable, and adaptable to the dynamic character of this digital environment. In addition to helping resolve disputes, this cooperative synergy fosters a regulatory atmosphere that encourages openness, trust, and the Metaverse's responsible expansion.[68]

Collaboration between these disciplines will be essential in the future to shape a legal and technological structure that serves the many demands and interests of the Metaverse's users. As decentralized governance models become more common in virtual communities, individuals will be able to actively influence the norms and regulations of the Metaverse. The transition to community-driven governance will call for adaptable and flexible conflict resolution procedures that consider the varied expectations and values of these online groups.[69]

As users navigate many virtual environments, the emergence of diverse Metaverse platforms may give rise to interoperability issues. Harmonized dispute resolution methods will become more necessary as disputes resulting from cross-platform interactions, ownership of assets across different platforms, and differing terms of service agreements grow more common.

[67] DJ Niemeyer, HR Gerber, 'Maker culture and Minecraft: Implications for the future of learning,' (2015) 52(3) Educational Media International, 216-226.
[68] Nils Köbis and Luca D Mossink, 'Artificial intelligence versus Maya Angelou: Experimental evidence that people cannot differentiate AI-generated from human-written poetry', (2021), Computers in human behavior 114 (2021), 106553
[69] H Ning, H Wang, Y Lin, W Wang, S Dhelim, F Farha, M Daneshmand, A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges' (2023) *IEEE Internet of Things Journal.*

4.2. Future Research Directions

In addressing the imperative of establishing robust mechanisms for conflict resolution within the Metaverse, it is recommended that industry-wide best practices and standards be formulated collaboratively. This collaborative effort should involve technologists, legal professionals, and business stakeholders to devise comprehensive rules to facilitate efficient, equitable, and consistent digital asset dispute resolution. Integrating direct conflict resolution mechanisms into smart contracts is integral to enhancing efficiency.[70]

To resolve disputes across various virtual worlds, efforts must be focused on creating standardized procedures and encouraging collaboration between various Metaverse platforms. Developing common standards and interoperability protocols is essential for smoothing the conflict resolution processes in cross-platform interactions. It is crucial to inform Metaverse users about their rights, obligations, and available dispute resolution channels. Encouraging users to learn about digital asset ownership, transaction security, and available dispute settlement avenues is vital for fostering a well-informed and cooperative online community.[71] Several intricate legal issues surround the Metaverse, including disagreements about jurisdiction, digital assets, and intellectual property.[72]

It is impossible to overestimate the significance of effective conflict resolution methods in this fast-paced digital world. Some of the most important conclusions are that the Metaverse is decentralised, that traditional legal frameworks are difficult to enforce, and that smart contracts and blockchain technology influence virtual property ownership. Effective conflict resolution is essential to maintaining the Metaverse's stability and reliability. Cooperation between technologists, legal experts, and commercial players is essential without a centralised regulatory agency. Developing creative solutions that fit with industry standards and adjust to the Metaverse's changing nature requires an interdisciplinary approach. There is a need for constant cooperation and adaptability as the Metaverse develops. There is a legal void because the swift advancement of technology has surpassed the creation of thorough legal frameworks. Closing the knowledge gap between industrial practices, technological advancements, and legal expertise will take continued cooperation. In addition to facilitating effective dispute resolution, this cooperative synergy will assist the Metaverse's responsible and dependable expansion.

[70] P Milgram, F Kishino, 'A taxonomy of mixed reality visual displays', (1994) 77(12) IEICE TRANSACTIONS on Information and Systems, pp. 1321-1329.
[71] S Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system,' (2008), Decentralized business review.
[72] MD Murray, Trademarks, NFTs, and the Law of the Metaverse (2022) 6 Ariz. LJ Emerging Tech., i.

Del Federico L, 'Riaffermazione e modernizzazione dei diritti dei contribuenti nella trasformazione digitale ' (2024) 1 EJPLT, 136-156.
DOI: https://doi.org/10.57230/EJPLT241LDF

EJPLT
ISSN 2704-8012



Riaffermazione e modernizzazione dei diritti dei contribuenti nella trasformazione digitale*

Reaffirmation and modernization of taxpayers' rights in digital transformation

Lorenzo Del Federico
Professore Ordinario di Diritto tributario
Università degli Studi G. D'Annunzio Chieti – Pescara

Abstract
La trasformazione digitale dei rapporti tra autorità fiscali e contribuenti da origine ad impulsi tecnocratici che mettono in crisi lo Stato di diritto. La trasformazione digitale è concepita come alibi per aggirare i limiti posti dalla legge all'esercizio dei poteri delle autorità fiscali. Tuttavia, è possibile trovare logiche di bilanciamento in ambito sovranazionale, giacché l'OCSE, il Consiglio d'Europa e l'Unione Europea mostrano sensibilità per la protezione dei dati personali ed i rischi legati all'uso dell'intelligenza artificiale.

The digital transformation of relations between tax authorities and taxpayers gives rise to technocratic impulses that undermine the rule of law. Digital transformation is conceived as an alibi to circumvent the limits placed by law on the exercise of the powers of tax authorities. However, it is possible to find balancing logics at a supranational level, since the OECD, the Council of Europe and the European Union show sensitivity to the protection of personal data and the risks linked to the use of artificial intelligence.

* Contributo destinato al volume "*La trasformazione digitale del sistema tributario*" (a cura di F. MONTANARI), contenente gli atti del convegno organizzato dall'Università di Chieti – Pescara, nei giorni 24 e 25 ottobre 2023, nell'ambito del progetto PRIN, *La trasformazione digitale dell'Amministrazione finanziaria*.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: diritto tributario; dati del contribuente; Statuto dei diritti del contribuente; accertamento fiscale; riscossione fiscale; intelligenza artificiale.

Summary: 1. Premessa. – 2. La trasformazione digitale dei rapporti tributari, la marginalizzazione dei diritti dei contribuenti e le prospettive sovranazionali. – 3. Le politiche dell'OCSE. – 4. Le iniziative del Consiglio d'Europa e la giurisprudenza della Corte EDU. – 5. I profili Unionali e la giurisprudenza della Corte di giustizia UE. – 6. Le convergenze sul piano delle garanzie. – 7. I percorsi per salvaguardare i diritti dei contribuenti. – 8. Conclusioni.

1. Premessa.

A livello globale è diffusa la sensazione che la vorticosa trasformazione digitale dei rapporti tributari stia comportando una crescente svalutazione dei diritti dei contribuenti, o quantomeno che i crescenti poteri digitali delle autorità fiscali non siano accompagnati da un corrispondente adeguamento delle garanzie. Ciò ha portato molti studiosi ad auspicare l'elaborazione di una carta dei diritti digitali dei contribuenti o l'adattamento delle carte vigenti[1].

La trasformazione digitale del rapporto tra autorità fiscali e contribuenti sta dando origine ad impulsi tecnocratici che mettono in crisi le fondamenta dello Stato di diritto. La trasformazione digitale è spesso concepita come un alibi per aggirare i limiti posti dalla legge all'esercizio dei poteri delle autorità fiscali.

In tutti gli Stati si percepisce un tentativo di sfruttamento, da parte del Potere Esecutivo, dell'attuale stagione improntata alla trasformazione digitale (in corso non solo in ambito fiscale) come opportunità per ridurre di fatto lo spazio di libertà, emarginando il ruolo del Potere Legislativo.

In materia fiscale, i Governi alimentano il tradizionale fiscalismo, sovraesponendo e strumentalizzando il problema dell'evasione fiscale, per giustificare le loro carenze nella gestione delle politiche economiche e per dare corpo a gravi mortificazioni dello Stato di diritto.

Di fronte allo scenario brevemente delineato risulta necessario uscire dalle logiche nazionali per recuperare un livello elevato di analisi ed elaborazione, non condizionato dalla demagogia e dall'opportunismo, che impantanano il dibattito politico-istituzionale a livello interno.

Nell'ambito della trasformazione digitale, al fine di trovare logiche di bilanciamento nelle relazioni tra autorità fiscali e contribuenti. verrà fatto essenzialmente riferimento ai due forum globali che subiscono meno i

[1] Per molteplici spunti in tal senso v.: P. Pistone, *News taxpayers' rights in the era of digital administration*, in AA.VV., *Digital transformation of Tax Administrations in the European Union*, (a cura di) A. Anton Anton, C. Garcia, Herrera Blanco, Madrid, 2023 24 ss.; F. Montanari, S. Giorgi, *Digital Government Taxpayer's Charter, ibidem, 279*; A. Contrino, *Digitalizzazione dell'amministrazione finanziaria e attuazione del rapporto tributario: questioni aperte e ipotesi di lavoro nella prospettiva dei princìpi generali*, in *Riv. dir. trib.*, 2023, 105 ss.; Id, *Protezione dei dati personali e pervasività delle banche dati fiscali: quale contemperamento?* in AA.VV., *La digitalizzazione dell'amministrazione finanziaria tra contrasto all'evasione e tutela del contribuente*, (a cura di) E. Marello, A. Contrino, Milano 2023, 123.

condizionamenti e gli egoismi nazionali [2], ovvero l'OCSE [3] ed il Consiglio d'Europa, riservando altresì una particolare attenzione all'evoluzione delle politiche dell'Unione Europea, che, pur subendo ormai da tempo i condizionamenti tipici del fiscalismo, mostra una notevole sensibilità rispetto ai temi che riguardano la protezione dei dati personali ed i rischi legati all'utilizzo dei sistemi dotati di intelligenza artificiale.

2. La trasformazione digitale dei rapporti tributari, la marginalizzazione dei diritti dei contribuenti e le prospettive sovranazionali.

Sul piano sovranazionale, per cogliere le potenzialità delle politiche Unionali, ma al tempo stesso i loro limiti sul fronte delle garanzie dei contribuenti, vanno considerati i due settori nevralgici ai fini della trasformazione digitale: quello della protezione dei dati personali e quello dell'intelligenza artificiale.

Tutto il poderoso impianto delle garanzie di cui al Regolamento UE 2016/679 (d'ora in avanti "GDPR" [4]) risulta infatti derogato dall'art. 23, relativo alle "Limitazioni", secondo cui il diritto dell'Unione o dello Stato può limitare, mediante misure legislative, la portata dei diritti tutelati, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare: a) la sicurezza nazionale; b) la difesa; c) la sicurezza pubblica; d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; ecc.

Ciononostante, la stessa norma aggiunge poi che tali misure legislative debbono contenere disposizioni specifiche riguardanti: a) le finalità del trattamento o le categorie di trattamento; b) le categorie di dati personali; c) la portata delle limitazioni introdotte; d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti; e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari; f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento; g) i rischi per i diritti e le libertà degli interessati; h) il diritto degli interessati di essere

---

[2] Sui profili comparatistici v. M. SERRAT ROMANI, *International analysis of digital transformation of Tax Administration and the new Taxpayer's rights in comparative law*, ed A. Collosa, *International analysis of digital transformation of Tax Administration and the new Taxpayer's rights in America,* in AA.VV., *Digital transformation of Tax Administrations in the European Union cit.*, 83, 113.

[3] E' bene evitare di farsi troppe illusioni sul ruolo dell'OCSE, ma è indubbio che al livello multilaterale i paesi sono indotti ad operare con alto livello di analisi ed elaborazione libera (o almeno alleggerita) dai condizionamenti domestici. Almeno questa è la speranza di chi confida nel multilateralismo. Non è un caso che nel 2011, per i suoi primi 50 anni, l'OCSE abbia adottato il motto *"Politiche migliori per vite migliori"*.

[4] General Data *Protection Regulation*; si tratta del noto Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

Soffermandoci sui profili che qui rilevano, si ritiene che si tratti di principi espressivi di un apprezzabile bilanciamento, in quanto la deroga alla tutela dei diritti in materia tributaria: -richiede un intervento legislativo; -fa salva l'essenza dei diritti e delle libertà fondamentali; -deve risultare misura necessaria e proporzionata in una società democratica per salvaguardare i superiori interessi pubblici; -deve comunque assicurare residuali e minimali garanzie attuative, fra le quali spiccano i rischi per i diritti e le libertà degli interessati ed il loro diritto ad essere informati della limitazione[5].

A proposito della base normativa su cui fondare tali deroghe, il considerando n. 41 del Regolamento prevede che laddove si "faccia riferimento a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato". Clausola comprensibile, considerando l'estrema varietà ordinamentale dei diversi Stati membri sul piano delle fonti, ma di certo inidonea a degradare il livello delle garanzie richiesto dalle prescrizioni costituzionali dei diversi Stati. Così, ad. es., nel nostro ordinamento la deroga al Regolamento Unionale dovrebbe necessariamente essere attuata con norma di legge, in ragione dell'equilibrio formale tra norma derogata e norma derogante, ma, soprattutto, in ragione delle prescrizioni costituzionali che sottopongono a riserva di legge le limitazioni della segretezza della corrispondenza e di ogni altra forma di comunicazione (art. 15 Cost.) e l'organizzazione dei pubblici uffici (art. 97 Cost.)[6].

Per quanto riguarda l'intelligenza artificiale, il Regolamento in materia – da ultimo approvato anche dal Parlamento europeo – e del quale dunque si attende ormai la sola pubblicazione in Gazzetta ufficiale[7], riconosce che le azioni delle autorità pubbliche basate su sistemi di IA "sono caratterizzate da un livello significativo di squilibrio di potere e possono portare alla sorveglianza, all'arresto o alla privazione della libertà di una persona fisica, come pure avere altri impatti negativi sui diritti fondamentali" garantiti nella Carta dei diritti fondamentali dell'Unione europea (c.d. carta di Nizza). Ed invero "il sistema di IA, se non è addestrato con dati di elevata qualità, se non soddisfa requisiti adeguati in termini di accuratezza o robustezza, o se non è

[5] È tuttavia opportuno evidenziare che spesso, nella maggior parte degli Stati membri, e segnatamente in Italia, il fiscalismo si riespande prepotentemente. Basti considerare che il d.l. vo 10 agosto 2018, n. 101, nell'adeguare il Codice italiano in materia di protezione dei dati personali (d.l. vo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679, ne ha completamente ignorato tutte le cautele e tutte le residuali garanzie, giungendo addirittura a subire una successiva modifica (mediante d.l. 8 ottobre 2021, n. 139), tale da legittimare deroghe anche mediante meri atti amministrativi generali (art. 2 *sexies*). E per cogliere la brutalità del fiscalismo si consideri che gli atti amministrativi generali in Italia rientrano nelle normali competenze gestorie della P.A. ed hanno un rango molto inferiore rispetto ai veri e propri regolamenti amministrativi (qualificate fonti del diritto). Sul tema v. le acute considerazioni di A. CONTRINO, *Protezione dei dati personali e pervasività delle banche dati fiscali cit.*, 123 ss. Sui profili relativi al considerando n. 41 del Regolamento GDPR v. *infra* note 5 e 30.

[6] Sui profili di illegittimità emergenti al riguardo nell'ordinamento italiano v. nota 4.

[7] Proposta di Regolamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'unione del 21 aprile 2021, noto come AI Act. Si segnala l'ultima versione, accessibile al seguente *link*: *https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_EN.pdf*.

adeguatamente progettato e sottoposto a prova prima di essere […] messo in servizio, può individuare le persone in modo discriminatorio o altrimenti errato o ingiusto. Potrebbe inoltre essere ostacolato l'esercizio di importanti diritti procedurali fondamentali, quali il diritto a un ricorso effettivo e a un giudice imparziale, nonché i diritti della difesa e la presunzione di innocenza, in particolare nel caso in cui tali sistemi di IA non siano sufficientemente trasparenti, spiegabili e documentati" (considerando 38).

Su tali basi l'Unione ha proseguito, ritenendo "opportuno classificare come ad alto rischio una serie di sistemi di IA destinati a essere utilizzati nel contesto delle attività di contrasto, in cui l'accuratezza, l'affidabilità e la trasparenza risultano particolarmente importanti per evitare impatti negativi, mantenere la fiducia dei cittadini e garantire la responsabilità e mezzi di ricorso efficaci. In considerazione della natura delle attività in questione e dei rischi a esse connessi, tra tali sistemi di IA ad alto rischio è opportuno includere, in particolare, i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per valutazione dei rischi individuali, come poligrafi e strumenti analoghi, oppure per rilevare lo stato emotivo delle persone fisiche, individuare 'deep fake', valutare l'affidabilità degli elementi probatori nei procedimenti penali, prevedere il verificarsi o il ripetersi di un reato effettivo o potenziale sulla base della profilazione delle persone fisiche, o valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso delle persone fisiche o dei gruppi, nonché ai fini della profilazione nel corso dell'indagine, dell'accertamento e del perseguimento di reati e dell'analisi criminale nei riguardi delle persone fisiche".

Viceversa, senza che sia esplicitata nei considerando motivazione alcuna, "i sistemi di IA specificamente destinati a essere utilizzati per procedimenti amministrativi dalle autorità fiscali e doganali non dovrebbero essere considerati sistemi di IA ad alto rischio utilizzati dalle autorità di contrasto a fini di prevenzione, accertamento, indagine e perseguimento di reati" (così laconicamente l'ultima parte del considerando 38).

Dal Regolamento emerge comunque che, a norma dell'art. 5, sono sempre e comunque vietate: - alcune forme di elaborazione o uso di sistemi di IA tali da poter provocare discriminazioni e danni, fisici o psicologici; - d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, salve alcune importanti eccezioni per esigenze di ordine pubblico.

Ai nostri fini spicca il divieto di elaborazione o uso "di sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari: i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità".

Ma la grave lacuna, ai fini fiscali, emerge sul fronte delle garanzie relative ai sistemi di IA ad alto rischio (artt. 6 ss.), per l'appunto a priori ed acriticamente escluse per i procedimenti amministrativi delle autorità fiscali e doganali.

In materia fiscale e doganale sono infatti esclusi gli apparati garantistici in tema di: - sistema di gestione dei rischi (art. 9); governance dei dati (art. 10); documentazione tecnica (art. 11); conservazione delle registrazioni (art. 12); trasparenza e fornitura di informazioni (art. 13); sorveglianza umana (art. 14); accuratezza, robustezza e cibersicurezza (art. 15); obblighi dei fornitori dei sistemi di IA (art. 16); sistema di gestione della qualità (art. 17); obbligo di redigere la documentazione tecnica (art. 18); valutazione della conformità (art. 19); log generati automaticamente (art. 20); misure correttive (art. 21); dovere di informazione (art. 22); cooperazione con le autorità competenti (art. 23); altri vari obblighi gravanti su fabbricanti, gestori, utenti ecc. (artt. 24 ss.).

Risulta quindi evidente che se da un lato l'Unione ha fatto storici passi avanti sul piano delle tutele legali e delle garanzie in materia di IA – d'altro canto si tratta della prima legge al mondo in materia –, dall'altro la medesima sembra aver subito i condizionamenti dello strisciante ed immanente fiscalismo, che è riuscito a stralciare il settore dalla rete di protezione dell'AI Act, dando addirittura corpo ad un arretramento rispetto a quanto previsto per la materia tributaria dal Regolamento in materia di protezione dei dati personali.

Diventa quindi indispensabile esplorare le logiche di bilanciamento in ambito OCSE e Consiglio d'Europa (a fianco del quale opera intensamente e proficuamente la Corte EDU), giacché forum globali meno condizionati dal fiscalismo e dagli egoismi nazionali, ferma restando la rilevanza delle politiche Unionali, che, sia pure con palesi contraddizioni, si mostrano all'avanguardia e sensibili rispetto al tema della tutela dei diritti nell'era digitale.

3. Le politiche dell'OCSE.

Nel processo di trasformazione digitale l'OCSE valorizza la «fiducia», intesa come «la convinzione di una persona che un'altra persona o istituzione agirà in modo coerente con le loro aspettative di comportamenti positivi» [8]. La trasformazione digitale arricchisce tale visione delle dinamiche giuridiche ed istituzionali di molteplici sfaccettature, quali l'emergere di incertezze, di gap tecnologici, di disparità fra le persone in ragione del logo grado di alfabetizzazione digitale e della disponibilità di strumenti tecnologici, ma, soprattutto, delle interdipendenze derivanti dalla digitalizzazione dei rapporti.

Poiché la fiducia è considerata «una condizione fondamentale per realizzare pienamente il potenziale di crescita e progresso sociale nell'era digitale» [9], l'OCSE si concentra su un approccio di gestione del rischio tale da garantire la fiducia sia dei singoli individui che delle organizzazioni. Pertanto, con l'aumento dell'utilizzo e della rilevanza dei dati, i rischi per la *privacy* devono essere gestiti

[8] OECD, *OECD Guidelines on measuring trust*, (Paris, 2017).

[9] Par. 18 OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C (80) 58 final, as amended on 11 July 2013 by C (2013) 79. Il tema è attentamente analizzato ed esteso all'IA da C. Garcia Herrera Blanco, *Principles in the use of Artificial Intelligence by Tax Administration: the need to build Trust to enhance its use*, in AA.VV., *Digital transformation of Tax Administrations in the European Union cit.*, 279

meglio, risultando necessaria anche una complessiva evoluzione dei sistemi giuridici.

I rapporti dell'OCSE rivelano il lato «oscuro» dell'importanza della *privacy*: la *privacy* non è cruciale di per sé, in quanto rappresenta un diritto fondamentale, ma non assoluto, non potendo ostacolare la libera circolazione dei dati personali attraverso le frontiere, funzionale all'innovazione e alla crescita economica. Pertanto, il focus dell'OCSE sembra concentrarsi maggiormente sulle modalità dell'acquisizione e della circolazione dei dati, piuttosto che sulla loro protezione, che si configura come elemento accessorio: i diritti individuali rappresentano un mero strumento per infondere fiducia e la fiducia è fondamentale per il corretto flusso dei dati nella più ampia prospettiva dello sviluppo economico.

Ciò è particolarmente evidente fin dalle Linee guida dell'OCSE sulla protezione della *privacy* e dei flussi transfrontalieri dei dati personali. L'obiettivo emergente è quello di impedire agli Stati di creare ostacoli ai flussi transfrontalieri di dati personali «in nome della tutela della riservatezza e delle libertà individuali» se tali limitazioni superano lo standard di protezione[10]. La tutela della *privacy* va quindi bilanciata ed al riguardo sono stati ritenuti particolarmente rilevanti i principi dell'equivalenza e della proporzionalità.

Anche nei più recenti rapporti OCSE, trasparenza e fiducia rappresentano i principali driver per l'evoluzione delle attività di controllo fiscale: "raccogliere quantità così grandi di dati può sollevare questioni di fiducia e necessita di essere attentamente spiegate, giustificate e protette (legalmente e praticamente)"[11].

Più in generale l'OCSE incoraggia una strategia specifica per l'attuazione dei quadri normativi sulla protezione dei dati personali a livello nazionale ma anche un processo di armonizzazione a livello internazionale. Alcuni punti sono identificati come cruciali in entrambi; le strategie nazionali dovrebbero garantire limiti nella raccolta dei dati, ma anche partecipazione e responsabilità individuale[12]. Tra i presidi a tutela della *privacy*, il diritto di accesso e la possibilità di contestazione del trattamento dei dati personali da parte dell'interessato sono generalmente considerati i più rilevanti.

Tuttavia, è bene ribadirlo, a livello generale per l'OCSE (e non solo) la tutela della *privacy* è un diritto fondamentale, ma non assoluto, giacché la preoccupazione di fondo è quella di consentire la libera circolazione dei dati personali attraverso le frontiere, in quanto ritenuta funzionale all'innovazione e alla crescita economica[13].

Ma -soprattutto in passato- l'OCSE ha mostrato una apprezzabile attenzione anche alle garanzie dei contribuenti[14], giungendo ad identificare tra i diritti

[10] Par. 18 OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C (80) 58 final, as amended on 11 July 2013 by C (2013) 79.
[11] OECD, *Tax Administration 3.0: The Digital Transformation of Tax Administration*, (Paris, 2020).
[12] Secondo le linee guida OCSE i principi fondamentali che dovrebbero applicarsi a livello nazionale riguardano: la limitazione della raccolta; la qualità dei dati; la specificazione dello scopo; la limitazione dell'uso; le garanzie di sicurezza e riservatezza; la partecipazione; la responsabilità.
[13] P. PISTONE, *News taxpayers' rights in the era of digital administration cit.*, 24 ss. Anche la modernizzazione della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, promossa dal Consiglio d'Europa nel 2018, si preoccupare di salvaguardare i flussi internazionali di dati (v. infra § 3).
[14] OECD, *Taxpayers' rights and obligations – A survey of the legal situation in OECD countries*, Paris, 2019.

meritevoli di tutela sia il diritto alla protezione dei dati personali sia il diritto alla riservatezza e segretezza[15].

Più di recente i diritti dei contribuenti sono stati ripresi e considerati nel rapporto dell'OCSE *"Tax Administration 2015 […]"*[16], con riguardo allo specifico settore dello scambio di informazioni[17].

In sintesi, dal complessivo orientamento dell'OCSE si desume che i contribuenti hanno il diritto di aspettarsi che le autorità fiscali non si intromettano inutilmente sulla loro *privacy* e che evitino perquisizioni irragionevoli e richieste di informazioni non specificamente rilevanti. Anzi, il diritto alla riservatezza e alla segretezza implica che le informazioni a disposizione delle autorità fiscali riguardanti gli affari di un contribuente siano confidenziali e possano essere utilizzate solo per gli scopi specificato nella legislazione fiscale.

Diventa quindi possibile cogliere alcuni spunti evolutivi:

– il primato della libera circolazione dei dati sulla tutela dei diritti;

– la "soluzione" di eventuali conflitti tra i due principi sulla base del principio di proporzionalità;

– la lettura del principio di proporzionalità in modo tale da salvaguardare il più possibile la libera circolazione dei dati;

– il significato primario del diritto alla *privacy,* alla riservatezza ed alla segretezza e la necessità di garantire il diritto di accesso e di contestare il trattamento dei dati personali da parte dell'interessato.

Tuttavia, è chiaro che l'OCSE si pone nella particolare visuale del potenziamento della trasparenza fiscale, della cooperazione fra Stati e dello scambio di informazioni, per cui gli spunti evolutivi rielevanti sul piano dei diritti dei contribuenti nell'era digitale risultano alquanto marginali.

Ma spicca una ineludibile esigenza di fondo.

I poteri delle pubbliche autorità debbono essere sempre bilanciati con i diritti dei contribuenti, mediante il fondamentale principio di proporzionalità.

Per quanto marginale rispetto alle politiche OCSE il tema della tutela dei diritti del contribuente/cittadino[18], prende corpo in ragione del ruolo dell'OCSE quale "custode" del rapporto di fiducia tra autorità e cittadini nella prospettiva globale dello sviluppo economico.

Del resto, il problema dei diritti nell'era della digitalizzazione è centrale nel dibattito globale sotto tutti i profili[19]; in tutti i settori del diritto emergono esigenze che in materia fiscale risultano palesi ed impellenti: per poter «avere

---

[15] OECD, *Centre for Tax Policy and Administration, Practice Note – Taxpayers' Rights and Obligations,* Paris, 2003.

[16] OECD, *Tax Administration 2015: Comparative Information on OECD and Other Advanced and Emerging Economies*, Paris, 2015, 282.

[17] OECD, *Keeping It Safe: The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes*, Paris, 2012, 10; OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C (80)58 final, as amended on 11 July 2013 by C, 2013, 79.

[18] Ma v.; V. WÖHRER, *Data Protection and Taxpayers' Rights: Challenges Created by Automatic Exchange of Information*, IBFD, 2018; R.C.L. PEREIRA, R. CODORNIZ LEITE, *The emergence of transparency and exchange of information for tax purposes on request as an international tax custom,* in *Intertax*, 2020, 624.

[19] S. FALK, A. RÖMMELE, M. SILVERMAN, *Digital Government Leveraging Innovation to Improve Public Sector Performance and Outcomes for Citizens*, Berlin, 2017; A. PAJNO, F. DONATI, F.A. PERUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione*, Bologna, 2022. Si consulti il recentissimo libro di G. FINOCCHIARO, *Intelligenza Artificiale. Quali regole?*, Bologna, 2023.

fiducia nel proprio sistema fiscale e rispettare i propri obblighi secondo la legge, i contribuenti devono avere fiducia in coloro che sono spesso sensibili le informazioni finanziarie non vengono divulgate in modo inappropriato intenzionalmente o accidentalmente»[20].

Il problema è che «i diritti» e «la legge» non riescono a tenere il passo della trasformazione digitale [21]. La continua e inarrestabile digitalizzazione dei rapporti tributari rende lo scambio di informazioni molto più semplice e diretto: di conseguenza emergono nuove esigenze di tutela e di equilibrio tra diversi interessi[22]. Ed è in tale contesto che ha preso corpo la modernizzazione della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, promossa dal Consiglio d'Europa nel 2018 (v. infra § 3).

Pertanto, l'OCSE fornisce suggerimenti ai governi affinché curino un bilanciamento tra gli enormi vantaggi che la tecnologia offre al Fisco nello scambio di informazioni e la fiducia che i cittadini devono avere nelle loro istituzioni: «i poteri più forti per le autorità fiscali devono essere combinati con una più forte tutela dei diritti dei contribuenti»[23]. Ed è chiaro che da questo punto di vista si aprono spiragli anche sul versante dell'utilizzo dell'IA, quantomeno in ragione del fatto che qualsivoglia sistema di IA è fondato su potentissimi *data base* nei quali sono stoccati, organizzati e gestiti enormi quantità di dati personali; l'intelligenza artificiale – secondo un'espressione ormai nota – si nutre di dati[24].

4. Le iniziative del Consiglio d'Europa e la giurisprudenza della Corte EDU.

Sul versante della protezione dei dati personali si riscontra un importante ruolo del Consiglio d'Europa ed un recente contributo della Corte EDU, intervenuta con due diverse ed opposte sentenze, la prima del 2021 alquanto rinunciataria, la seconda del 2023 decisamente orientata a favore della salvaguardia delle garanzie.

La Corte è stata chiamata ad occuparsi del diritto alla protezione dei dati personali a fronte della legislazione ungherese, che prevedeva la pubblicazione di una lista di evasori sul sito della Autorità fiscale nazionale, anche con evidenza dei dati personali. Tuttavia, non si è trattato della mera applicazione dei principi della CEDU, giacché sullo sfondo delle controversie si staglia la modernizzazione della Convenzione sulla protezione delle persone rispetto al

[20] OECD, *Keeping It Safe: The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes*, cit., 5.
[21] D.U. GALETTA, *Public Administration in the Era of Database and Information Exchange Networks: Empowering Administrative Power or Just Better Serving the Citizens ?, in EU Public Law*, 2019, 171.
[22] V. WÖHRER, *Data Protection and Taxpayers' Rights,* cit.; P. PISTONE, *News taxpayers rights in the era of digital administration,* cit., 18 ss.
[23] E. KRISTOFFERSSON, M. LANG, *Tax Secrecy and Tax Transparency*, in *The Relevance of Confidentiality in Tax Law*, Bristol, 2013, 2.
[24] Cfr. Commissione consultiva della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, *Report on Artificial Intelligence. Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, 25 gennaio 2019. L'intersezione tra le regole che governano i sistemi dotati di intelligenza artificiale e la disciplina in materia di protezione dei dati perdonali, in particolare, è magistralmente approfondita nel recente lavoro di G. FINOCCHIARO, *Intelligenza artificiale*, cit.

trattamento automatizzato di dati a carattere personale, promossa dal Consiglio d'Europa nel 2018, ormai ratificata da molti Stati, ma non ancora entrata in vigore.

Con la prima sentenza del 2021 la Corte aveva ritenuto che la valutazione di proporzionalità delle misure legislative nazionali dovesse essere rimessa alla discrezionalità degli Stati, salvo i casi di manifesta irrazionalità; conseguentemente, stando al caso concreto, la pubblicazione su internet dei dati personali degli evasori da parte dell'Autorità fiscale è stata considerata compatibile con l'art. 8 della CEDU in materia di protezione della riservatezza, ritenendosi tale ingerenza nella vita privata giustificata e proporzionata in una società democratica, ossia rientrante nel margine di apprezzamento concesso agli Stati in materia di scelte di politica sociale ed economica, al cui interno rientra quella fiscale[25].

Questa pronuncia rinunciataria è stata poi ribaltata dalla Grande Camera della Corte EDU, con una coraggiosa e sofferta decisione del 9 marzo 2023[26], in cui, nel medesimo caso, è stata rinvenuta la violazione dell'art. 8 cit., giacché il margine di apprezzamento riconosciuto agli Stati, anche in materia tributaria, non è illimitato, risultando doverosamente subordinato al rispetto di requisiti tali da assicurare un bilanciamento tra interessi pubblici, interesse fiscale e tutela dei contribuenti.

Nello specifico la Corte ha ritenuto che debbano essere bilanciati e ponderati in base al principio di proporzionalità i seguenti parametri:

- l'interesse pubblico alla diffusione delle informazioni;

-la natura delle informazioni divulgate;

-le ripercussioni ed i rischi per la vita privata riguardo alle persone interessate;

-la tipologia del 'mezzo di comunicazione' tramite il quale sono rese note le informazioni, in quanto, a seconda del mezzo utilizzato, i dati possono avere una diversa diffusione;

-i principi fondamentali sulla protezione dei dati, compresi quelli sulle finalità, conservazione, minimizzazione dei dati ed accuratezza dei dati.

Orbene, nella concreta fattispecie, il legislatore ungherese non aveva ponderato i suddetti interessi e principi, giacché non aveva effettuato alcuna puntuale valutazione dei possibili effetti della divulgazione dei dati personali sulla vita privata dei contribuenti, né dell'efficacia dei presidi esistenti per assicurare la tutela dell'interesse erariale alla luce del principio di

---

[25] Sentenza 21 gennaio 2021, con note di: A. TOMO, *Liste evasori e CEDU: riflessioni in merito alla (dubbia) proporzionalità delle misure di public shame*, in *Riv. tel. dir. trib.,* 2021, I, 677 ss.; A. MARINELLO, *Pubblicazione di dati personali dei contribuenti e rispetto della vita privata secondo la Corte EDU: la difficile ricerca di un equilibrio tra interesse fiscale e diritto alla riservatezza,* in *Riv. dir. trib.,* 2022, IV, 12.

[26] Secondo la Corte EDU*, Grand Chamber* – sentenza del 9 marzo 2023 sul caso L.B. contro Ungheria (n. 36345/16) – *la pubblicazione di un elenco di grandi evasori, corredato di dati personali dei contribuenti, sul sito* web *di un'Autorità fiscale nazionale deve essere considerata in contrasto con l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), in materia di protezione della vita privata e del diritto alla riservatezza. Di per sé, la misura prevista dalla legislazione nazionale ungherese persegue lo scopo legittimo di proteggere il benessere economico del Paese, tanto che, almeno in astratto, essa potrebbe essere considerata necessaria in una società democratica. Tuttavia, in assenza di una adeguata ponderazione degli interessi in gioco da parte del Parlamento nazionale, l'adozione generalizzata di tale misura deve essere considerata sproporzionata in relazione alla portata dei dati personali pubblicati e alle modalità di pubblicazione* (in *Riv. dir. trib.*, 2023, IV, 119, con nota di A. MARINELLO, *"Name and shame" e diritto al rispetto della vita privata: la Grand Chamber della Corte EDU censura la gogna mediatica per gli evasori fiscali.*

proporzionalità. Nel dettaglio la Corte ha censurato l'automatismo della misura, basata esclusivamente su profili oggettivi ed operante "indipendentemente dall'esistenza o meno di alcuna colpa soggettiva o di altre circostanze individuali"; ancor più nel merito la misura "non richiedeva una ponderazione degli interessi individuali e pubblici concorrenti o una valutazione individualizzata della proporzionalità da parte dell'Autorità fiscale".

La circostanza decisiva è stata rinvenuta nell'assenza di una adeguata ponderazione degli interessi in gioco non solo sul piano amministrativo di attuazione della misura, ma anche da parte del Parlamento nazionale sul piano dell'attività legislativa.

Si tratta di una circostanza estremamente rilevante, ben oltre la logica della motivazione elaborata dalla Corte EDU, in quanto la novellata Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, promossa dal Consiglio d'Europa sin dal 2018, a fronte del deciso rafforzamento delle garanzie sulla protezione dei dati (artt. 5 -8), afferma che "non è ammessa alcuna eccezione alle disposizioni" sulle garanzie, ma ammette che "è possibile derogare] quando tale deroga è prevista dalla legge […] e costituisce una misura necessaria, in una società democratica: a per la protezione della sicurezza dello Stato, per la sicurezza pubblica, per gli interessi monetari dello Stato o per la repressione dei reati […]" (art. 9). Pertanto, in sintonia con la logica decisoria della Corte EDU, l'introduzione di misure atte a comprimere o limitare i diritti sulla protezione dei dati personali, deve sempre e comunque salvaguardare i principi di legalità e di necessità, declinando quest'ultima in termini di proporzionalità ed in ottica di ponderazione e bilanciamento fra i vari interessi in gioco.

D'altro canto, è lo stesso Regolamento in materia di protezione dei dati personali a porre l'accento sull'equilibrio degli opposti interessi e a considerare il diritto alla protezione dei dati personali necessario oggetto di bilanciamento, disponendo: "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ottemperanza al principio di proporzionalità"[27].

Prescindendo dal caso in questione, in prospettiva, stando alla materia tributaria, si potranno ipotizzare deroghe soltanto in presenza di specifiche esigenze di protezione della sicurezza e degli interessi monetari dello Stato o per la repressione dei reati, giammai in presenza di meri inadempimenti,

[27] Così il considerando n. 4 del GDPR. Sulla necessità del bilanciamento tra diritto alla protezione dei dati personali e altri diritti fondamentali si v. G. FINOCCHIARO, *Il necessario bilanciamento di interessi*, in G. FINOCCHIARO (diretto da), *La protezione dei dati personali in Italia*, Bologna, 2019, 25 ss. Per inciso, è opportuno rilevare come anche la giurisprudenza di legittimità, in più di un'occasione ha ricordato come nonostante il diritto alla protezione dei dati personali sia qualificato come pretesa ad esigere una corretta gestione dei propri dati personali, pur rientrando nei diritti fondamentali della persona, il medesimo non rappresenti "un totem al quale possano sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale" e, dunque, la disciplina in materia "va coordinata e bilanciata da un lato con le norme che tutelano altri e prevalenti diritti (tra questi, l'interesse pubblico alla celerità, trasparenza ed efficacia all'attività amministrativa); dall'altro, con le norme civilistiche in tema di negozi giuridici" (in tal senso Cass., sent. n. 10280/2015). Sul punto v. A. RICCI, *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in *Contratto e Impresa*, 2017, 2, 586-612.

violazioni amministrative e/o comportamenti antigiuridici bagatellari o comunque irrilevanti ai suddetti fini.

5. I profili Unionali e la giurisprudenza della Corte di giustizia UE.

Un cenno sul quadro normativo Unionale è stato anticipato nell'introduzione, qui sembra sufficiente riprendere alcuni spunti desumibili dalla giurisprudenza che, pur presentando un interessante casistica non è ancora giunta a maturazione sui temi della tutela dei dati personali e dell'IA, solo di recente oggetto di interventi normativi organici nel diritto dell'Unione.

Frequenti, ma sterili, risultano essere le pronunce sulla tutela dei dati personali nell'ambito della cooperazione e dell'assistenza reciproca in materia tributaria[28].

Viceversa meritevoli di particolare attenzione sono certamente le due sentenze Digital Rights Ireland del 2014 e Tele2 Sverige del 2016, con le quali la Corte di giustizia ha dichiarato incompatibili norme che prevedevano, seppur per rilevanti fini di interesse pubblico (contrasto al terrorismo e alla criminalità internazionale), la raccolta ed il trattamento di dati personali su base generalizzata in palese contrasto con il principio di proporzionalità. Le controversie riguardavano l'obbligo (Svezia e Regno Unito) gravante sui fornitori di servizi di comunicazione elettronica di conservare i dati, sulla base di una Direttiva del 15 marzo 2006. La Corte ha prima dichiarato invalida la Direttiva 2006/24/CE (8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland),* e poi ha affermato l'incompatibilità di una normativa interna tale da consentire la raccolta e conservazione generalizzata e indifferenziata dei dati (cause riunite C-203/15 e C-698/15, *Tele2 Sverige*): in linea di principio gli Stati possono prevedere, a titolo preventivo, la raccolta ed il trattamento di dati allo scopo di contrastare gravi fenomeni di criminalità, a condizione che tale raccolta sia limitata allo stretto necessario per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone implicate, nonché la durata di conservazione prevista; in ogni caso, l'accesso delle autorità nazionali ai dati deve essere assoggettato a condizioni protettive, tra cui in particolare un controllo preventivo da parte di un'autorità indipendente e la conservazione dei dati nel territorio dell'Unione.

L'orientamento garantista della Corte di giustizia è stato poi ampliato dalla sentenza 27 settembre 2017, causa C-73/16, *Puskar,* avente ad oggetto la contestazione del contribuente in merito all'acquisizione di dati personali per l'inserimento di liste di persone che rivestivano fittizie funzioni direttive e societarie in banche dati fiscali, al fine di garantire la riscossione delle imposte e la lotta alle frodi fiscali; la Corte si è pronunziata a favore dell'ammissibilità della misura, rinviando al giudice nazionale la valutazione di "proporzionalità"

[28] V. da ultimo Corte giust. UE, 6 ottobre 2020, cause riunite C-245/19 e C-246/19, *Etat Luxembourgeois*, ed in dottrina S.M. RONCO, *Data Protection in Direct Tax Matters and Developments from the EU Standpoint: The Case of Automatic Exchange of Information*, in *Intern. Tax Studies*, 2020, 20 ss

dell'adempimento rispetto agli obiettivi. Ma per la verità tale sentenza è più articolata e meritevole di considerazione di quanto non emerga *prima facie*[29].

Nel merito infatti la Corte ha ritenuto che l'art. 47 della Carta di Nizza "deve essere interpretato nel senso che esso non osta a una normativa nazionale che subordina la possibilità di esperire un ricorso giurisdizionale da parte di una persona che afferma sia stato violato il suo diritto alla tutela dei dati personali […] al previo esaurimento dei rimedi disponibili dinanzi alle autorità amministrative nazionali, a condizione che le modalità concrete di esercizio di detti rimedi non pregiudichino eccessivamente il diritto ad un ricorso effettivo dinanzi a un giudice […]". Al riguardo, infatti, la Corte -nel dispositivo- giunge ad evidenziare la necessità "che l'esaurimento dei rimedi disponibili dinanzi alle autorità amministrative nazionali non comporti un ritardo sostanziale per la proposizione di un ricorso giurisdizionale, produca la sospensione della prescrizione dei diritti interessati e non provochi costi eccessivi". Considerazioni da sole sufficienti a scardinare i sistemi di tutela differita dei diritti dei contribuenti diffusi in molti Stati membri (e soprattutto in Italia ed in Francia). Inoltre, prosegue la Corte, l'art. 47 cit. "deve essere interpretato nel senso che esso osta a che un giudice nazionale respinga, quale mezzo di prova di una violazione della tutela dei dati personali […], un elenco […] presentato dalla persona interessata e contenente dati personali di quest'ultima, qualora tale persona si sia procurata l'elenco senza il consenso, richiesto per legge, del responsabile del trattamento di tali dati, a meno che tale rigetto sia previsto dalla normativa nazionale e rispetti al tempo stesso il contenuto essenziale del diritto ad un ricorso effettivo e il principio di proporzionalità"[30].

Infine sulla questione centrale la Corte ha concluso ritendendo che il quadro 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 procede con la redazione di un elenco di persone […], senza il consenso delle persone interessate, a condizione, da un lato, che a tali autorità siano stati affidati compiti di interesse pubblico […], 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".

Infine, per ora, spiccano ancora due importanti sentenze garantiste in tema di protezione dei dati personali nei settori dell'antiriciclaggio e dei controlli tributari.

Con la sentenza 24 febbraio 2022, C-175/20, SS SIA la Corte di giustizia è stata chiamata a pronunciarsi su una normativa Lettone attributiva di

[29] Per qualche spunto v. ad es. A. CONTRINO, *Protezione dei dati personali e pervasività delle banche dati fiscali,* cit., 112-114.

[30] Sul delicato tema del rapporto tra diritto alla protezione dei dati personali ed esigenze di giustizia v. C. DEL FEDERICO, *Il diritto alla protezione dei dati personali nel processo civile: la prevalenza delle esigenze di giustizia*, in *Giustiziacivile.com*, 2020, 9, 3 ss.

penetranti poteri alle Autorità fiscali in merito all'acquisizione di dati personali ai fine di attività di controllo tributario[31].

Si tratta di sentenza molto importante ai nostri fini in quanto vertente sull'interpretazione dell'art. 5 GDPR – rubricato "principi applicabili al trattamento di dati personali" – e sulla protezione dei dati personali in materia tributaria. Nello specifico si trattava di una controversia tra l'Autorità fiscale Lettone ed una società commerciale avente ad oggetto la comunicazione mensile di tutti i dati dei contribuenti che pubblicavano annunci di vendita di veicoli sul sito internet gestito dalla società commerciale intermediaria. La Corte di giustizia ha chiarito che le disposizioni del GDPR non ostano a che l'Autorità fiscale di uno Stato membro imponga ad una società commerciale di comunicare informazioni relative ai contribuenti propri clienti, fermo restando che "l'amministrazione tributaria […] non può derogare alle disposizioni dell'articolo 5 […] se un diritto siffatto non le è stato riconosciuto da una misura legislativa ai sensi dell'articolo 23 […]"; la Corte ha poi puntualizzato che "le disposizioni del Regolamento […] devono essere interpretate nel senso che non ostano a che l'amministrazione tributaria […] imponga a un fornitore di servizi di annunci pubblicati su Internet di comunicarle informazioni relative ai contribuenti che abbiano pubblicato annunci […] 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".

Da ultimo la Corte con una sentenza del 22 novembre 2022, ha dichiarato l'invalidità di alcune disposizioni della Direttiva antiriciclaggio 2015/849 che consentivano l'accessibilità al pubblico, senza condizioni, per tutte le informazioni contenute in un Registro dei titolari effettivi delle società e delle altre entità costituite nel territorio dello Stato (Lussemburgo), ritenendo che ciò determinasse un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali (artt. 7 ed 8 della Carta di Nizza), palesemente proporzionata rispetto all'obiettivo di prevenire il riciclaggio di denaro ed il finanziamento del terrorismo[32].

---

[31] Sentenza edita in *Dir. prat. trib. int.*, 2022, 908, con nota di A. TOMO, *La "forza centripeta" del diritto alla protezione dei dati personali: la Corte di giustizia sulla rilevanza in ambito tributario dei principi di proporzionalità, accountability e minimizzazione*. La sentenza brilla per garantismo e pragmatismo, ma è stata fortemente criticata da alcuni autori italiani, in quanto la Corte a proposito della "*misura legislativa*" nazionale idonea *ex* art. 23 GDPR ad introdurre deroghe al regime generale di protezione dei dati personali, ha osservato che "*il riferimento in tale Regolamento a una «misura legislativa» non richiede necessariamente l'adozione di un atto legislativo da parte del Parlamento*" (CONTRINO A., *Protezione dei dati personali e pervasività delle banche dati fiscali,* cit,.115-116). Si tratta di uno spunto incidentale giustificato dal considerando n. 41 del Regolamento GDPR, ma nella prospettiva italiana le preoccupazioni sono condivisibili, considerata la deriva fiscalista della legislazione italiana che sta tentando di comprimere quanto più possibile i diritti dei contribuenti depotenziando i limiti posti dal GDPR (v. *retro* note 4 e 5).

[32] Sentenza *WM, Sovim SA,* 22 novembre 2022, cause riunite n. C-37/20 e C-601/20, con nota M. LASSALLE, *Who cares about financial privacy?: the Court of Justice in WM, Sovim SA v Luxembourg Business Registers*, in *EU Law Live,* 16 dicembre 2022.

6. Le convergenze sul piano delle garanzie.

Come si è avuto modo di evidenziare, collocando l'indagine sull'evoluzione digitale dei rapporti giuridici a livello dell'OCSE, del Consiglio d'Europa, dell'Unione Europea e delle giurisdizioni sovranazionali si colgono alcuni significativi spunti a favore della riaffermazione e della modernizzazione dei diritti dei contribuenti[33]. Spunti non univoci, sofferti e talvolta contraddittori, ma comunque apprezzabili rispetto alle aride esperienze nazionali, nelle quali la trasformazione digitale dei rapporti tributari è concepita come strumento di deciso rafforzamento dei poteri delle autorità fiscali, con mortificazione dei diritti dei contribuenti.

A livello nazionale la trasformazione digitale si muove a senso unico.

Basti pensare al caso Italiano in cui si assiste da oltre un decennio al continuo e costante potenziamento degli apparati informatici, dei data base e degli strumenti tecnologici a disposizione dell'Agenzia delle Entrate, senza alcun segnale sul versante dell'adeguamento dei diritti dei contribuenti alla trasformazione digitale[34].

Di tutto ciò è sintomatico il ridimensionamento delle garanzie Unionali in tema di protezione dei dati personali e del ruolo del Garante nazionale della *privacy* sul fronte dei rapporti tributari[35]. Ma possono essere colti anche esempi relativi all'attività di controllo.

Ormai da anni tutto il sistema degli adempimenti dei contribuenti, delle comunicazioni e delle notifiche è stato informatizzato, ma purtroppo in ragione del diffuso gap tecnologico si ha notizia di centinaia di casi di contribuenti vittime di incolpevoli errori informatici.

Orbene, in materia tributaria non è prevista la rimessione in termine per errore scusabile (rimessione invece normalmente prevista in tutti i procedimenti civili ed amministrativi), per cui è emersa la necessità di introdurre una norma secondo cui "*l'amministrazione in ambito procedimentale e il giudice in ambito processuale, dispongono, anche d'ufficio, la rimessione in termini per errore scusabile in ragione delle oggettive ragioni di incertezza su questioni di diritto o di gravi impedimenti di fatto o di errori conseguenti dall'uso delle procedure informatiche e digitali*"[36]. Ma le Istituzioni nazionali si sono mostrate insensibili, nonostante la presenza di molteplici norme che viceversa

---

[33] Sulla necessità dell'approccio multilivello per la tutela dei contribuenti v. da ultimo A. CARINCI, Il sistema multilivello dei diritti del contribuente, tra pluralità di fonti e molteplicità di modelli di tutela, in A. CARINCI, T. TASSANI (a cura di*), I diritti del contribuente. Principi, tutele e modelli di difesa*, Milano, 2022, 3 ss.

[34] Su tali vicende v.: A. CONTRINO, *Digitalizzazione dell'amministrazione finanziaria e attuazione del rapporto tributario cit.*; Id., *Banche dati tributarie, scambio di informazioni fra autorità fiscali e "protezione dei dati personali"* cit.; F. FARRI, *Digitalizzazione dell'amministrazione finanziaria e diritti dei contribuenti*, in *Riv. dir. trib.*, 2021, 115 ss.; A. CARINCI, *Fisco e privacy: storia infinita di un apparente ossimoro*, in *Fisco*, 2019, 4407 ss.

[35] Su tale fenomeno nell'esperienza Italiana v.: A. CARINCI, *Fisco e privacy,* cit.*;* C. LAUDANNA, *Norme privacy in rapporto alla lotta all'evasione fiscale*, in *Data Protection Law*, 2021, 1, 34 ss. *(https://www.dataprotectionlaw);* L. IZZO, *Il difficile rapporto tra il diritto alla privacy e il dovere di contribuzione alla spesa pubblica*, in EJPLT, 2022, 2, 197-200 (https://doi.org/10.57230/EJPLT222LI); G. CONSOLO, *Sul trattamento dei dati personali nell'ambito delle nuove procedure automatizzate per il contrasto dell'evasione fiscale*, in AA.VV., *La digitalizzazione,* cit., 186-188. Per una lettura in chiave comparata si segnala C. FRANCIOSO, *Automated decision making by tax authorities and protection of taxpayers' rights in a comparative perspective*, in *Rivista Trimestrale di Diritto Tributario*, 2023, 3, 541 ss.

[36] Nell'ambito delle recenti riforme tributarie in Italia, l'Associazione Italiana dei Professori e degli Studiosi del Diritto Tributario - AIPSDT ha vanamente proposto di inserire nello Statuto dei Diritti del contribuente una norma volta a colmare tale grave lacuna.

consentono rimedi a fronte di errori dell'Amministrazione o derubricano a mere irregolarità tollerabili vere e proprie violazioni di legge presenti negli atti impositivi.

Prendiamo poi il caso della fatturazione elettronica, in Italia ormai da tempo obbligatoria per legge: in passato, l'Agenzia delle Entrate doveva svolgere indagini cartolari complesse, effettuare accessi, controlli ed ispezioni per acquisire materialmente i dati relativi ai contribuenti, alle operazioni, alle fatture, ecc.; ora l'Agenzia riceve per via telematica tutte le copie di tutte le fatture tempo reale, man mano che vengono emesse, così come riceve immediata comunicazione telematica di tutti i flussi dei versamenti iva; il sistema consente all'Agenzia di acquisire in tempo reale dati personali di imponente rilevanza qualitativa e quantitativa, tanto da aver occasionato anche interventi da parte del Garante nazionale per la *privacy*[37]. Se in passato il termine per i controlli iva era di cinque anni, dalla presentazione della dichiarazione iva annuale, ora, con l'avvento della fatturazione elettronica, stante l'immediata conoscibilità delle operazioni e dei flussi, le notifiche tramite posta elettronica certificata ecc., tale termine dovrebbe essere ridotto, con adattamento consequenziale, basato sul principio di proporzionalità; viceversa si è assistito ad un ampliamento di tali termini, mediante interventi legislativi strumentalmente giustificati dal contrasto dell'evasione.

Lo stesso vale per la riscossione dei crediti tributari: l'Agenzia della Riscossione normalmente ha un termine di prescrizione di dieci anni, ma questo termine è anacronistico. Una volta l'Agente della riscossione doveva cercare fisicamente o manualmente su base cartacea beni mobili, immobili, conti bancari, ecc., e quindi avviare il pignoramento; oggi la ricerca viene effettuata in via informatica in pochi minuti, grazie ai potenti database a disposizione dell'Agente di riscossione (che ovviamente contengono dati personali meritevoli di protezione)[38]; inoltre l'Agenzia può ora avvalersi di notifiche a mezzo posta elettronica e di tanti altri moderni strumenti digitali; di conseguenza, il termine decennale dovrebbe essere notevolmente ridotto. Si è invece assistito ad una enorme dilatazione dei tempi della riscossione, mediante atti interruttivi dei termini o norme di legge di proroga, tanto che ancora oggi il carico dei crediti tributari da riscuotere ricomprende somme risalenti addirittura agli anni 2.000 – 2.010[39].

Del resto, come sempre, nella logica dello Stato di diritto, una misura di garanzia per il contribuente è quanto più è ragionevole, quanto più risponde anche all'interesse pubblico. Ed è appena il caso di evidenziare che non ha senso consentire che l'Amministrazione impieghi cinque anni per effettuare un controllo che tecnicamente può essere effettuato in pochi mesi o impieghi venti anni per riscuotere un credito. L'affidamento su lunghi termini di decadenza e/o prescrizione induce l'Amministrazione a rallentare la tempistica della propria attività, dando corpo a gravi inefficienze.

Nella maggior parte dei Paesi a fiscalità complessa, la trasformazione digitale ha profondamente inciso sui rapporti tributari, molto di più di altre branche del diritto, in quanto, in questa materia, la digitalizzazione è stata

[37] Sui quali v. i riferimenti di cui alla nota 33.
[38] Sul tema v. i riferimenti di cui alla nota 33.
[39] OCSE, *Italy's tax administration. A review of institutional and governance aspects*, 2016.

caratterizzato dalla coattività, giustificata da logiche di efficienza e modernizzazione funzionali alle esigenze della fiscalità di massa (del controllo di una platea dei contribuenti sempre più ampia) ed ai crescenti bisogni della finanza pubblica. Eppure, nonostante la marcata trasformazione digitale dell'azione impositiva, l'esigenza di adeguamento delle garanzie dei contribuenti al mutato contesto stenta ad assumere evidenza ed è fortemente resistita dalla autorità fiscali, che tendono a marginalizzarla dal dibattito politico istituzionale, dall'attenzione del legislatore e più in generale dall'agenda tributaria.

Ecco prender corpo la chiave di lettura che spinge l'indagine sull'evoluzione digitale dei rapporti giuridici a livello dell'OCSE, del Consiglio d'Europa, dell'Unione Europea e delle giurisdizioni sovranazionali, laddove è possibile cogliere alcuni spunti a favore della riaffermazione e della modernizzazione dei diritti dei contribuenti, che meritano di essere ripresi e valorizzati.

Il GDPR si pone come importante punto di riferimento laddove per un verso assicura un adeguato livello di tutela per la protezione dei dati personali, ma poi, come è inevitabile, consente di limitare, mediante misure legislative, la portata dei diritti tutelati, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare vari interesse pubblici di particolare rilevanza, tra i quali, ai nostri fini, spicca l' interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria (v. retro § 1). E' inoltre necessario che le misure legislative di deroga contengano disposizioni specifiche riguardanti il bilanciamento tra i vari interessi in gioco, con particolare riferimento alle finalità ed alle categorie di trattamento, alle categorie di dati personali, alla portata delle limitazioni, alle garanzie per prevenire abusi o accessi o trasferimenti illeciti, l'indicazione precisa del titolare del trattamento, dei periodi di conservazione, delle garanzie applicabili ecc.; soprattutto va salvaguardato il diritto degli interessati di essere informati della limitazione (a meno che ciò possa compromettere la finalità della stessa).

L'AI Act non contiene un analogo livello di garanzie specificamente dedicato ai sistemi di IA, ma postula comunque l'applicabilità del GDPR alla protezione dei dati personali posti a base dei sistemi di IA (e comunque sui sistemi di IA è il diritto interno a fungere da solido baluardo garantistico – v. infra § 6).

Viceversa, la novella della Convenzione sui dati personali, promossa dal Consiglio d'Europa, segue uno schema giuridico analogo a quello del coevo Regolamento in materia di protezione dei dati personali, laddove ammette la deroga alle garanzie "quando tale deroga è prevista dalla legge […] e costituisce una misura necessaria, in una società democratica" per la protezione della sicurezza dello Stato, per la sicurezza pubblica, per gli interessi monetari dello Stato o per la repressione dei reati.

Il punto di convergenza, desumibile anche dalle sentenze passate in rassegna (§§ 3 e 4), è quindi quello della possibilità di limitare i diritti sulla protezione dei dati personali per esigenze finanziarie, ferma restando tuttavia la salvaguardia dei principi di legalità, di necessità e di proporzionalità, mediante ponderazione e bilanciamento fra i vari interessi in gioco; il tutto declinato alla luce del noto principio di minimizzazione dettato dal Regolamento e secondo cui il

trattamento dei dati personali dovrebbe avere ad oggetto soltanto i dati strettamente necessari e pertinenti rispetto alle specifiche finalità perseguite.

E vero che il GDPR, rispetto alla Convenzione, prevede un superiore livello di tutele, che debbono essere comunque salvaguardate anche in caso di deroghe; ed è altrettanto vero che gli interessi monetari dello Stato, rilevanti ai fini delle deroghe consentite dalla Convenzione, sembrano molto più delimitati rispetto all'interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, cui fa riferimento il Regolamento, ma è il suindicato punto di convergenza ad orientare l'orientamento garantista della Corte EDU e della Corte di giustizia UE.

Dal canto suo anche l'OCSE evoca la necessità di un bilanciamento fra i vari interessi in gioco: i poteri delle autorità fiscali debbono rispondere al principio di proporzionalità e soprattutto debbono essere regolamentati ed esercitati in modo da salvaguardare la fiducia che i cittadini devono avere nei loro governi.

7. I percorsi per salvaguardare i diritti dei contribuenti.

A questo punto vanno tratteggiati i percorsi utili per riaffermare e modernizzare i diritti dei contribuenti nell'era digitale.

Riprendere, e contestualizzare rispetto ai rapporti tributari, il sistema delle garanzie del Regolamento in materia di protezione dei dati personali ed il collaterale sistema delle garanzie della novella Convenzione del Consiglio d'Europa sui dati personali.

Prendere atto che una base normativa per fondare ed individuare i diritti digitali dei contribuenti esiste e risulta alquanto solida e strutturata a livello sovranazionale, stanti le garanzie poste dal GDPR e dalla novella Convenzione sui dati personali.

Acquisire la consapevolezza della necessità di sottoporre a stretta interpretazione ed applicazione i presupposti e le misure di deroga ai sistemi di garanzia, in conformità dei criteri di prudenza e fedeltà rispetto alla ratio legis, che, di volta in volta, fa del sistema di garanzie la regola base e considera la deroga come eccezione alla regola.

Con conseguenziale rigoroso vaglio critico sul rispetto delle condizioni di ammissibilità e legittimità di tali deroghe.

Valorizzare le linee guida dell'OCSE sulla necessità di bilanciamento fra i vari interessi in gioco, sul principio di proporzionalità e sulla salvaguardia del rapporto di fiducia fra cittadini ed Amministrazione.

L' "*acquis*" dello Stato di diritto non può essere sopraffatto dalla trasformazione digitale. Anzi, man mano che la trasformazione digitale prende forma e si rafforzano i poteri delle autorità fiscali, anche il sistema delle garanzie dei contribuenti deve essere modernizzato e proporzionalmente rafforzato.

Nella salvaguardia dell'"*acquis*" dello Stato di diritto l'ordinamento giuridico Italiano ha maturato un significativo grado di metabolizzazione dell'applicazione dell'IA ai fini dell'istruttoria e delle decisioni amministrative, riferibile de plano anche all'istruttoria ed alle decisioni tributarie.

Dopo un inziale dibattito dottrinale e giurisprudenziale vi è ormai concordia nel recepire i ragionevoli ed antesignani approdi cui è giunto il Consiglio di Stato.

E' stato chiarito che di fronte a «procedure seriali o standardizzate, implicanti l'elaborazione di ingenti quantità di istanze e caratterizzate dall'acquisizione di dati certi ed oggettivamente comprovabili e dall'assenza di ogni apprezzamento discrezionale..., l'assenza di intervento umano... e l'affidamento di tale attività a un efficiente elaboratore elettronico appaiono come doverose declinazioni dell'art. 97 Cost. coerenti con l'attuale evoluzione tecnologica»[40]. Tuttavia, è stato acutamente precisato come «l'utilizzo di procedure "robotizzate"» non possa essere «motivo di elusione dei princìpi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa», quale quelli di «pubblicità e trasparenza»[41].

In tale ottica laddove vengano introdotte forme di una automatizzazione del procedimento amministrativo, assume rilevanza ancora più accentuata l'obbligo di motivazione, in quanto «la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice»[42]. Tirando le fila "in uno scenario di decisioni amministrative adottate grazie a strumenti ICT quali gli algoritmi d'intelligenza artificiale (debole o forte che sia), l'obbligo di motivazione, lungi dal perdere significato, ne esce rafforzato"[43].

Sul piano della legislazione, nei diversi ordinamenti, si riscontra l'inerzia ed il disinteresse per la riaffermazione e la modernizzazione dei diritti dei contribuenti. In alcuni ordinamenti si rinviene da tempo la presenza di apposite carte dei diritti digitali dei cittadini, per lo più collegate all'avvento del c.d. *e-government*, ma ormai da anni emerge una diffusa ritrosia ad affrontare il problema di un loro reale ed efficacie adeguamento alla vorticosa evoluzione digitale in atto.

Fa eccezione la recente proposta dell'Unione per una "Dichiarazione sui diritti e principi digitali per il decennio digitale", che nasce su iniziativa politica del Parlamento, grazie a sollecitazioni provenienti dall'opinione pubblica[44]. A

---

[40] Cons. Stato, sez. VI, 8 aprile 2019, n. 2270, punto 8.1.

[41] Cons. Stato n. 2270/2019 cit., punto 8.2.

[42] Cons. Stato n. 2270/2019 cit., punto 8.4.

[43] In tal senso, tra le tante, Cons. Stato: n. 2270/2019 cit.; 13 dicembre 2019, n. 2963; 13 dicembre 2019, n. 8472; 4 febbraio 2020, n. 881 (con pregnanti riferimenti alla normativa sovranazionale). Per un quadro del dibattito e degli approdi concreti cui esso ha dato luogo nella giurisprudenza amministrativa v.: , D.U. GALETTA, *Digitalizzazione e diritto ad una buona amministrazione (Il procedimento amministrativo, fra diritto UE e tecnologie ICT*, in R. CAVALLO PERIN, D.U. GALETTA (a cura di), *Il Diritto dell'Amministrazione Pubblica digitale*, Torino, 2020, 85 ss.; Id., *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in *Riv. It. dir. Pubbl. com.*, 2020, 3; E. CHITI, B. MARCHETTI, N. RANGONE, *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni italiane: prove generali*, in A. PAJNO, F. DONATI, F.A. PERUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione, Bologna, 2022, 43 ss. Sulla rilevanza degli orientamenti del CdS anche in materia tributaria* v.: F. PAPARELLA, *Procedimento tributario, algoritmi e intelligenza artificiale: potenzialità e rischi della rivoluzione digitale*, in AA.VV., *La digitalizzazione dell'amministrazione finanziaria tra contrasto all'evasione e tutela del contribuente*, (a cura di) E. MARELLO, A. CONTRINO, Milano 2023, partic. 32-35; S. DORIGO, *L'intelligenza artificiale ed il possibile "rinascimento del sistema sanzionatorio tributario*, *ibidem*, partic. 90-94; D. CONTE, *Digitalizzazione, data protection e tecniche di profilazione nell'attività di accertamento tributario: quali diritti per i contribuenti?, ibidem*, partic. 152 ss. e per l'adeguamento dello statuto dei diritti del contribuente, 174 ss.

[44] "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale", 26 gennaio 2022 COM(2022) 28 final, ora promossa dal Parlamento, dal Consiglio e dalla Commissione.

livello Unionale, quindi, sebbene non sia ancora maturata la consapevolezza della necessità di modernizzare i diritti dei contribuenti nei confronti delle Autorità fiscali, è comunque avvertita l'esigenza di adeguamento dei diritti dei cittadini nell'era digitale.

Tuttavia, ormai, la vorticosa trasformazione digitale degli ordinamenti giuridici e dei rapporti tributari impone l'adeguamento non solo dei diritti digitali dei cittadini, ma anche delle carte dei diritti dei contribuenti, presenti nei diversi sistemi tributari

8. Conclusioni.

Per quanto rileva specificamente in questa sede, i percorsi utili per riaffermare e modernizzare i diritti del contribuente nell'era digitale sono stati tratteggiati, ma sullo sfondo si pone una questione epocale: si tratta di capire se limitarsi all'aggiornamento dei diritti tradizionali o elaborare nuovi diritti peculiari dell'era digitale[45].

I diritti tradizionali potrebbero essere semplicemente essere riaffermati, introducendo specificità "digitali". Ad esempio, il diritto a motivazioni chiare ed alla trasparenza dell'attività amministrativa dovrebbe includere l'esplicitazione degli algoritmi su cui si basa la decisione e le ragioni per cui l'Amministrazione ha applicato tale algoritmo, dando conto delle situazioni di fatto e di diritto, dell'iter logico seguito ecc.

In ogni caso, la codificazione dei diritti tradizionali sembra essere meno problematica, in quanto è ragionevole supporre che il nocciolo duro dei diritti sarà comunque riconosciuto ed adeguato in via interpretativa al contesto digitale.

Viceversa, la sfida più impegnativa riguarda i nuovi diritti dell'era digitale, ma, quantomeno a livello nazionale, siamo ancora in una fase di scarsa consapevolezza da parte dell'opinione pubblica e di disinteresse da parte delle istituzioni, che per la materia tributaria risultano condizionate dall'imperante fiscalismo.

Un primo nucleo dei nuovi diritti digitali dei contribuenti è di massima identificabile nei generali sistemi delle garanzie poste dal GDPR e dalla novella Convenzione sui dati personali, aventi portata normativa e cogente, sia pure con i limiti suindicati.

Un ulteriore e nuovo catalogo dei diritti digitali va altresì prendendo corpo, per ora sul piano della soft law, mediante la "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale". Tra i nuovi diritti digitali per il decennio digitale spiccano:

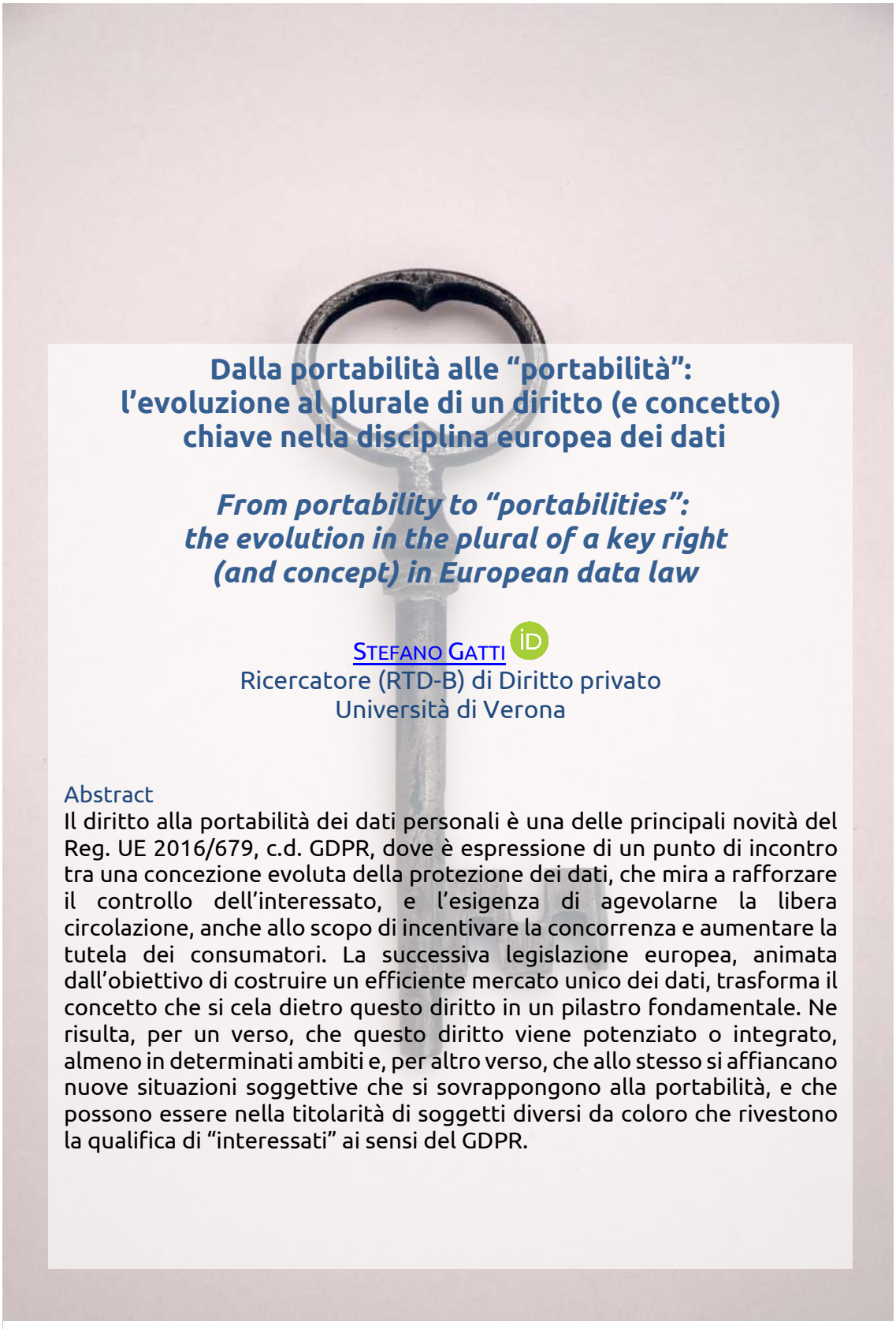
- il diritto alla connettività;
- il diritto ad una rete internet neutra ed aperta in cui le applicazioni, i servizi e i contenuti non siano bloccati o degradati in modo ingiustificato;
- il diritto all'istruzione, alla formazione e all'apprendimento permanente per le competenze digitali di base e avanzate;

[45] Sul punto v.: M. SERRAT ROMANI, *International analysis of digital transformation of Tax Administration cit.,* 102 ss.; F. MONTANARI, S. GIORGI, *Digital Government Taxpayer's Charter cit.*

- il diritto a disconnettersi per l'equilibrio tra vita professionale e vita privata in un ambiente digitale;
- il diritto ai servizi pubblici digitali online;
- il diritto di non subire aggravi istruttori, nel senso che a nessuno deve essere chiesto di fornire dati più spesso di quanto necessario durante l'accesso ai servizi pubblici digitali;
- il diritto ad una identità digitale accessibile, sicura e affidabile;
- il diritto dei cittadini all'accesso ed al riutilizzo su vasta scala delle informazioni della pubblica amministrazione;
- la libertà di scelta nelle interazioni con algoritmi e sistemi di intelligenza artificiale (ogni persona deve poter godere dei benefici offerti dall'intelligenza artificiale facendo le proprie scelte informate nell'ambiente digitale, e rimanendo al contempo protetta dai rischi ai diritti fondamentali);
- il diritto alla trasparenza in merito all'uso degli algoritmi e dell'intelligenza artificiale, per fare in modo che le persone, quando interagiscono con essi, siano autonome, responsabili e informate;
- la garanzia che i sistemi algoritmici siano basati su insiemi di dati adeguati al fine di evitare discriminazioni illecite e consentano la supervisione umana dei risultati;
- la garanzia di sistemi digitali e di intelligenza artificiale sicuri e gestiti nel pieno rispetto dei diritti fondamentali;
- il diritto alla protezione dei dati personali online.

Gatti S, 'Dalla portabilità alle "portabilità": l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati' (2024) 1 EJPLT, 157-177.
DOI: https://doi.org/10.57230/EJPLT224SG

EJPLT
ISSN 2704-8012



Dalla portabilità alle "portabilità": l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati

From portability to "portabilities": the evolution in the plural of a key right (and concept) in European data law

STEFANO GATTI
Ricercatore (RTD-B) di Diritto privato
Università di Verona

Abstract
Il diritto alla portabilità dei dati personali è una delle principali novità del Reg. UE 2016/679, c.d. GDPR, dove è espressione di un punto di incontro tra una concezione evoluta della protezione dei dati, che mira a rafforzare il controllo dell'interessato, e l'esigenza di agevolarne la libera circolazione, anche allo scopo di incentivare la concorrenza e aumentare la tutela dei consumatori. La successiva legislazione europea, animata dall'obiettivo di costruire un efficiente mercato unico dei dati, trasforma il concetto che si cela dietro questo diritto in un pilastro fondamentale. Ne risulta, per un verso, che questo diritto viene potenziato o integrato, almeno in determinati ambiti e, per altro verso, che allo stesso si affiancano nuove situazioni soggettive che si sovrappongono alla portabilità, e che possono essere nella titolarità di soggetti diversi da coloro che rivestono la qualifica di "interessati" ai sensi del GDPR.

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

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
The right to personal data portability is one of the main novelties of the EU Reg. 2016/679, so called GDPR. In this Regulation, data portability acts as a meeting point between an advanced conception of data protection, which aims to strengthen the data subject's control over his or her own data, and the need to facilitate the free movement of data, also with the aim of boosting competition and increasing consumer protection. In subsequent European legislation aimed at creating an efficient single market for data, the concept underpinning the right to data portability becomes a key pillar. As a result, on the one hand, this right is strengthened or complemented, at least in certain areas; on the other hand, the right to data portability is joined by new overlapping subjective rights, which may be in the hands of parties other than GDPR "data subjects".

Keywords: portabilità dei dati; diritto alla portabilità; dati personali e non personali; protezione e circolazione dei dati personali

Sommario: 1. Premessa. Le varie forme della portabilità e l'art. 20 GDPR come punto di osservazione della ricerca. – 2. Il diritto alla portabilità dei dati personali nel GDPR: un innovativo strumento di autodeterminazione dell'interessato… – 3. … il cui potenziale è frenato da numerose limitazioni di compromesso. – 4. La progressiva affermazione della portabilità come propellente della circolazione dei dati: il Regolamento europeo relativo ai dati non personali (c.d. Regolamento Free-flow), la Legge europea sulla governance dei dati (Data Governance Act) e la Legge europea sulla governance dei dati (Data Governance Act) e la Legge europea sui mercati digitali (Digital Markets Act). – 5. L'ulteriore evoluzione della portabilità nell'architettura dei più recenti interventi normativi dell'UE: la compiuta rottura degli argini soggettivi del diritto dell'interessato nella Legge europea sui dati (Data Act). – 6. La duplice veste della portabilità nella Proposta di regolamento sullo spazio europeo dei dati sanitari (European Health Data Space Act). – 7. Osservazioni conclusive. La declinazione al plurale della portabilità e la sua rilevanza al di fuori della disciplina dei dati.

1. Premessa. Le varie forme della portabilità e l'art. 20 GDPR come punto di osservazione della ricerca.

Questo lavoro riflette sullo sviluppo del concetto di portabilità dei dati nella magmatica disciplina europea ad essi dedicata, in tumultuosa espansione dall'emanazione del Regolamento europeo sulla protezione dei dati personali (Reg. UE 2016/679, d'ora in avanti abbreviato con l'acronimo inglese, invalso nella prassi, GDPR). Il dirompente diritto dell'interessato codificato nell'art. 20 GDPR offre un punto di osservazione privilegiato per seguire le traiettorie evolutive della portabilità anche negli atti normativi successivi, consentendo di misurare i traguardi di volta in volta raggiunti nel garantire il controllo e l'effettiva circolazione delle informazioni a chi, avendone la legittimazione, vi dà impulso. Lo stesso legislatore europeo suggerisce questa prospettiva allorché compara espressamente le disposizioni più recenti alla versione "base" della portabilità, che viene, al pari di altri diritti dell'interessato, "rafforzata" o

"integrata". Allo stesso tempo, l'insistenza sull'obiettivo della circolazione dei dati ha reso presto stretta, per la portabilità, la veste esclusiva di un diritto del data subject: il concetto corre infatti più veloce di questa forma, con l'emersione nella normativa di ulteriori strumenti che si sganciano dalla disciplina della protezione dei dati in senso stretto – sempre presupponendone, però, il rispetto, in ossequio al principio (costantemente ribadito) della prevalenza del GDPR su altre norme eventualmente confliggenti. Alla portabilità, come si vedrà, si collegano ora non solo il diritto previsto dall'art. 20 del Regolamento, ma anche prerogative che possono venire esercitate da soggetti diversi dai data subjects, e, più in generale, una condizione dei dati che li rende pronti alla circolazione[1].

2. Il diritto alla portabilità dei dati personali nel GDPR: un innovativo strumento di autodeterminazione dell'interessato…

Fin dalle prime indagini sulle novità introdotte dal GDPR, è stato messo in luce il carattere innovativo e polivalente del diritto dell'interessato alla portabilità dei dati personali[2]. Emancipandosi dal già noto diritto all'accesso (art. 15 GDPR), ancora inserito in una prospettiva che guarda con una certa cautela il trattamento dei dati, la portabilità (art. 20 GDPR) è espressione di una prospettiva dinamica, finalizzata a garantire all'interessato la gestione attiva e il riuso dei propri dati[3].

La polivalenza della portabilità è sottolineata dalla moltitudine delle *rationes* collegate a questo diritto: accanto a quella, basilare, di riequilibrare il rapporto tra titolare del trattamento ed interessato[4], rafforzando il controllo di quest'ultimo sui propri dati[5], anche per consentirgliene uno sfruttamento

[1] Sul carattere «*multi-faceted*» del concetto di portabilità, v. già R. JANAL, *Data Portability – A tale of Two Concepts*, in *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, 2017, Vol. 8, 59 - 69. Segnala l'emersione e il consolidamento, nelle relazioni di mercato, del nuovo paradigma della 'condivisione dei dati' G. MARINO, *Accesso, portabilità e condivisione nella disciplina europea del mercato dei dati*, in AA. VV., *Persona e mercato nella società digitale*, a cura di G. GUZZARDI, Napoli, 2024, 53 ss.

[2] Per tutti, v. S. TROIANO, *Il diritto alla portabilità dei dati personali*, in AA. VV., *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. ZORZI GALGANO, Milano-Padova, 2019, 199 ss.; A. RICCI, *I diritti dell'interessato*, in AA. VV., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, n. 101, a cura di G. FINOCCHIARO, Bologna, 2019, 219.

[3] E. BATTELLI, G. D'IPPOLITO, *Il diritto alla portabilità dei dati personali*, in AA. VV., *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice della Privacy*, a cura di E. TOSI, Milano, 2019, 193.

[4] GRUPPO DI LAVORO ARTICOLO 29 (WP29), *Linee guida sul diritto alla portabilità*, adottate il 13 dicembre 2016 e da ultimo riviste e adottate il 5 aprile 2017, 4. Consultabili online: https://ec.europa.eu/newsroom/article29/items/611233 (ultimo accesso: 18 luglio 2024).

[5] Considerando 68 GDPR. Va comunque sottolineato che, nel quadro giuridico previgente, il complesso di diritti dell'interessato sui propri dati personali (artt. 12 ss. dir. 95/46/CE, attuati in Italia prima nell'art. 13 legge 31 dicembre 1996, n. 675, e infine trasfusi nell'art. 7 d.lgs. 196/2003, c.d. codice della *privacy*, oggi abrogato) già suggeriva un'impostazione non limitata alla tradizionale prospettiva difensiva nei confronti di ingerenze esterne, ma aperta all'idea di un controllo dell'interessato sulle informazioni personali e, di conseguenza, sull'identità rilevata al pubblico: v. E. BARGELLI, sub art. 7, in AA. VV., *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196 («Codice della* privacy*»)*, a cura di C.M. Bianca e F.D. Busnelli, I, Padova, 2007,134 ss., la quale ha evidenziato che tale controllo non sfociava in una logica proprietaria sui dati, quanto, piuttosto, nell'enfasi dell'autodeterminazione informativa della persona (che risponde pur sempre ad una logica di bilanciamento). Il diritto alla portabilità, rispetto a questo quadro, esalta «la *dimensione dinamica* del controllo, proiettando la protezione nella sfera della disponibilità dei dati da parte dello stesso interessato»: S. TROIANO, *op. cit.*, 199.

economico[6], sono state evidenziate le conseguenze positive sulla platea dei consumatori e, più in generale, degli utenti di servizi online. La portabilità elimina infatti un ostacolo di natura tecnica, che rende più difficoltoso cambiare fornitore di tali servizi, anche se l'offerta del concorrente è più conveniente (c.d. effetto lock-in) [7]. Al rafforzamento del consumatore (consumer empowering)[8] segue l'incentivo ad una competizione positiva tra imprese, in una duplice direzione: per un verso e in termini generali, la maggiore libertà di movimento degli utenti spinge i fornitori ad elevare gli standard qualitativi e la convenienza economica della propria offerta; per altro verso, e in termini più specifici, l'aspettativa maturata di godere di questa libertà induce le imprese a sviluppare o a reperire sul mercato tecnologie innovative per assicurare ai consumatori l'effettività di questo diritto[9].

Oltre ai vantaggi di natura economica, di immediata percezione, merita altresì sottolineare l'intimo collegamento con la sfera della personalità dell'interessato: il diritto alla portabilità, permettendo una circolazione fluida delle informazioni personali sotto il controllo dell'interessato, costituisce un potente mezzo nelle mani degli individui per costruire ed affermare la propria identità nell'ambiente digitale, superando le barriere fisiche dello spazio e del tempo[10]; essa contribuisce, inoltre alla creazione di sistemi più efficienti di gestione dei propri dati personali, ciò che incrementa le possibilità di esercizio

[6] GARANTE EUROPEO DEI DATI PERSONALI (EDPS), *Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability*, Opinion 7/2015, 13. Consultabile online: https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf (ultimo accesso: 18 luglio 2024).

[7] In merito all'effetto positivo della portabilità sui cc.dd. *switching costs* e, in particolare, di quelli «*data-induced*», v. J. KRÄMER, P. SENELLART, A. DE STREEL, *Making Data Portability more effective for the Digital Economy. Economic Implications and regulatory Challenges*, *Report*, Centre on Regulation in Europe (CERRE), 2020, 55 ss., nonché 272 ss. i quali sottolineano la limitata efficacia del diritto, per come congegnato nel GDPR, nei confronti delle situazioni di *lock-in* generate dal c.d. effetto network (ivi, 57: «Network effects arise whenever a consumer's value of a good or service depends on how many other consumers are using the same good or service»): per contrastare un tale effetto, la portabilità dovrebbe avere ad oggetto, più che singoli set di dati, l'identità dell'interessato *(identity portability*), che comprende i collegamenti (come "amici" o "follwers") che, attraverso il primo servizio, sono stati instaurati con altre persone.

[8] V. G. COLANGELO, M. MAGGIOLINO, *From fragile to smart consumers: shifting paradigm for the digital era*, in *Computer Law & Security Review*, 2019, Vol. 35, 173 - 181.

[9] Sulla valenza concorrenziale del diritto alla portabilità, v., tra i molti, E. BATTELLI, G. D'IPPOLITO, *op. cit.*, 187 ss., i quali (ivi, 217 ss.), sulla scorta di quanto già osservato dal WP 29, in esordio delle linee guida citate sopra alla nota 4 (ivi, 4), sottolineano che rimane ferma la natura del diritto, che appartiene non già alle logiche della concorrenza ma, specificamente, al diritto della protezione dei dati personali: l'impatto che, indiscutibilmente, questo nuovo strumento dell'interessato ha sul mercato disvelerebbe piuttosto un obiettivo di orientarne lo sviluppo (tecnologico) verso una dimensione «aperta e inclusiva del ruolo dell'utente/interessato».

[10] M. FENWICK, M. FERTIK, P. JURCYS, T. MINSSEN, *Data Portability Revisited. Toward the Human-Centric, AI-Driven Data Ecosystems of Tomorrow*, articolo sottoposto alla rivista *Common Market Law Review* e consultato nella versione pre-stampa disponibile al sito https://ssrn.com/abstract=4475106 (ultimo accesso: 18 luglio 2024). La portabilità si candida a divenire strumento di controllo dei propri dati anche in funzione di costruire e governare la propria identità digitale (sul cui dinamismo v., da ultimi, i riferimenti di M. TESCARO, *L'identità digitale e la profilazione dell'utente*, in AA. VV., *Manuale di diritto privato dell'informatica*, a cura di R. BOCCHINI, Napoli, 2023, 79 ss.; S. SICA, V. D'ANTONIO, I *diritti della personalità in rete*, ivi, 91 ss.). Per una riflessione sull'intima connessione tra la portabilità e la personalità dell'individuo, anche in un sistema, quello argentino, dove il corrispondente diritto non è stato codificato, v. A. LAJE, *El derecho a la portabilidad de datos como derecho personalísimo*, in AA. VV., *Diritto privato e nuove tecnologie. Riflessioni incrociate tra esperienze giuridiche a confronto*, a cura di S. TROIANO, Napoli, 2022, 9 ss.

e di tutela dei propri diritti della personalità[11], ad esempio del diritto alla salute[12].

La portabilità concepita dal GDPR è, in sostanza, lo strumento congegnato per permettere alle persone fisiche di autodeterminarsi con riguardo ai propri dati[13] (e grazie ai propri dati[14]), sia sul piano patrimoniale sia su quello personale.

Secondo una logica di flessibilità che mira ad adeguarne l'attuazione a seconda del grado di avanzamento tecnologico dei vari settori di mercato, il diritto dell'interessato si snoda in due versioni. La prima, più elementare, consiste in due poteri che possono essere esercitati anche disgiuntamente dall'interessato: a) richiedere al titolare del trattamento di trasmettergli i dati a lui previamente «forniti» (purché trattati con mezzi automatizzati[15] sulla base del consenso oppure dell'esecuzione di un contratto che lega questi soggetti), in un formato con requisiti minimi di interoperabilità («formato strutturato, di uso comune e leggibile da dispositivo automatico»); b) trasmettere i dati ricevuti dal titolare del trattamento ad un diverso titolare del trattamento senza impedimenti da parte del primo (art. 20, par. 1, GDPR). La seconda forma di portabilità, più avanzata, riguarda le medesime categorie di dati e legittima l'interessato a richiedere il trasferimento diretto degli stessi da un titolare del trattamento ad un altro, ma è limitato a quei casi in cui una tale attività risulti «tecnicamente fattibile» (art. 20, par. 2, GDPR).

3. … il cui potenziale è frenato da numerose limitazioni di compromesso.

Nonostante la centralità di questo diritto nella costruzione di una dimensione antropocentrica dell'ambiente digitale[16], spiccano, già ad una piana lettura dell'attuale formulazione dell'art. 20 GDPR, specie se confrontata con

[11] Sulla portabilità si basano i Personal Information Management Systems (PIMSs), i quali, offrendo agli interessati un servizio di raccolta dei dati personali detenuti dai vari titolari del trattamento e di gestione degli stessi in una interfaccia unica, rappresentano un'occasione di (modesto) guadagno per gli interessati e agevolano l'esercizio dei diritti su quei dati (revoca del consenso, cancellazione, rettifica, e la stessa portabilità). L'attività di questi intermediari di dati è ora regolata dal Reg. UE 2022/868, relativo alla governance europea dei dati (su cui *infra*, par. 4).

[12] *Infra*, par. 5.

[13] Il diritto alla portabilità può essere dunque concepito come strumento che fissa uno standard ancora più elevato del diritto alla protezione dei dati personali (sulla cui autonomia come diritto della personalità, anche sul piano dei contenuti e della disciplina, nonostante l'indubbia valenza strumentale alla realizzazione di altri diritti e l'ottica di bilanciamento che lo stesso sovente impone, v. C.M. Bianca, *Note introduttive*, in Aa. Vv., *La protezione dei dati personali*, cit., XX ss., nonché Id., *Diritto civile*, 1, *La norma giuridica. I soggetti*, Milano, 2002, 180). Come osserva S. Troiano, *op. cit.*, 199ss., tuttavia, l'evoluzione della «proiezione positiva» della protezione dei dati personali impressa dalla portabilità svela la logica polifunzionale di tale strumento, tesa non solo ad enfatizzare l'autodeterminazione dell'individuo, ma anche a rafforzare «una visione patrimonialistica e obiettivizzata dei dati personali» e a concorrere alla «regolamentazione del mercato dei dati».

[14] V. D. Copetti Cravo, *How to Make Data Portability Right More Meaningful for Data Subjects*, in *European Data Protection Law Review*, 2022, Vol. 8, 53.

[15] Ancorché vi sia intervento umano: L.R. Bianchi, *Il diritto alla portabilità dei dati*, in Aa. Vv., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, a cura di R. Panetta, Milano, 2019, 224.

[16] Sottolineano la dimensione *user-centric* della portabilità già P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, in *Computer Law & Security Review*, 2018, Vol. 34, 193 - 203; v. anche considerando 3 del Reg. UE 2022/868 (DGA).

quella degli altri diritti dell'interessato, numerose limitazioni, frutto della soluzione di compromesso adottata, nel percorso legislativo, dalle istituzioni dell'Unione[17]. Queste limitazioni trovano in larga parte spiegazione, per un verso, in ostacoli di natura tecnica[18] e, per altro, nei possibili rischi nei quali possono incorrere, per effetto di questo diritto, i soggetti del trattamento. Senza perdere di vista la prospettiva dell'interessato[19], occorre prendere in considerazione anche quelle del titolare del trattamento e dei terzi. Il primo, oltre a sopportare l'onere economico della richiesta, corre principalmente il rischio di essere costretto a svelare informazioni, deducibili dai dati personali trasmessi, che si traducano in vantaggi competitivi per i concorrenti (dati lavorati e, grazie a questi, strategie di trattamento e di mercato)[20]. Gli altri vedono la propria posizione minacciata principalmente allorché i dati oggetto della richiesta dell'interessato comprendano informazioni che riguardano anche loro[21]. Tenendo conto di questo, l'art. 20 GDPR non solo indugia in alcune

[17] Come è noto, il diritto alla portabilità è, almeno nel campo della tutela dei dati personali, una novità introdotta dal GDPR: v. L. SCUDIERO, *Bringing Your Data Everywhere: A Legal Reading of The Right to Portability*, in *European Data Protection Law Review*, 2017, Vol. 3, 119. L'idea di fondo era però già nota: nel diritto europeo almeno dalla dir. 2002/22/CE (c.d. direttiva servizio universale), che ha introdotto la portabilità del numero telefonico (cfr. S. TROIANO, *op. cit.*, 196 ss.; ma v. anche l'obbligo alla portabilità transfrontaliera di servizi di contenuti online di cui al Reg. UE 2017/1128); nelle prassi di alcune delle principali imprese del settore digitale, ad iniziare dai primi progetti di Google, descritti sinteticamente da F. CATALANO, *Il diritto alla portabilità dei dati tra interessi individuali e prospettiva concorrenziale*, in *Europa dir. priv.*, 2019, III, 837 ss. Suggerito da numerosi atti preparatori, il diritto alla portabilità era già previsto, seppure embrionalmente, nell'art. 18 della Proposta di GDPR della Commissione, COM (2012) 11 *final*. Nella formulazione finale, dopo il fallimento del tentativo di accorparla al diritto all'accesso, la portabilità è affermata come diritto autonomo ma è d'altra parte connotata dalle limitazioni che si esamineranno *infra*, nel testo. Scompare infine il ruolo della Commissione di specificare norme tecniche in relazione al formato in cui l'interessato ha diritto di ricevere i dati e neppure vi è più riferimento ai formati che devono essere accettati dal titolare del trattamento ricevente.

[18] Ciò non solo sul piano dell'interoperabilità (v. *infra*), ma anche dei costi che può implicare soddisfare le richieste di portabilità (ragione per cui, ad esempio, è previsto che il diritto si applichi solo allorché i dati siano trattati con mezzi automatizzati), in modo sicuro: v. E. BATTELLI, G. D'IPPOLITO, *op. cit.*, 199.

[19] Ad es., l'art. 20, par. 3, GDPR prevede esplicitamente che l'interessato non perde il diritto alla cancellazione dei dati: da questa previsione si è ricavato che l'esercizio di un diritto è indipendente dall'altro e si è altresì escluso che la portabilità abbia ripercussioni sul piano del rapporto contrattuale tra interessato e titolare del trattamento (considerando 68 GDPR).

[20] Con riguardo a questa seconda tipologia di rischio, si spiega la limitazione della portabilità ai dati «forniti» dall'interessato, dati grezzi (raw data), escludendo le ulteriori informazioni ricavate (dati inferiti o inferenziali, e dati previsti). Ancora, la portabilità non può pregiudicare i segreti industriali e la proprietà intellettuale del titolare del trattamento, a cui spetta la possibilità di valutare di non dare seguito alla richiesta dell'interessato che rechi pregiudizio ai propri diritti, fermo che – come precisato dal considerando 63 GDPR, in relazione al diritto all'accesso, ma con un discorso senz'altro estensibile alla portabilità – «tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni».

[21] Poiché i dati personali sono spesso caratterizzati da una «intrinseca complessità e relazionalità», la portabilità può riguardare informazioni che concernono più soggetti contemporaneamente e non sempre è possibile o ragionevole, rispetto alla finalità dell'interessato, epurare tali dati da ciò che riguarda persone diverse dal richiedente. Per questa ragione, la disposizione secondo cui il diritto alla portabilità «non deve ledere i diritti e le libertà altrui» (art. 20, par. 4, GDPR), pur perentoria nel contenuto, deve essere debitamente interpretata, se non si vuole svuotare completamente di significato la disposizione normativa. Il punto è stato approfondito dal WP29, secondo cui la trasmissione di dati può riguardare anche informazioni di terzi (ad esempio, contatti, fotografie e messaggi) nella misura in cui questa serva all'interessato per realizzare una finalità di natura personale (in sostanza, rispetto a questi dati l'interessato ha una posizione assimilabile a quella di un titolare del trattamento, per il quale tuttavia le regole dello stesso Regolamento non vengono in rilievo alla luce dell'eccezione di cui all'art. 2, par. 2, lett. c, c.d. household exception) e tali dati non siano utilizzati per finalità ulteriori dal titolare del trattamento a cui essi vengano trasmessi, per il quale, invece, la base giuridica utile all'impiego di tali dati può essere rinvenuta nel legittimo interesse (art. 6, lett. f], GDPR) di prestare l'attività in favore dell'interessato (WP29, *Linee guida sul diritto alla portabilità*, cit., 11 s.).

precisazioni in relazione ad eventuali conflitti tra la portabilità e gli altri diritti dell'interessato o di altri soggetti (art. 20, par. 3 e 4, GDPR), ma circoscrive, a monte, l'ambito di applicazione di questo diritto[22]. In particolare, come già si è accennato, l'interessato può esercitare le prerogative della portabilità esclusivamente con riguardo ai dati da lui «forniti» al titolare del trattamento e che questo tratta sulla base del consenso o dell'esecuzione di un contratto (ovvero di misure precontrattuali), ricorrendo a mezzi automatizzati. La palpabile tensione tra le finalità sottese a questo innovativo strumento e il quadro dei principi di fondo del regolamento (e del diritto della concorrenza), si traduce in alcune rilevanti insicurezze nell'interpretare l'articolato normativo e le soluzioni adottate nel tentativo di bilanciare le diverse istanze[23].

Dal punto di vista dell'effettività del diritto alla portabilità, il principale limite[24] è quello, di natura tecnica, consistente nella mancanza di una garanzia di interoperabilità dei dati tra i titolari del trattamento[25], elemento che, confrontato con l'attuale realtà tecnologica, non solo relega la dimensione più avanzata del diritto ad una dimensione eventuale (come si è detto, la trasmissione diretta può essere richiesta solo «se tecnicamente fattibile»)[26],

[22] L'inapplicabilità del diritto alla portabilità non esclude poi la possibilità di esercitare il diritto all'accesso: E. Battelli, G. Ippolito, *op. cit.*, 193.

[23] Come è noto e come risulta pianamente dal suo primo articolo, il GDPR intende proteggere i diritti delle persone fisiche (ad iniziare da quello alla riservatezza), ad un tempo incoraggiando una più fluida circolazione dei dati personali, condizione fondamentale per la creazione e lo sviluppo del mercato digitale. Questa duplice dimensione (o «anima»: N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla privacy*, in Aa. Vv, *Persona e mercato dei dati*, cit., 36 ss.) implica un bilanciamento tra esigenze difficilmente conciliabili, al punto che la portabilità, esprimendole entrambe, è congenitamente affetta da un inevitabile 'strabismo': così, efficacemente, S. Troiano, *op cit.*, 207 ss. Emblematico è l'esempio dell'ampiezza della portabilità in base al significato del concetto di dati «forniti» dall'interessato: esclusi, come detto (*supra*, nota 20) i dati inferenziali (inferred data), rimane il problema se siano invece compresi i dati semplicemente 'osservati' grazie ad un dispositivo (ad es., lo smartwatch: observed data), o se vadano considerati oggetto della portabilità i soli dati attivamente forniti dall'interessato (volunteered data). L'interpretazione estensiva del WP29 (invero non accolta unanimemente, come osserva F. Catalano, *op. cit.*, 844; in termini dubitativi anche S. Troiano, *op. cit.*, 19 s.; in senso favorevole, si è però assestato l'orientamento dominante: E. Battelli, G. D'Ippolito, *op. cit.*, 195, che invero raccomandano sul punto una valutazione caso per caso; J. Krämer, *Personal data portability in the platform economy: economic implications and policy recommendations*, in *Journal of Competition Law & Technologies*, 2020, Vol. 17, 290, nelle conclusioni; A. Dix, *Sub art. 20*, in Aa. Vv., *General Data Protection Regulation. Article-by-Article Commentary*, a cura di I. Spiecker gen. Döhmann, V. Papakonstantinou, G. Hornung, P. De Hert, Baden-Baden-München-Oxford, 2023, 513) si giustifica certamente con l'intento di estendere la portata del diritto, ma un tale obiettivo non deve essere assolutizzato, se si tiene conto che ogni passo in quella direzione accentua una contraddizione col principio della minimizzazione dei dati (art. 5, par. 1, GDPR) e eleva lo standard di mercato ad un livello che rischia di escludere piccole e medie imprese dal mercato digitale, concentrandolo, ancora di più, nelle mani delle grandi piattaforme digitali: cfr. R.H. Weber, *Data Portability and Big Data Analitycs. New Competition Policy Challenges*, in *Concorrenza e Mercato*, 2016, 70; v. pure F. Bravo, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, I, 225 ss.

[24] Frequentemente sottolineata è, per il vero, la scarsa dimestichezza degli interessati rispetto ad uno strumento non ancora noto e diffuso, e le cui potenzialità non sono immediatamente percepibili dai singoli: v., anche sull'importanza di sviluppare strumenti *user-friendly*, S. Kuebler-Wachendorff *et al., The Right to Data Portability: conception, status quo, and future directions*, in *Informatik Spektrum*, Vol. 44, 2021, 266 ss.

[25] Come confermato dal considerando 68, il Regolamento non intende porre in capo ai titolari del trattamento un obbligo di adottare formati interoperabili (né, tantomeno, impone il risultato della perfetta compatibilità), limitandosi solamente a fissare criteri generali e di base (ossequiosi del principio di neutralità tecnologica: A. Dix, *op. cit.*, 514; v. considerando 15 GDPR) che, si auspica, consentano di rendere le informazioni trasmesse realmente utilizzabili dall'interessato e dal nuovo titolare del trattamento. Oltre a queste indicazioni di carattere generale, il GDPR non va oltre al semplice 'incoraggiamento' a che i titolari del trattamento sviluppino «formati interoperabili che consentano la portabilità dei dati».

[26] Seppure si rinvenga l'opinione, segnalata da F. Catalano, *op. cit.*, 862, che la norma avrebbe l'effetto di addossare al titolare del trattamento l'onere della prova della non fattibilità tecnica.

ma getta altresì una pesante ombra sulla realizzazione degli obiettivi sottesi alla 'versione di base' del diritto (riutilizzare i dati già forniti ad un primo titolare trasmettendoli ad un secondo titolare), giacché, se il titolare del trattamento è obbligato a trasmettere all'interessato i dati che lo riguardano «in un formato strutturato, di uso comune e leggibile da dispositivo automatico»[27], l'ulteriore titolare del trattamento che riceve tali dati non è obbligato ad adottare misure tecniche che ne consentano l'immediata fruizione[28].

4. La progressiva affermazione della portabilità come propellente della circolazione dei dati: il Regolamento europeo relativo ai dati non personali (c.d. Regolamento Free-flow), la Legge europea sulla governance dei dati (Data Governance Act) e la Legge europea sui mercati digitali (Digital Markets Act).

Rispetto al quadro di partenza, sopra descritto per sommi capi, i successivi interventi del legislatore europeo si sono mossi, su più fronti, nella direzione del consolidamento[29] e di un deciso potenziamento della portabilità dei dati[30].

---

[27] Sullo spostamento del focus normativo dall'interoperabilità dei servizi a quello dei formati dei dati trasmessi, v. E. BATTELLI, G. D'IPPOLITO, *op. cit.*, 202 ss., che ne sottolineano i punti di forza, oltre che la evidente finalizzazione alla circolazione dei dati. Simmetriche preoccupazioni si sono affacciate nel dibattito: cfr. S. TROIANO, *op. cit.*, 209 ss., che porta alla luce come la predeterminazione dei formati e la facilitazione della circolazione dei dati attraverso la rimozione delle barriere tecniche aumentino le occasioni di violazione da parte di terzi e agevolino altresì comportamenti poco prudenti degli stessi interessati.

[28] L'interoperabilità è un pilastro tecnico senza il quale l'effettività del diritto non può essere garantita: v. F. CATALANO, *op. cit.*, 847 ss.; D. COPETTI CRAVO, *op. cit.*, 56 s. e, per una sintesi di alcune soluzioni tecniche, v. JOHANN KRANZ *et al.*, *Data portability*, in *Business & Information Systems Engineering*, Vol. 65, 2023, 601 ss. Per una recente analisi empirica sulla distanza tra l'auspicio del legislatore europeo e la realtà del mercato, v. S. KUEBLER-WACHENDORFF *et al., op. cit.*, 268 s., i quali, anche sulla base di questa ragione, discorrono di una «blunt sword».

[29] Il concetto di portabilità ha fatto il suo ingresso anche nella disciplina consumeristica. Nella dir. 770/2019/UE sui contratti di fornitura di contenuti e servizi digitali, in particolare, si prevede il diritto dei consumatori, che recedono dal contratto, alla portabilità, non solo dei dati personali (che, nel testo finale della direttiva, si risolve nel richiamo generale al GDPR, all'art. 16, par. 2, attuato dall'art. 135-*noviesdecies*, co. 3, cod. cons.: v. A. METZGER, Z. EFRONI, L. MISCHAU, J. METZGER, *Data-Related Aspects of the Digital Content Directive*, in *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, 2018, Vol. 9, 102 s.; K. SEIN, G. SPLINDER, *The New Directive on Contracts for the Supply of Digital Content and Digital Services – Conformity Criteria, Remedies and Modifications – Part 2*, in *European Review of Contract Law*, 2019, Vol. 15, 381 ss.) ma anche dei 'contenuti digitali', ossia dati diversi da quelli personali generati dal consumatore nell'utilizzo del contenuto o del servizio digitale oggetto del contratto risolto (art. 16, parr. 4, dir., attuato dall'art. 135-*noviesdecies*, co. 5, c. cons.). Disposizioni simili sono contenute nella disciplina del recesso nei contratti a distanza e conclusi al di fuori dei locali commerciali, in base alla dir. 2011/83/UE, come emendata dalla dir. 2019/2161/UE, c.d. *omnibus* (art. 13, parr. 4 e 6, attuati dall'art. 56, co. 3-*bis* e 3-*quater*, c. cons.). Come è stato puntualmente osservato, però, da G. COLANGELO, M. MAGGIOLINO, *op. cit.*, 177, il diritto contemplato dalle direttive, almeno con riguardo ai dati non personali, non si estende sino a comprendere la portabilità diretta.

[30] Conformemente al chiaro indirizzo espresso nella Comunicazione della Commissione del 19 febbraio 2020, COM(2020) 66 final, *Una strategia europea per i dati*, 22. Il deciso cambio di passo dell'Unione, teso a favorire la circolazione, condivisione e riuso dei dati è sottolineato, tra gli altri, da D. POLETTI, *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio delle fonti*, 2023, 368 ss., consultabile al sito https://www.osservatoriosullefonti.it (ultimo accesso: 18 luglio 2024); A. METZGER, H. SCHWEITZER, *Shaping Markets, A Critical Evaluation of the Draft Data Act*, in *Zeitschrift für Europäisches Privatrecht*, 2023, I, 43 ss. In questo si sostanzia il progressivo e inesorabile 'scivolamento' della prospettiva europea da una logica unipolare e difensiva (ancora prevalente, seppure con l'emersione ben più decisa dell'incentivo della circolazione, nel GDPR) ad una tesa a considerare i dati come risorsa economica e di sviluppo sociale, riutilizzabile a costo zero: cf. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, IV, 973 ss.

Finendo per trascendere i confini di una situazione giuridica soggettiva, la portabilità è divenuta la pietra d'angolo su cui si reggono molti dei pilastri dell'economia europea dei dati: per un verso, questo concetto è scelto dal Reg. UE 2018/1807 (relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, c.d. Regolamento Free-flow) come cifra distintiva della circolazione del dati non personali[31]; per altro verso, lo stesso è alla base dell'attività di condivisione delle informazioni, personali e non, (c.d. data sharing), incentivata quale condizione imprescindibile per la costruzione di un mercato dei dati equo e contendibile[32]. Non sorprende dunque che il Reg. UE 2022/868, c.d. Data Governance Act (DA)[33], nel disciplinare l'attività degli intermediari dei dati (in particolare, agli artt. 10-15)[34], presti attenzione a quello che, nei fatti, si è rivelato essere il principale limite all'effettività del diritto alla portabilità dei dati personali, vale a dire l'interoperabilità degli stessi: così, si prevede che gli intermediari debbano «agevola[re] lo scambio dei dati nel formato in cui li ricev[ono] da un interessato o da un titolare dei dati» per «convertir[li] in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale, se richiesto dall'utente dei dati, se prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati», salva la necessità di «offr[ire] agli interessati o ai titolari dei dati la possibilità di non partecipare a tali conversioni, a meno che la conversione non sia prescritta dal diritto dell'Unione» (art. 12, lett. d, DGA)[35].

L'effettività del diritto alla portabilità dei dati, personali e non, è al cuore anche del Reg. UE 2022/1925, relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali o Digital Markets Act, d'ora in avanti abbreviato con l'acronimo DMA)[36]. Questa disciplina, che ha lo scopo di rivitalizzare la concorrenza nel mercato dei «servizi di piattaforma di base»[37] e, per l'effetto, limitare il potere delle grandi piattaforme digitali anche negli altri settori[38], impone una serie di stringenti obblighi in capo ad alcuni soggetti del mercato che, alla luce di indicatori quantitativi e qualitativi previsti dallo stesso

[31] V., in particolare, art. 6 e considerando 29 dello stesso Regolamento.
[32] V. considerando 2 DGA.
[33] L. VON DITFURTH, G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, in *Journal of Competition and Regulation in Network Industries*, 2022, Vol. 23, 274; A. OWUSU, *Data sharing in the personal data economy. Does sharing mean caring?*, in *EJPLT*, 2023, II, 6 ss. V. anche F. BRAVO, *Intermediazione di dati*, cit., 251 s.
[34] La centralità di questi nuovi attori del mercato è riconosciuta dallo stesso DGA (cfr. considerando 27). Come già osservato *supra*, alla nota 11, l'attività di alcuni di questi soggetti (specialmente le PIMSs, ma anche le Cooperative di dati) ha il merito di rafforzare la posizione di controllo dell'interessato sui propri dati: v. D. POLETTI, *op. cit.*, 370 ss.
Il Regolamento disciplina altresì la condivisione volontaria e gratuita di dati per obiettivi di interesse generale (c.d. data altruism): Artt. 15 e 16-25 DGA.
[35] Lo osserva F. BRAVO, *Le cooperative dei dati*, in *Contratto e impresa*, 2023, III, 777 s.; v. già ID., *Intermediazione di dati*, cit., 251 s.
[36] Per una panoramica generale, v. S. FORASASSI, *Il nuovo Regolamento europeo sui mercati digitali (Digital Markets Act). Inquadramento generale e criticità*, in *Contratto e Impresa Europa*, 2023, I, 145 – 176.
[37] Definiti in un elenco contenuto dall'art. 2, n. 2, DMA, che comprende il servizio di intermediazione online, motori di ricerca, social network, condivisione di video, servizi di comunicazione interpersonali indipendenti dal numero, sistemi operativi, browser web, assistenti virtuali, servizi di cloud computing, servizi pubblicitari online.
[38] Come osservano S. KUEBLER-WACHENDORFF *et al., op. cit.*, 265 s., «As a consequence, these platforms grow ever more powerful in their primary markets and leverage their data silos, market power and installed user base to enter other markets».

Regolamento, sono qualificati (e designati dalla Commissione) come gatekeepers[39]. In questa cornice, visto il rilievo della disponibilità dei dati nell'espansione trasversale di queste grandi realtà, la portabilità rappresenta uno strumento che le altre imprese possono stimolare (trattandosi di un diritto dell'interessato) per ottenere l'accesso ad una grande quantità di informazioni, rendendosi così competitive sul mercato digitale. In questo si spiega, rispetto all'art. 20 GDPR[40], la notevole estensione del campo di applicazione del diritto[41] e, in generale, il considerevole rafforzamento dello stesso allorché sia esercitato nei confronti dei gatekeepers, sotto la forma di un obbligo loro imposto (art. 6, par. 9, DMA)[42].

Nel più recente testo normativo, scompare ogni limitazione concernente la base giuridica del trattamento; oggetto del diritto, inoltre, non sono solo i dati «forniti», ma anche quelli «generati mediante l'attività dell'utente finale nel contesto dell'utilizzo del pertinente servizio di piattaforma di base».

L'effettività della portabilità è qui parte integrante dell'obbligo imposto ai gatekeepers (al punto che la norma discorre di «effettiva portabilità» e, poco dopo, di «effettivo esercizio di tale portabilità»), traducendosi nella previsione non più solo di standard minimi per favorire l'interoperabilità, ma anche della garanzia di questo risultato («fornendo a titolo gratuito strumenti per agevolar[lo]»)[43]. È altresì prevista la possibilità che la Commissione, per concretizzare quest'obbligo, adotti atti di esecuzione (art. 46, par. 1, lett. b, DMA) oppure si avvalga, allo stesso scopo, delle organizzazioni europee di normazione (art. 48 DMA). L'interoperabilità deve essere assicurata – come precisa il considerando 59 – con «misure tecniche adeguate e di elevata qualità». Andando ancora oltre, e mutuando un risultato già raggiunto settorialmente nel diritto dell'Unione, si prevede segnatamente una portabilità immediata e continua, ossia con accesso «continuo e in tempo reale»[44].

Tali caratteri, implicando la superfluità di una ripetuta richiesta da parte dell'interessato in relazione a specifici set di dati, rappresentano un'evoluzione

[39] Il procedimento di designazione dei gatekeeper è stabilito all'art. 3 DMA. Come riportato dal Comunicato stampa del 6 settembre 2023, i primi sei gatekeeper designati dalla Commissione sono Alphabet, Amazon, Apple, ByteDance, Meta e Microsoft (https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328).

[40] Fermo che, come normalmente accade nella normativa europea in materia di dati, si ritrova anche nel DMA l'affermazione che il regolamento lascia 'impregiudicate' le norme del GDPR (considerando 12), è significativa la precisazione secondo cui «l'obbligo per il gatekeeper di garantire l'effettiva portabilità dei dati a norma del presente regolamento integra il diritto alla portabilità dei dati a norma del regolamento (UE) 2016/679».

[41] J. KRANZ *et al.*, *op. cit.*, 598.

[42] L'art. 5 DMA proibisce la combinazione di dati personali provenienti dal servizio di piattaforma di base offerto «con dati personali provenienti da altri servizi di piattaforma di base o da eventuali ulteriori servizi forniti dal gatekeeper o con dati personali provenienti da servizi di terzi» (par. 2, lett. b) e l'uso incrociato di tali dati «in altri servizi forniti separatamente dal gatekeeper, compresi altri servizi di piattaforma di base, e viceversa» (par. 2, lett. c).

[43] In base al considerando 59 DMA, infatti, «[i] dati dovrebbero essere ricevuti in un formato immediatamente ed effettivamente accessibile e utilizzabile da parte dell'utente finale o dei pertinenti terzi autorizzati dall'utente finale a cui i dati sono trasferiti».

[44] Sono citate direttamente, come esempio di misure tecniche, le interfacce di programmazione delle applicazioni (API), già segnalate dal WP29 (*Linee guida*, cit., 15), a commento dell'art. 20 GDPR, come strumento per facilitare il trasferimento dei dati nell'ambito dei servizi offerti dalla società dell'informazione. Secondo la definizione dello stesso organismo (ivi, nota 27), si tratta di «interfacce di applicazioni o servizi web che i titolari rendono disponibili per consentire ad altri sistemi o applicazioni di connettersi e operare con i propri sistemi»; v. pure D. COPETTI CRAVO, *op. cit.*, 56 s.; sulle possibili costellazioni tecniche che possono consentire ad una effettiva portabilità, v. J. KRANZ *et al.*, *op. cit.*, 606 s.

già auspicata dalla dottrina in sede di interpretazione dell'art. 20 GDPR[45]. I rilievi relativi ai benefici di una c.d. continuous portability in termini di rafforzamento della posizione del consumatore e di conseguente stimolo per la concorrenza e lo sviluppo tecnologico si ritrovano citati anche nel considerando 59 DMA: in particolare, questa modalità di esercizio asseconda la tendenza degli utenti finali al c.d. multihoming, situazione che perdura per un tempo anche considerevole, in cui, anziché mutare il fornitore di servizi *online*, gli stessi preferiscono mantenere attivi entrambi i servizi.

È peraltro significativo che il Regolamento abbia tenuto conto di uno dei principali rischi di un requisito qualitativo così elevato della portabilità, ossia quello di un costo eccessivamente alto per le piccole e medie imprese: secondo un approccio basato sulla proporzionalità, l'obbligo è infatti posto solamente a carico dei colossi digitali, appunto i gatekeepers[46].

Titolari del diritto alla portabilità previsto dal DMA sono gli «utenti finali», ossia coloro che utilizzano il servizio di piattaforma per scopi diversi (commerciali o non) da quelli di fornire beni o servizi (art. 1, n. 20, DMA). Invero, anche agli utenti commerciali, ossia a coloro che fanno ricorso alla piattaforma («nell'ambito delle proprie attività commerciali o professionali»: art. 1, n. 21, DMA) è riconosciuto un diritto di «accesso efficace, di elevata qualità, continuo e in tempo reale a dati aggregati e non aggregati, compresi i dati personali» e il gatekeeper deve garantire l'uso di tali dati (art. 6, par. 10, DMA)[47]. Questo diritto si riferisce anche ai dati degli utenti finali (quindi di un soggetto diverso da quello che esercita la prerogativa), a condizione che si tratti di dati connessi con l'uso che questi abbiano fatto dei prodotti e dei servizi offerti dall'utente commerciale tramite il servizio di piattaforma gestito dal gatekeeper oppure che lo stesso utente finale ne abbia accettato la condivisione esprimendo un consenso.

5. L'ulteriore evoluzione della portabilità nell'architettura dei più recenti interventi normativi dell'UE: la compiuta rottura degli argini soggettivi del diritto dell'interessato nella Legge europea sui dati (Data Act).

[45] J. KRÄMER, *op. cit.*, 296: «In summary, we therefore argue in favour of a new proportionate rule that gives consumers the right to transfer their personal data (as under Article 20 GDPR) continuously and in real time from their existing digital service provider to another provider».

[46] Nell'ampliare l'ambito di applicazione oggettivo del diritto, il legislatore europeo supera, almeno in buona parte, un ulteriore rischio, lucidamente messo in rilievo dalla dottrina (v. J. KRÄMER, *op. cit.*, 296 s.), ossia amplificare le incertezze giuridiche che riguardano questo aspetto nella versione 'base' della portabilità: è infatti evidente che la versione 'rafforzata' dal DMA si muove decisamente nella direzione di privilegiare le istanze del mercato. Rimane però aperto il tema del pericolo di incentivare prassi di migrazione dei dati, magari dietro promessa di incentivi economici, verso ambienti meno sicuri, rischio che si è proposto di mitigare facendo ricorso alle cautele adottate dalla legislazione europea nel settore bancario, dove pure è presente una portabilità *real-time* e continua (che, in questo senso, integra il GDPR): v. ancora J. KRÄMER, *op.* cit., 297. Il riferimento è alla direttiva UE 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD2, in particolare agli artt. 66, par. 4, e 67, par. 3): v. J. KRÄMER, P. SENELLART, A. DE STREEL, *op. cit.*, 31 s.

[47] Come precisa lo stesso art. 6, par. 10, DMA si tratta dei «dati che sono forniti o generati nel contesto dell'uso dei pertinenti servizi di piattaforma di base o dei servizi forniti contestualmente o in ausilio ai pertinenti servizi di piattaforma di base». V. pure il considerando 60 DMA. Un ulteriore obbligo di condivisione riguarda taluni dati generati dagli utenti finali sui motori di ricerca online del gatekeeper ("dati relativi a posizionamento, ricerca, click e visualizzazione"): questi deve garantirne ai prestatori di servizi di motori di ricerca che ne facciano richiesta, l'accesso "a condizioni eque, ragionevoli e non discriminatorie" (Art. 6, par. 11, DA).

L'apertura, a soggetti diversi dall'interessato, dell'accesso e della condivisone dei dati dischiude un'ulteriore traiettoria evolutiva del diritto alla portabilità, che ne proietta l'ambito di applicazione soggettivo in una dimensione più ampia rispetto alla sfera dell'interessato. Allo stato, la più significativa espressione di questa dimensione è oggi contenuta nel Reg. UE 2023/2854, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (regolamento sui dati o Data Act, d'ora in avanti DA)[48].

Lo scopo dello strumento, rispetto alla cui compatibilità con il GDPR il legislatore europeo è molto attento, non è tutelare i diritti dell'interessato, ma incentivare la circolazione dei dati, personali e non, generati dai prodotti connessi e dai servizi ad essi correlati[49].

Dalla prospettiva che qui interessa, la figura centrale è quella dell'utente del prodotto connesso o del servizio correlato [50] : a questo soggetto, il Regolamento garantisce il diritto di accesso e di condivisione con terzi, per scopi commerciali e non, di una serie molto ampia di dati detenuti da un «titolare dei dati» (data holder) [51] , purché nella "pronta disponibilità" di quest'ultimo[52]. Sono compresi i dati osservati, non solo nella forma "grezza", ma anche in quella definita dal Regolamento "pretrattata", oltre ai cc.dd.

[48] Cfr. D. POLETTI, *op. cit.*, 373 ss., che osserva come la normativa abbia lo scopo di incentivare la circolazione dei dati dal titolare dei dati al destinatario (entrambi soggetti imprenditoriali), mentre il ruolo dell'interessato è per così dire relegato ad «agente legittimante», al quale rimane però il potere di scegliere dove veicolare i dati che lo riguardano.

[49] Come specificato nel considerando 32, l'obiettivo del Data Act «non è solo promuovere lo sviluppo di prodotti connessi o di servizi correlati nuovi e innovativi e stimolare l'innovazione nei servizi post-vendita, ma anche stimolare lo sviluppo di servizi completamente nuovi che utilizzano i dati in questione, anche sulla base di dati provenienti da una varietà di prodotti connessi o servizi correlati».

[50] La definizione di prodotto connesso richiama l'idea di "Internet of Things" (IoT): «un bene che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati del prodotto tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo, e la cui funzione primaria non è l'archiviazione, il trattamento o la trasmissione dei dati per conto di una parte diversa dall'utente» (art. 2, n. 5, DA). Il servizio correlato è il servizio digitale, presente sin dall'origine o successivamente installato, grazie al quale il prodotto svolge tutte o anche solo una delle sue funzioni (cfr. art. 2, n. 6, DA). Sono compresi gli assistenti virtuali, anche se forniti da soggetti diversi (considerando 23), che interagiscono con un prodotto connesso o un servizio correlato (art. 1, par. 4, DA). La definizione di utente del prodotto o del servizio è molto ampia (art. 2, n. 12, DMA: «una persona fisica o giuridica che possiede un prodotto connesso o a cui sono stati trasferiti contrattualmente diritti temporanei di utilizzo di tale prodotto connesso o che riceve un servizio correlato»), con la conseguenza che più soggetti possono rivestire contemporaneamente questa qualifica (considerando 18).

[51] Il data holder (impresa) e il data recipient, destinatario dei dati (impresa), sembrano essere i veri protagonisti di questa normativa, mentre i diritti degli utenti si traducono in previsioni inderogabili nelle relazioni contrattuali (B2B) tra i primi: A. METZGER, H. SCHWEITZER, *op. cit.*, 44. Il data holder è definito come «una persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale adottata conformemente al diritto dell'Unione, di utilizzare e mettere a disposizione dati, compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato» (art. 2, n. 13, DA). Si tratta, in sostanza, di un proprietario 'di fatto' dei dati (v. ancora A. METZGER, H. SCHWEITZER, *op. cit.*, 54), ossia di un soggetto che ha un controllo materiale sugli stessi. V., a proposito degli scenari aperti dal Data Act sui diritti sui dati non personali generati dall'IoT, M. ECKARDT, W. KERBER, *Property rights theory, bundles of rights on IoT data, and the EU Data Act*, in *European Journal of Law and Economics*, 2024, vol. *Data Economy.* Consultabile al sito: https://link.springer.com/article/10.1007/s10657-023-09791-8.

[52] L'art. 2, n. 17, DA definisce 'prontamente disponibili': i «dati del prodotto e dati di un servizio correlato che un titolare dei dati ottiene o può ottenere legittimamente dal prodotto connesso o dal servizio correlato senza che ciò implichi uno sforzo sproporzionato che vada al di là di una semplice operazione».

metadati[53]; rimangono ancora esclusi dal campo di applicazione della disciplina quelli inferenziali[54].

Gli standard qualitativi imposti per l'accesso, la «messa a disposizione» dei dati (art. 4 DA) e la condivisione con terzi[55] degli stessi su richiesta dell'utente (art. 5 DA) sono molto elevati, nel senso di garantire l'effettività e l'interoperabilità: «senza indebito ritardo, con la stessa qualità di cui dispone il titolare dei dati, in modo facile, sicuro, a titolo gratuito per l'utente[56], in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico». Se «pertinente e tecnicamente possibile», il flusso di dati è «continuo e in tempo reale».

Superando una evidente limitazione della versione di base della portabilità, l'attenzione a questo risultato si traduce altresì in norme destinate ai fabbricanti dei prodotti connessi e ai fornitori dei servizi correlati (affinché prodotti e servizi siano realizzati di modo che, di default, i dati concernenti il loro utilizzo siano agevolmente accessibili in formati fruibili), e, in aggiunta, a coloro che vendano o concedano in godimento tali prodotti (che sono gravati da precisi obblighi informativi da soddisfare prima della conclusione del contratto)[57].

Dalla prospettiva dei dati personali[58], le definizioni soggettive del Data Act devono collegarsi con quelle, imprescindibili, del GDPR. Se l'utente del prodotto è anche l'interessato (data subject) è evidente che gli artt. 4 e 5 DA si sovrappongono al diritto alla portabilità di cui all'art. 20 GDPR, amplificandolo

---

[53] Il 'pretrattamento' consiste nel procedimento attraverso il quale i dati grezzi (raw data) raccolti dai prodotti connessi o dai servizi ad essi correlati vengono resi comprensibili ed utilizzabili per successive attività di trattamento (cfr. considerando 15 DA); i «metadati» sono invece definiti dall'art. 2, n. 2, DA come «una descrizione strutturata del contenuto o dell'uso dei dati che agevola la ricerca o l'utilizzo di tali dati».

[54] Dalla lettura del considerando 15 DA, emerge la moltitudine di dati oggetto dei diritti degli utenti dei prodotti connessi e dei servizi correlati, intesi in senso ampio come «digitalizzazione delle azioni o degli eventi degli utenti». Alla luce degli obiettivi del Regolamento, non rientrano invece i dati relativi ai software e ai contenuti non correlati, ossia «i dati generati da tali prodotti connessi dotati di sensori quando l'utente registra, trasmette, visualizza o riproduce contenuti, nonché i contenuti stessi, spesso soggetti a diritti di proprietà intellettuale, anche per l'uso da parte di un servizio online» (considerando 16 DA, che altresì precisa che il Data Act «non dovrebbe inoltre applicarsi ai dati ottenuti, generati o consultati dal prodotto connesso, o ad esso trasmessi, a fini di archiviazione o altre operazioni di trattamento per conto di altre parti diverse dall'utente, come nel caso di server o infrastrutture cloud gestiti dai rispettivi proprietari interamente per conto di terzi, anche per uso da parte di un servizio online»).

[55] Sui quali gravano gli obblighi previsti dall'art. 6 DA, tra i quali spicca il principio di minimizzazione, esteso anche ai dati non personali (ma, solo in questo caso, derogabile).

[56] Il compenso può essere chiesto non già all'utente, ma al destinatario dei dati, alla luce di un accordo che, ai sensi degli artt. 8 ss. DA, quest'ultimo deve stipulare con il titolare dei dati. È significativa la precisazione dell'art. 5, par. 8, DA, secondo la quale «[l]a mancanza di accordo, da parte del titolare dei dati e del terzo, sulle modalità per la trasmissione dei dati non ostacola, impedisce o interferisce con l'esercizio dei diritti dell'interessato a norma del regolamento (UE) 2016/679 e, in particolare, con il diritto alla portabilità dei dati di cui all'articolo 20 di tale regolamento».

[57] Art. 3 e considerando 20-24. L'art. 7 e il considerando 41 DA fanno eccezioni per le microimprese e le piccole imprese (e dettano talune regole di favore anche per le medie imprese), alla luce di una valutazione di opportunità di mercato. Sempre valutazioni di questo tipo (ma di segno contrario) sono alla base dell'esclusione dei *gatekeeper* dalla possibilità di «chiedere o ottenere l'accesso ai dati degli utenti generati dall'uso di un prodotto connesso o di un servizio correlato o da un assistente virtuale ai sensi del presente regolamento. Inoltre, i terzi cui i dati sono messi a disposizione su richiesta dell'utente «non possono mettere i dati a disposizione di un gatekeeper»: così il considerando 40 DA, che si traduce nelle stringenti previsioni degli artt. 5, par. 3, e 6, par. 2, lett. d), DA.

Si noti, infine, che al tema dell'interoperabilità è dedicato un un capo specifico del Regolamento (VIII).

[58] Lo stesso vale «anche qualora i dati personali e non personali all'interno di un insieme di dati siano indissolubilmente legati»: considerando 34 DA.

e superandone molte delle limitazioni sopra esaminate, in linea con l'evoluzione normativa che si è tratteggiata[59]. L'inclusione dei dati 'osservati', in particolare, supera in modo definitivo il dilemma interpretativo con riguardo alla nozione di dati "forniti", almeno con riguardo a quelli collegati all'Internet of Things. Se invece le informazioni personali di cui l'utente del prodotto domanda l'accesso e la condivisione si riferiscono ad altre persone fisiche, il diritto riconosciuto dal Data Act getta luce su una diversa manifestazione della portabilità, che, per non urtare contro i principi del GDPR, deve essere considerata un trattamento: ne discende che l'utente del prodotto è un titolare del trattamento, come pure, prima di lui e poi assieme a lui, il titolare dei dati (al quale è infatti domandato di compiere una certa attività con riguardo a quei dati). L'equilibrio raggiunto tra le due normative è dunque a favore del GDPR: rispetto a nessuna delle attività previste dal *Data Act* (messa a disposizione o condivisione dei dati) e per entrambi i soggetti, tale disciplina fornisce una base giuridica che legittima il trattamento, la quale continuerà pertanto ad essere necessaria ai sensi dell'art. 6 GDPR[60].

Pur con tutte queste cautele, rimane sicuramente impressa all'interprete questa ulteriore configurazione della portabilità, la quale sottende qui non solo un diritto dell'interessato, ma integra altresì una prerogativa del titolare del trattamento[61], seppure alla condizione dell'esistenza di una base giuridica a sostegno di tale operazione[62].

6. La duplice veste della portabilità nella Proposta di regolamento sullo spazio europeo dei dati sanitari (European Health Data Space Act).

Un'ultima evoluzione del diritto (e del concetto di) portabilità si rinviene nella Proposta di regolamento relativo ad uno spazio europeo dei dati sanitari[63]. Come preannunciato nelle linee programmatiche della Commissione

[59] Questo diritto di portabilità rafforzato non sostituisce, ma si affianca a quello generale: v. *supra* nota 56 e considerando 35.

[60] Come ribadito più volte nel testo normativo, il legislatore non ha inteso conferire ai data holder un nuovo diritto di utilizzare i dati: v. considerando 5, 7 e 25 DA, il quale ultimo precisa che il Regolamento «non costituisce [per questi ultimi] una base giuridica per consentire l'accesso ai dati personali o per mettere i dati personali a disposizione di terzi». Anche gli utenti del prodotto connesso o del servizio correlato devono avere una base giuridica, allorché non siano i data subject e nella misura in cui si applichi il GDPR (non dunque nel caso di un uso domestico condiviso di un prodotto connesso), in quanto titolari del trattamento: così gli artt. 4, par. 12, e 5, par. 7, e il considerando 34 DA, il quale ultimo prende altresì in considerazione l'ipotesi in cui titolare dei dati e utente del prodotto siano entrambi, nella prospettiva del Regolamento sulla protezione dei dati personali, contitolari del trattamento e precisa che, una volta che l'utente abbia a disposizione i dati per averli ricevuti dal titolare dei dati, può divenire a sua volta, a norma del Data Act, un titolare dei dati. Il legislatore europeo ha dunque seguito un Trennungsprinzip rispetto alla disciplina delle informazioni personali, la quale continua a regolare in via esclusiva le basi giuridiche che legittimano qualsiasi attività di trattamento: M. SCHMIDT-KESSEL, *Einordnung des Data Act in das Mehrebenensystem des Unionsprivatrechts*, in *MMR. Zeitschrift für IT-Recht und Recht der Digitalisierung*, 2024, I, 127; v. pure A. METZGER, H. SCHWEITZER, *op. cit.*, 76 ss.

[61] Così perlomeno rievocando la costruzione di un "diritto" al trattamento, da intendersi come insieme di prerogative del titolare: v. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano-Padova, 2018, *passim*.

[62] In termini generali, l'art. 5, par. 13, DA specifica che «Il diritto di cui al paragrafo 1 non deve ledere i diritti degli interessati a norma del diritto dell'Unione e nazionale applicabile in materia di protezione dei dati personali».

[63] COM (2022) 197 final, 3 maggio 2022. Per prime osservazioni, cfr. I. RAPISARDA, *Sul costituendo spazio europeo dei dati sanitari*, in *Resp. medica*, 2023, IV, 413 – 425. Sul testo sono intervenuti gli emendamenti del

emanate all'avvio del decennio in corso[64], ad una normativa orizzontale in materia di dati (il cui perno, con riguardo ai dati personali, continua a trovarsi nel GDPR), sono destinate ad affiancarsi alcune discipline settoriali, che mirano a rafforzare il quadro giuridico e ad incentivare la circolazione delle informazioni rilevanti nell'ambito di settori strategici. Il testo normativo interviene con riguardo sia al c.d. uso primario dei dati sanitari elettronici[65], ossia per finalità concernenti la cura delle persone – intesa in termini piuttosto ampi (art. 2, lett. d, Accordo provvisorio) – sia al c.d. uso secondario degli stessi dati, vale a dire per scopi diversi da quelli iniziali (ad esempio attinenti alla finalità di cura tipica dell'uso primario), alla luce dei quali sono stati raccolti o generati (art. 2, par. 2, lett. e, Accordo provvisorio). Le finalità legittime dell'uso secondario sono elencate nell'art. 34 Accordo provvisorio (ad esempio, la ricerca scientifica).

Nel contesto dell'uso primario, la proposta mira a «specificare» e «integrare»[66] i diritti dell'interessato sui propri dati, con prevalente riguardo al diritto all'accesso e al diritto alla portabilità[67], specialmente con riferimento alle informazioni che rientrano nelle categorie prioritarie definite dal Regolamento[68]. Sciogliendo un nodo interpretativo che la Proposta rischiava di lasciare insoluto, l'Accordo precisa che i diritti di nuova generazione non si

---

Parlamento europeo del 13 dicembre 2023. Infine, è stato raggiunto da Parlamento e Consiglio un accordo provvisorio (14 marzo 2024), che dovrebbe preludere alla definitiva approvazione del testo normativo, a seguito degli opportuni adattamenti linguistici e giuridici. I riferimenti qui di seguito adottano la numerazione provvisoria dell'accordo, disponibili al seguente link https://www.consilium.europa.eu/media/70909/st07553-en24.pdf (ultimo accesso: 18 luglio 2024).

[64] COM (2020) 66 *final*, *Una strategia europea per i dati*, cit., 24 ss.

[65] I dati sanitari elettronici sono tutti quelli, personali e non personali, trattati in formato elettronico, «relativi alla salute e i dati genetici» (art. 2, par. 2, lett. a e b). La difficoltà di discernere quali informazioni della persona vi rientrino concretamente, segnalata dal soppresso riferimento ai fattori determinanti lo stato di salute (sul quale v. W. Li, P. Quinn, *The European Health Data Space: An expanded right to data portability*, in *Computer Law & Security Review*, 2024, Vol. 52, 8), è solo in parte riassorbita dall'attuale richiamo al GDPR. In ogni caso, la mole dei dati è estremamente ampia, se si considera che nella categoria possono essere annoverati anche le informazioni raccolte da applicazioni scaricate su dispositivi mobili o indossabili. Altra problematica, segnalata già dal Parere congiunto del Comitato europeo per la protezione dei dati personali e del Garante europeo per la protezione dei dati personali sulla proposta, (EDPB-EDPS, *Opinion 3/2022*, adottato il 12 luglio 2022, 14), è quella, pratica, di distinguere i dati personali da quelli non personali (ed è anche noto che l'anonimizzazione non escluda il rischio di reidentificazione, attraverso procedimenti logici e di data mining: v. pure considerando 49 e 64 della Proposta). Su raccomandazione di queste stesse Istituzioni, la definizione di dati non personali precisava, nel testo emendato dal Parlamento europeo, che «laddove i dati personali e non personali laddove i dati personali e non personali una serie di dati siano indissolubilmente legati, l'intera serie di dati e trattata come dati sanitari elettronici personali» (art, 2, par. 2, lett. b). Tale precisazione è però scomparsa nel testo dell'Accordo provvisorio.

[66] Art. 1, par. 2, lett. a), Accordo provvisorio. Nella formulazione originaria della proposta della Commissione, si accentuava l'idea che tali diritti fossero "rafforzati".

[67] Mentre la proposta della Commissione faceva riferimento al solo diritto di accesso (pur già imbastendo un confronto con l'Art. 20 GDPR nei Considerando), il testo risultante dall'Accordo provvisorio definisce espressamente come "diritto a alla portabilità" (Art. 8e), l'insieme delle facoltà degli individui descritte nell'originario l'art. 3, par. 8, della Proposta. Invero, tale qualificazione, tanto più che il diritto è parso sin da subito modellato sulla base della forma più avanzata della portabilità nota al GDPR (quella "diretta", di cui all'Art. 20, par. 2), appariva già fuori di dubbio: v. W. Li, P. Quinn, *op. cit.*, 6. Vi è peraltro da osservare che, in questo testo di nuova foggia, la differenza tra il diritto di accesso (Art. 8a) e diritto alla portabilità nella versione base dell'Art. 20, par. 1, GDPR tende a farsi evanescente. La persona fisica che esercita questo diritto, infatti, riceve i dati in formato elettronico, immediatamente, gratuitamente e in formato agevolmente leggibile, consolidato ed accessibile. A cavallo tra tali diritti, si aggiunge ora (dopo il passaggio al Parlamento europeo) il diritto di scaricare i dati sanitari elettronici nella propria cartella clinica elettronica.

[68] Art. 5 Accordo. Si tratta di dati essenziali a ricostruire lo stato di salute della persona fisica, in larga parte già digitalizzati nell'UE (ad esempio i profili sanitari sintetici dei pazienti, i risultati di laboratorio, i referti per immagini e le lettere di dimissioni).

sostituiscono a quelli previsti dal GDPR, ma ad essi si affiancano, lasciando all'interessato la scelta del quadro giuridico di riferimento sul quale poggiare la propria richiesta (a patto che, naturalmente, ne ricorrano i rispettivi presupposti)[69].

Con riguardo al diritto alla portabilità, la formulazione del testo normativo ha conosciuto alcune significative evoluzioni. Nella proposta della Commissione, l'art. 3, par. 8, riconosceva alle persone fisiche il diritto di richiedere ai «titolari dei dati sanitari» (health data holder)[70], purché si trattasse di soggetti «del settore sanitario o della sicurezza sociale o dei servizi di rimborso»[71], la trasmissione (diretta) dei propri dati sanitari ad altri soggetti dello stesso settore. Nella versione attuale, che risulta dall'Accordo raggiunto dalle Istituzioni UE (Art. 8d), destinatari della richiesta degli individui – oltre che dei dati trasmessi su iniziativa degli stessi – sono, più specificamente, i prestatori di assistenza sanitaria. In aggiunta, è consentita la trasmissione («one way only») ad un soggetto, "chiaramente individuato" del settore della sicurezza sociale o dei servizi di rimborso. Queste modifiche soggettive valgono come conferma di un'ulteriore limitazione, sul piano oggettivo, che invero già traspariva dal testo originario della Proposta: in questa forma[72], il diritto alla portabilità può essere esercitato nel solo contesto dell'uso primario dei dati sanitari elettronici[73].

Nonostante queste limitazioni sul piano oggettivo e soggettivo, per un verso, riemergono i progressi altrove già segnati dalla portabilità (in particolare: l'irrilevanza della base giuridica, l'immediatezza della trasmissione, il coinvolgimento dei fabbricanti dei servizi informatici nei conseguenti obblighi[74])[75], e sono raggiunti, per altro verso, ulteriori traguardi.

---

[69] Considerando 6 del testo risultante dall'Accordo. Per un confronto con le attuali potenzialità del diritto alla portabilità di cui all'art. 20 GDPR, che infatti già può avere ad oggetto dati sanitari (nei limiti della sua disciplina), v. D. TUZZOLINO, *La portabilità dei dati sanitari*, in AA. VV., *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, a cura di A. THIENE e S. CORSO, Napoli, 2023, 59-90.

[70] Il titolare dei dati sanitari, ai sensi dell'art. 2, par. 2, lett. y), della Proposta, come rivisto dall'Accordo provvisorio, è «any natural or legal person, public authority, agency or other body in the healthcare or the care sectors; including reimbursement services when needed as well as any natural or legal person developing products or services intended for the health, healthcare or care sectors; developing or manufacturing wellness applications; performing research in relation to the healthcare or care sectors; or acting as a mortality registry; as well as any Union institution, body, office or agency», che, alternativamente, riveste la qualità di titolare del trattamento di dati sanitari (avendo il diritto o l'obbligo di trattare tali dati nei contesti rilevanti indicati dalla norma) oppure ha la capacità di rendere disponibili, registrare, fornire (o restringere l'accesso ai) dati sanitari elettronici non personali, mediante il controllo della progettazione tecnica di un prodotto e dei servizi correlati,

[71] Non erano quindi comprese le applicazioni per il benessere, pur essendo queste in grado di registrare dati sanitari, utili tanto ad un uso primario (v. *infra*), quanto ad un uso secondario.

[72] Rimane dunque ferma la possibilità di esercitare il diritto generale alla portabilità dei dati, ai sensi dell'art. 20 GDPR.

[73] Tale limitazione poteva già ricavarsi, nella formulazione dell'art. 3, par. 8, della Proposta, oltre che dalla collocazione della disposizione, anche dalla specificazione che il "titolare dei dati" dovesse essere affiliato al «settore sanitario o della sicurezza sociale». Cfr., su questo punto, W. LI, P. QUINN, *op. cit.*, 8 s. Secondo l'opinione che tali Autori hanno formulato con riguardo alla formulazione originaria della Proposta, tuttavia, dall'assenza di un riferimento specifico alla finalità nell'articolato normativo, sembrava più convincente ritenere che, pur dovendo i dati provenire dal contesto dell'uso primario, tale uso non fosse poi vincolante per il destinatario, a condizione che tale soggetto possa dirsi comunque appartenente alla categoria dei prestatori di servizi sanitari (ivi, 9 s.).

[74] V. artt. 1, par. 3, e 17 ss. Accordo provvisorio, in relazione alle cartelle cliniche e alle applicazioni per il benessere che dichiarano l'interoperabilità con un sistema di cartelle cliniche elettroniche.

[75] Cfr. Considerando 11 dell'Accordo provvisorio.

Anzitutto, questa versione del diritto alla portabilità, che ripete il modello "diretto" dell'art. 20, par. 2, GDPR, non è limitato, come in quella sede, ai casi in cui risulta «tecnicamente fattibile». La fattibilità tecnica, oltre che l'immediatezza della trasmissione, è, infatti, data per presupposta dal nuovo Regolamento[76]. Superando un ulteriore limite di effettività della portabilità generale del GDPR, l'interoperabilità dei dati (almeno di quelli che rientrano nelle categorie prioritarie di cui all'art. 5 Accordo provvisorio) è garantita dall'impiego dei formati europei di scambio delle cartelle elettroniche elaborati dalla Commissione, pure nel caso in cui i prestatori di attività sanitarie sono situati in diversi Stati membri[77].

Meritano, infine, di essere segnalate l'inclusione dei dati inferenziali [78], nonché la completa gratuità (non solo per l'interessato ma) anche per il destinatario dei dati, qualità, questa, già prevista dalla Proposta[79], confermata dall'Accordo interistituzionale[80].

Sempre nel contesto dell'uso primario, riaffiora altresì una diversa idea della portabilità, che non ha i contorni della situazione soggettiva, ma che si ricollega immediatamente all'obiettivo della libera circolazione dei dati sanitari attraverso canali sicuri[81], direttamente funzionale al diritto alla salute nella sua dimensione digitale [82], attraverso l'alimentazione delle cartelle sanitarie

È dubbio se il diritto contemplato nella Proposta riguardi, oltre ai dati personali, anche quelli non personali. Sul punto, si registrano indicazioni letterali contrastanti: da un lato, infatti, il riferimento ai dati *tout court* e al prestatore di assistenza sanitaria (e, prima, nella versione originaria al *data holder*) anziché al titolare del trattamento induce ad una risposta positiva al quesito; d'altro canto, l'intitolazione della Sezione I in cui è inserito l'art. 3 induce a restringere il campo di applicazione ai soli dati personali (v., in questo senso, W. Li, P. Quinn, *op. cit.*, 7 s.). Inoltre, se si confronta questa evoluzione del diritto alla portabilità con quella che ha caratterizzato altri strumenti recenti del diritto dell'Unione (ad esempio, il Data Act: v. *supra*, par. precedente), si nota come questo diritto tenda ad estendersi anche ai dati non personali se tale situazione soggettiva è strumentale ad una logica di mercato, aprendosi piuttosto il problema di selezionare un criterio di rilevanza che giustifichi la portabilità di informazioni non legate ad un individuo (nel citato Data Act, tale criterio consiste nel fatto che il dato non personale rientra pur sempre nell'ambito di una definizione che scopre un qualche collegamento con l'utente del bene o del servizio correlato, trattandosi di una «digitalizzazione delle azioni e degli eventi» ad essi relativi: v., *supra* nota 54). Tale logica non è però condivisa dal provvedimento normativo ora in esame.

[76] I. Rapisarda, *Sul costituendo spazio europeo dei dati sanitari*, cit., 417.

[77] V. l'art. 6 dell'Accordo manda alla Commissione la definizione dei formati europei di scambio delle cartelle elettroniche. I dati ricevuti in questo formato, oltre che dovere essere accettati, devono potere essere pure fruiti: v. artt. 6, par. 3, e 8d, parr. 2 e 4 dell'Accordo. V. infine anche il considerando 12.

[78] Vi rientrano diagnosi, test e esami medici: Considerando 5. L'inclusione di questi dati consente una visione olistica del paziente (W. Li, P. Quinn, *op. cit.*, 7), ciò che è alla base della medicina personalizzata e di precisione.

[79] Nella versione originaria l'art. 3, par. 8, comma 3, della Proposta prevedeva una "deroga" all'art. 9 DA. Un successivo emendamento del Parlamento europeo alla medesima disposizione («[U]n titolare dei dati sanitari, un destinatario dei dati sanitari o un terzo non addebita direttamente o indirettamente agli interessati tariffe, compensazioni o costi per la condivisione dei dati o l'accesso agli stessi») si spiegava con l'intento di bandire pratiche di traslazione dei costi che avrebbero vanificate nella sostanza la previsione della gratuità.

[80] Art. 9a Accordo provvisorio.

[81] Per l'uso secondario dei dati sanitari, la Proposta mira a creare una base giuridica per il trattamento, ai sensi degli artt. 6 e 9 GDPR (cfr., in particolare, considerando 37 Accordo provvisorio). Si specifica, tuttavia, il diritto delle persone fisiche di esercitare un (revocabile) opt out rispetto all'uso dei propri dati per l'uso secondario (art. 35f Accordo provvisorio).

[82] Come ricorda il considerando 19 del testo risultante dall'Accordo, obiettivo dell'Unione è che tutti i cittadini abbiano accesso ai loro fascicoli sanitari elettronici entro il 2030: Programma strategico per il decennio digitale 2030 (Decisione UE 2022/2481del Parlamento europeo e del Consiglio dell'Unione del 14 dicembre 2022).

elettroniche[83]. Qui confluiscono i dati dei pazienti, ai quali i professionisti sanitari possono accedere[84] per prestare l'attività di cura e per aggiornarli[85], salve limitazioni poste dai pazienti medesimi[86], i quali non sono invece tenuti ad un'azione positiva per rendere possibile la circolazione delle informazioni che li riguardano[87].

7. Osservazioni conclusive. La declinazione al plurale della portabilità e la sua rilevanza al di fuori della disciplina dei dati.

Se si guarda dalla prospettiva dell'interessato (data subject), il diritto alla portabilità sui propri dati personali, nei pochi anni di vita a far data dalla sua codificazione nell'art. 20 GDPR, ha conosciuto una evoluzione significativa, grazie ai numerosi interventi legislativi che, affinandone le potenzialità, ne hanno via via esteso l'ambito di applicazione (per un verso, quanto all'oggetto, includendo chiaramente, oltre ai dati forniti, quelli osservati e, persino, in certi

[83] La «cartella clinica elettronica», secondo una nomenclatura che non corrisponde a quella nazionale in uso (v. C. SARTORIS, *Sanità digitale e tutela dei dati personali*, in AA. VV., *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche e sulle loro conseguenze giuridiche*, a cura di A. ADINOLFI e A. SIMONCINI, Napoli, 2022, 356 ss.) è definita dall'art. 2, par. 2, lett. m), come «una raccolta di dati sanitari elettronici relativi a una persona fisica e rilevati nell'ambito del sistema sanitario, il cui trattamento avviene ai fini della prestazione di servizi di assistenza sanitaria». Nell'ordinamento italiano, l'art. 12 d.lg. n. 179/2012, modificato numerose volte, ha introdotto il fascicolo sanitario elettronico (FSE), definito al co. 1°, come «l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale»: v., per una chiara sintesi, S. CORSO, *Sanità digitale riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, in AA. VV., *La protezione dei dati sanitari*, cit., 91 – 128. La disciplina, oltre che nel menzionato articolo, è attualmente contenuta nel d.m. 7 settembre 2023, emanato a seguito delle *Linee guida per l'attuazione del Fasciolo sanitario elettronico* (d.m. 20 maggio 2022) nell'ambito degli obiettivi del PNRR (v. S. CORSO, *Il fascicolo sanitario elettronico 2.0. Spunti per una lettura critica*, in *Leggi civili comm*, 2024, II, 334 – 462; I. RAPISARDA, *Appunti sul fascicolo sanitario elettronico 2.0*, in *Resp. medica*, 2024, I, 57 – 68). In linea di principio, al fascicolo i sanitari possono accedere solo con il consenso esplicito dell'assistito (salvo casi di emergenza: artt. 8 e 20); non sono visibili i «dati soggetti a maggiore tutela dell'anonimato» (elencati nell'art. 6 d.m. cit., ad es., la sieropositività all'HIV), salva diversa determinazione dell'interessato. L'alimentazione (art. 12) delle informazioni non richiede il consenso dell'assistito, il quale può però esercitare un diritto all'oscuramento di alcuni dati, peraltro sempre revocabile (art. 9). Lo stesso interessato può aggiungere, in una sezione particolare del fascicolo (c.d. «taccuino personale») alcuni dati ulteriori, «anche generati dai dispositivi medici e/o wearable» (art. 5).

[84] Ai sensi dell'art. 7a Accordo provvisorio (v. già art. 4, par. 3, della Proposta originaria). Tali dati possono comprendere quelli raccolti dalle applicazioni per il benessere che offrono l'interoperabilità con la infrastruttura tecnica della cartella clinica: art. 31a Accordo provvisorio, il quale precisa che, in ogni caso, la condivisione la trasmissione di tali dati deve basarsi sul consenso della persona fisica.

[85] Alla luce dei principi di minimizzazione e di limitazione della finalità, l'accesso è limitato per entità ed estensione alla funzione di cura prestata dal professionista. Su invito del Parere congiunto dell'EDPB e dell'EDPS (ivi,18 s.), era stato precisato da un emendamento del Parlamento europeo all'art. 4, par. 3, dell'originaria Proposta che il trattamento è lecito in forza della base giuridica di cui all'art. 9, par. 2, lett. h), GDPR (e nei limiti della medesima, senza la necessità del consenso). Nonostante tale precisazione non sia più ripresa, almeno in termini chiari, dal testo risultante dall'Accordo, si può confermare tale conclusione anche nel nuovo assetto, movendo specialmente dalla valorizzazione della volontà negativa del paziente: v. *infra*.

[86] Artt. 8e e 8h Accordo provvisorio, che prevedono rispettivamente il diritto di restringere l'accesso ai dati contenuti nella cartella clinica o a parte di essi e un diritto, che può essere introdotto dagli Stati membri, di opt out dall'accesso di tali dati nel contesto dell'uso primario.

[87] Le persone fisiche possono inserire nella propria cartella clinica elettronica dati relativi alla loro salute: questi devono essere contraddistinti per la loro provenienza e in nessun caso possono alterare i dati inseriti dai professionisti sanitari (art. 8b Accordo provvisorio), ferma la possibilità di esercitare il diritto di rettifica (Art. 8c Accordo provvisorio).

casi, quelli inferenziali; per altro verso, superando, quanto a presupposti, il riferimento alle basi giuridiche del consenso o dell'esecuzione del contratto). In linea con la dimensione di compromesso del diritto (tra interesse della persona fisica e interessi contrapposti del titolare del trattamento, da un lato, e tra quello che rappresenta l'ottimo ideale sul piano degli obiettivi e la realtà della tecnica e la condizione economica delle imprese, dall'altro), il rafforzamento della portabilità non è stato generalizzato, ma ha riguardato, per così dire a macchia di leopardo, diverse realtà, alla luce ora della tipologia dei soggetti coinvolti (ad esempio i gatekeeper, per la posizione che essi hanno sul mercato), ora del tipo di dati oggetto della disciplina (ad esempio, i dati raccolti dall'IoT), ora, sebbene ancora solo in prospettiva, del particolare settore a cui questi si riferiscono (i cc.dd. spazi europei dei dati, ad iniziare da quello, che va profilandosi, dei dati sanitari). L'espansione della portabilità ha assunto diverse forme: in alcuni casi, il legislatore europeo ha fissato, nella veste di una sorta di obblighi di risultato, determinati standard qualitativi che superano quelli della 'versione base' dell'art. 20 GDPR (art. 6, par. 9, DMA); ancora, in molti casi, sono stati previsti diritti che si affiancano alla portabilità originaria, finendo per 'integrarla' nel perimetro in cui le due situazioni soggettive coincidono, ma disvelando altresì un contenuto che va ben oltre. Mentre l'estensione ai dati non personali rappresenta è sempre più frequente, tali diritti concernono, in alcuni casi (art. 6, par. 10, DMA e art. 5 DA), financo dati personali di terzi.

Ne discende una declinazione al plurale della portabilità, che si afferma già sul piano della tutela dell'individuo e del controllo che questo deve potere esercitare sui propri dati, ma che lo trascende, disvelando una prospettiva nuova con la quale il legislatore europeo guarda ai dati.

Nella direzione del rafforzamento del controllo dell'individuo sui propri dati, va segnalato che, nella *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, proclamata solennemente dalla Commissione, dal Parlamento e dal Consiglio, le Istituzioni dell'Unione si sono impegnate, tra le altre cose, «a garantire l'effettiva possibilità per i singoli individui di trasferire facilmente i propri dati personali e non personali tra diversi servizi digitali, in linea con i diritti di portabilità» (Capitolo V, "Vita privata e controllo individuale sui dati")[88].

Più in generale, emerge chiaramente, dal rapido incedere legislativo, la tendenza all'emancipazione della portabilità dalla logica e dai confini della tutela dei data subject, per divenire, altresì, veicolo di trasmissione anche di dati non personali (nei limiti in cui chi ne ha interesse sia legittimato a domandarla), fino a dare forma ad una pretesa esercitabile anche da un titolare di trattamento, purché ricorra una base giuridica che, ai sensi del GDPR (art. 6 e, in caso di informazioni sensibili, 9 del Regolamento), legittimi una simile operazione sui dati personali altrui. Il tutto senza trascurare che, in taluni settori, il trasferimento dei dati si giustifica in via automatica, ciò che richiede, anche in questo caso (nella misura in cui si abbia a che fare con dati personali),

[88] Sul valore programmatico della Carta, sulle orme della Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza nel dicembre del 2001, v. G. Alpa, *La dichiarazione europea dei diritti digitali*, in *Contratto e impresa Europa*, 2023, II, 185.

una base giuridica (che, come si è visto, la Proposta per un regolamento sullo spazio europeo dei dati sanitari si premura di codificare per questo settore).

In questa veste plurale, la portabilità dei dati si è così progressivamente consolidata come uno degli assi portanti dell'economia europea dei dati[89]. Nel continuo e complesso bilanciamento tra protezione della persona ed esigenze di circolazione, prendono piede meccanismi di condivisione dei dati sempre più articolati[90], che enfatizzano la natura strumentale delle informazioni rispetto ad obiettivi che si iscrivono sia all'interno della sfera della personalità (come nel caso del diritto alla salute), sia nella logica di mercato (potenziare il consumatore, favorire lo sviluppo di nuovi servizi, incentivare la concorrenza).

Alla complessità delle dimensioni della portabilità e al collegamento funzionale dei dati con finalità ulteriori, si collega inevitabilmente la necessità, da parte degli interpreti e degli operatori, di ampliare lo sguardo, uscendo dal diritto dei dati in senso stretto, per esaminare anche gli ambiti rispetto ai quali questo è contiguo.

Due esempi riguardano la tutela del diritto dei consumatori e del mercato, dalla cui prospettiva può divenire rilevante il mancato raggiungimento di determinati standard qualitativi della portabilità dei dati, e ciò persino dove la normativa ad essa dedicata non è ancora giunta ad imporre obblighi specifici in termini di risultati da garantire all'interessato (ad esempio, con riguardo alla interoperabilità).

Con riguardo ai consumatori, la dottrina tedesca ha già messo in evidenza che l'utilizzo da parte di fornitori di contenuti o servizi digitali di formati per i dati personali trattati che compromettono l'interoperabilità e, dunque, l'effettività del diritto alla portabilità *ex* art. 20 GDPR, può rilevare nei termini di un difetto di un requisito di conformità – in relazione al ciò che può normalmente attendersi il consumatore – dell'oggetto dell'acquisto[91]. Sul versante della tutela della concorrenza, infine, è emersa, anche prima del DMA, la prospettiva che rinviene un possibile abuso di posizione dominante nelle condotte delle piattaforme digitali che ostacolano la portabilità effettiva dei dati dei propri utenti, impedendo loro di estrarli e di trasmetterli alle imprese concorrenti, e così finendo per ledere principalmente la contendibilità del mercato[92].

---

[89] Accesso ai dati, interoperabilità e portabilità transfrontaliera dei dati sono tra gli obiettivi dell'attività legislativa europea in materia di dati, come si legge nella Risoluzione del Parlamento europeo del 25 marzo 2021 su una strategia europea per i dati (2021/C494/04).

[90] G. Marino, *op. cit.*, 53 ss.

[91] M. SCHMIDT-KESSEL, *La responsabilità contrattuale del gestore di una piattaforma per la protezione dei dati personali del cliente nella prospettiva dei requisiti di qualità dell'adempimento*, in *Pactum*, 2023, 153 – 162: 159; M. DÜMELAND, *Sachmangelhaftigkeit von Software bei nicht DSGVO-konformer Entwicklung*, in *DSRI-Tagungsband*, 2018, Edewecht, 649. Che la violazione delle regole sul trattamento dei dati personali possa tradursi in un difetto di conformità (arg. *ex* considerando 48 dir.) è del resto chiaro anche alla dottrina italiana: v. già C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.*, 2019, III, 514; C. IRTI, *Consenso negoziato e circolazione dei dati personali*, Torino, 2021, 140.

[92] L'AGCM, su segnalazione di una società operativa nel mercato emergente dell'intermediazione dei dati (e la cui attività si fonda, in particolare, sull'esercizio del diritto alla portabilità da parte degli utenti di grandi piattaforme digitali, al fine di raccogliere i dati da questi condivisi e investirli riversando sugli stessi utenti buona parte dei profitti), ha avviato il 5 luglio 2022 un'istruttoria contro Google-Alphabet (provvedimento disponibile al sito https://www.agcm.it/dotcmsCustom/getDominoAttach?urlStr=192.168.14.10:8080/41256297003874BD/0/B7FC348D8D737417C1258883004DD3E7/$File/p30215.pdf; ultimo accesso: 18 luglio 2024), rilevando

che il servizio da questo creato per consentire ai propri utenti l'esercizio del diritto alla portabilità (*Google Takeout*) non fosse sufficiente a garantire l'effettività di questo diritto, a causa della farraginosità che connota tale servizio e della necessità di un continuo intervento da parte degli interessati. Nella sostanza, sono stati rilevati «ostacoli all'individuazione di meccanismi di interoperabilità idonei a rendere i dati presenti nella (…) piattaforma disponibili a piattaforme alternative», così determinando «un indebito sfruttamento (…) dei consumatori finali». Tale condotta limiterebbe i «benefici che i consumatori potrebbero trarre dalla valorizzazione dei loro dati personali», oltre che «la possibilità di operatori alternativi a Google di sviluppare forme innovative di utilizzo» degli stessi, così consentendo a Google di «preservare la propria posizione nello sfruttamento commerciale della mole dei dati personali resi a essa disponibili attraverso la posizione detenuta su una varietà di mercati digitali». Il presupposto del ragionamento dell'Autorità è che la portabilità configuri «uno strumento normativo teso a garantire il pieno esplicarsi di dinamiche competitive nell'ambito dei mercati digitali». Con successivo provvedimento del 18 luglio 2023 (://www.agcm.it/dotcmsCustom/getDominoAttach?urlStr=192.168.14.10:8080/41256297003874BD/0/42A8996C723B26AAC12589FD003925C3/$File/p30736.pdf ultimo accesso: 18 luglio 2024), l'AGCM ha reso vincolanti gli impegni assunti da Google, i quali, nella sostanza, vertono, sullo sviluppo dell'automatizzazione di *Takeout* e sul miglioramento dei meccanismi di interoperabilità che assicurino alle altre piattaforme l'accessibilità ai dati raccolti da Google. È previsto, infine, il rilascio di una soluzione di portabilità diretta da servizio a servizio, tramite un API (*Application Programming Interface*). Da ultimo il progetto è stato ribadito da Oliver Bethell, *Legal Director* presso Google, nel post «*Un aggiornamento su come ci stiamo preparando al Digital Markets Act*», pubblicato il 17 gennaio 2024 sul Blog di Google Italy (https://blog.google/intl/it-it/notizie-aziendali/un-aggiornamento-su-come-ci-stiamo-preparando-al-digital-markets-act), soprattutto in vista dell'obiettivo di adeguarsi all'obbligo di portabilità effettiva a cui la stessa Google (Alphabet) è soggetta in base al DMA in quanto *gatekeeper* (*supra*, par. 3). Oltre a *Takeout*, è stata altresì richiamata la *Data Transfer Initiative*, organizzazione di esperti creata su impulso di Apple, Meta, and Google per la creazione di soluzioni interoperabili finalizzate all'attuazione della portabilità diretta (https://dtinit.org/). Un successivo post dello stesso autore sul medesimo blog («*Come ottemperiamo al Digital Markets Act*», pubblicato il 5 marzo 2024, https://blog.google/intl/it-it/come-ottemperiamo-al-digital-market-acts) ha annunciato il lancio della "Data Portability API per gli sviluppatori". Sul possibile collegamento tra la portabilità e l'abuso di posizione dominante v. pure da H. SCHWEITZER, A. METZGER, *Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?*, in *GRUR International*, 2023, IV, 340 ss.

SECTION III

FOCUS PAPERS

Popa Tache CE, Săraru CS, Kouroupis K, 'Different perspectives concerning the right not to use the internet and some analogies with education' (2024) 1 EJPLT, 179-193.
DOI: https://doi.org/10.57230/EJPLT241CEPTCSSKK

EJPLT
ISSN 2704-8012



Different perspectives concerning the right not to use the internet and some analogies with education

Diverse prospettive sul diritto a non usare internet ed alcune analogie con l'istruzione

CRISTINA ELENA POPA TACHE
Associate Professor of Public International Law and Communications and New Technologies Law
Bucharest University of Economic Studies
Researcher at CIRET - Center International de Recherches et Études Transdisciplinaires, Paris

CĂTĂLIN SILVIU SĂRARU
Associate Professor of Administrative Law
Bucharest University of Economic Studies

KONSTANTINOS KOUROUPIS
Assistant Professor of European and Data Rights Law
Frederick University

Abstract
This paper investigates the recent option regarding the right not to use the internet, establishing direct connections with related rights. In the era of digital connectivity, we observe how, at the heart of shaping societal dynamics, the concept of an individual's right to abstain from online participation raises fundamental questions regarding legal and ethical aspects. The article critically analyses some theoretical considerations and the legal implications associated with the right not to use the internet. The line pursued involves a detailed examination of potential intersections and similarities with the more well-defined right to refuse education. Through a comparative approach, not necessarily targeting specific population samples, the analysis traverses legal systems, international human rights standards, and tested societal norms. The aim of this endeavor is to learn some lessons from the synergies and tensions between these rights. The boundaries of individual autonomy, privacy, and access to information represent the focal point where the state and the individual must now find a balanced solution together.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Questo articolo indaga la recente opzione relativa al diritto a non utilizzare Internet, stabilendo connessioni dirette con i diritti connessi. Nell'era della connettività digitale, osserviamo come, al centro delle dinamiche sociali, il concetto di diritto individuale ad astenersi dalla partecipazione online sollevi questioni fondamentali riguardanti aspetti legali ed etici. L'articolo analizza criticamente alcune considerazioni teoriche e le implicazioni legali associate al diritto a non utilizzare Internet. La linea adottata prevede un esame dettagliato delle potenziali intersezioni e similitudini con il diritto a rifiutare l'istruzione, tema maggiormente trattato. Attraverso un approccio comparativo, non necessariamente rivolto a campioni specifici di popolazione, l'analisi attraversa i sistemi giuridici, gli standard internazionali dei diritti umani e le norme sociali testate. Lo scopo di questo elaborato è quello di trarre alcuni insegnamenti dalle sinergie e dalle tensioni tra questi diritti. I confini dell'autonomia individuale, della privacy e dell'accesso alle informazioni rappresentano il punto focale in cui lo Stato e l'individuo devono trovare insieme una soluzione equilibrata.

Keywords: internet; international law; human rights; technology; education; society; state responsability.

Summary: 1. Introduction. – 1.1. Scientific relevance and importance of the topic. – 2. A definition and analysis of the right not to use the internet. – 3. A legal perspective on the right to refuse education. – 4. Parallels between the right not to use the internet and the right to refuse education. – 5. Conclusions.

1. Introduction.

The right not to use the internet is considered one of the most sensitive and difficult issues in society today. It is true that we cannot discuss internet use as a general phenomenon, but when comparing it with education, we can consider the common parameters that draw the boundaries between the two[1]. We face not only legal dilemmas, but also ethical or social dilemmas. Most considerations call for a balance in theoretical debates in general. Among the most relevant is that this possibility is a personal choice motivated by several factors. In deciphering legal solutions sociology has provided a base of useful results such as quantity of use, variety of use and types of internet use[2]. So far, the right to refuse education is based on this. In analysing internet use sociologists have often used standard demographic variables based on four categories of education: absence of education, secondary education, higher

[1] Although the present paper is fabricated from legal research material, from a sociological point of view, see more on the ownership space of the internet use and the three main dimensions: amount of use, variety of different uses, and types of use in G Blank, D Groselj, 'Dimensions of internet use: amount, variety, and types' (2014) 17(4) Information, Communication & Society, 417-435.

[2] See PB Brandtzæg, 'Towards a unified media-user typology (MUT): A meta-analysis and review of the research literature on media-user typologies' (2010) 26(5) Computers in Human Behaviour, 940-956; or AH Barton, 'The concept of property space in social research', in PF Lazarsfeld and M Rosenberg (eds), *The language of social research: A reader in the methodology of social research* (Free Press, 1955) 40-53. For some sociological differences also see AJ van Deursen, JA van Dijk, 'The digital divide shifts to differences in usage, New Media & Society' (2013) Advance online publication <DOI: 10.1177/1461444813487959> accessed 15 January 2024.

education and university education. Going further in our demonstration, in search of legal custom, it should be noted that in terms of social point of view the considerations are given by: race (white or non-white), location (urban versus rural), living status (students, employed, unemployed and retired), marital status, gender and age. From these perspectives there may be found some similarities between the internet and education, which leads and supports lawyers to find similar regulatory possibilities[3]. Demographically there are sociological variations but legally speaking the primary guidelines derive from international conventions which are absorbed into national laws. In other words, the dimensions analysed separately by sociology are found united in the legal sciences. Legal phenomena are identified by sociology and then transposed into rules by the legal sciences. The use of the internet or new technologies as a form of education is indicated to be expressly mentioned in international and national legal instruments together with their characteristic limits. In democratic societies, it is recognized that individual rights and personal freedom are fundamental, established under the auspices of many European and international legal texts, such as the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights. All these reasons may increasingly resemble the right to refuse education, which has also come to intersect with new technologies. As far as Internet use is concerned, the experience from education that no one can be legally forced to exercise this right without restrictions can be applied. 'The law must reflect, in its progressive flexibility, the increasing possibilities of choice for rights holders who are adults *in fieri*'[4]. How can humanity enjoy a healthy individual autonomy?

The contents of this article are intended to provide answers which would stimulate critical thinking and scientific sparks. Staying off the internet can be a way for some to protect their privacy and avoid exposure to online security risks, as some people choose to keep their personal information and activities away from digital space. Offline lifestyles lead individuals to choose to live in a more traditional way, focusing on face-to-face interactions and traditional activities over online ones. Sociologically, the preference for reading in print, socialising in person and other offline activities have been included in these trends. However, this article will, by its specific features, fall into the category of legal research work at an inter- and multidisciplinary level.

The analysis touches on the issue of state responsibility and legal protection. Their tendency is either to protect or to restrict the right not to use the internet

[3] For example, S Livingstone, H Helsper, 'Gradations in digital inclusion: Children, young people and the digital divide' (2007) 9(4) New Media & Society, 671-696 <DOI: 10.1177/1461444807080335> accessed 15 January 2024 or N James, 'Countering Far-Right Threat through Britishness: The Prevent Duty in Further Education' (2022) Critical Terrorism Studies <DOI: 10.1080/17539153.2022.2031135> accessed 16 January 2024. Online first, for regression analysis in investigating the impact that strains and resilience, individuals' gender, economic situations, individual life experiences, and internet use have on their propensity to associate with, engage with, and support far-right ideologies and associated violence see J Skoczylis, S Andrews 'Strain theory, resilience, and far-right extremism: the impact of gender, life experiences and the internet' (2022) 15(1) Critical Studies on Terrorism, 143-168 <DOI: 10.1080/17539153.2022.2031137> accessed 15 January 2024.

[4] JL Gaviria, 'Education: a Compulsory Right? A Fundamental Tension within a Fundamental Right' (2022) 70(6), British Journal of Educational Studies, 653-675 <DOI: 10.1080/00071005.2021.2024136> accessed 15 February 2024.

in the public interest. For individuals, however, opting out of the internet can be a form of protection against digital addiction in order to maintain a balance in their lives, but also to avoid the negative impact of excessive internet use. The reasons for this are diverse and their analysis points to cross-disciplinary methodologies, without which it seems almost impossible to advance human rights. This may include the decisions of a part of the world's population to avoid the internet for ethical or philosophical reasons related to data collection, manipulation of information or other aspects of the online environment[5]; for others, access to the internet may be limited due to financial or geographical resources, so that giving up the internet may be a consequence of lack of accessibility to technology.

The issues take on conflicting nuances when those who claim this right find themselves antagonistic, at some point, to those for whom, in the modern world, the internet has become an essential tool for access to information, communication and participation in various aspects of social and economic life. This is therefore a personal choice that may have certain consequences. Both the premises and the effects of the right not to use the internet are analogous to the right to refuse education.

1.1 Scientific relevance and importance of the topic.

Scientifically approaching the subject presented requires a multidisciplinary (even transdisciplinary) perspective that encompasses legal, social, psychological, educational, religious, cultural and technological sciences. According to the authors, neither the obligation to use the internet nor the right not to use it is enshrined. Both the right not to use the internet and the right to refuse education are manifestations of individual autonomy, with significant implications for privacy, personal development and freedom of choice. in addition to all this, there a need for uniform regulation.

Relevant discussions concern the current context of the digital society and the importance of education in the information age, the rationale, the social and psychological effects of giving up the internet, internet addiction, the assessment of the social impact on individuals who choose not to use the internet, the rights of vulnerable people such as children and the elderly, for example, or the impact on personal and professional development. Ultimately, we are faced with the imperative of reconciling society's needs and interests, especially from a legal point of view, where the way out is to identify the limits and rules that could ensure a balance between individual rights and the common good.

2. A definition and analysis of the right not to use the internet.

The right not to use the internet can be conceptualised as an expression of individual autonomy, recognised as part of the right to privacy and personal

[5] See A Weinstein, M Lejoyeux, 'Internet Addiction or Excessive internet Use' (2010) 36(5) The American Journal of Drug and Alcohol Abuse, 277-283 <DOI: 10.3109/00952990.2010.491880> accessed 15 February 2024.

liberty. The European Convention on Human Rights has given a broad interpretation of the term "private life" corresponding not only to physical but also to psychological and ethical integrity[6]. This prerogative gives individuals the possibility to voluntarily distance themselves from the online environment, based on ethical choices, personal values or security concerns, without affecting their fundamental rights to education and access to information in available non-digital alternatives. Sometimes these socio-legal possibilities of distancing oneself from the internet are justified by medical sciences which claim the emergence of a new type of addiction, as discussed in the literature[7]. Internet addiction has been found to exist to a similar extent as drug and alcohol abuse, pathological gambling and even video game addiction [8]. However, from this point of view we cannot say that there is also abuse of education, although the new internet addiction can create marital, academic and work-related problems sometimes in the same way as education. Without going into the differences between pathology and problematic, we will only seek to facilitate the identification of launch pads for optimal legal regulation. Another side is finding the dividing lines between abuse and need. In terms of access to the internet versus access to technologies, differences arise from the impossibility of accessing certain treatments due to inaccessibility, lack of knowledge, etc. For example, adequate health care is thus recognised as part of the human right to health[9]. Such inaccessibility would therefore affect the right to health itself and this can be suggested as one of the limitations of not using the internet (or health technologies).

Globally, explicit recognition of the right not to use the internet is still in its early stages and is more implicit than explicit in international legal documents. The evolution of this concept is shaped by the modern dynamics of international law and can be seen in the broader context of individual rights and their adaptation to societal trends, including the growing influence of technology and the internet.

Although not universally recognized, the right not to use the internet can now be defined as an individual's option to choose not to participate directly and actively online without facing negative consequences or discrimination, while still being free to manage their digital presence and always having their privacy protected. Ensuring respect for human rights is the responsibility of states, which must reconcile it with their interests in maintaining the security and smooth functioning of society in the digital age.The parallelism being noted in this material is also useful for new technologies in general, whether

---

[6] *X and Y v. The Netherlands*, 25 March 1985, no. 8978/80, *R and R v. Poland*, no. 27617/04 ECHR 2011, *Costello-Roberts v. UK*, 25 March 1993, no. 13134/87, LA Sicilianos, European Convention on Human Rights: Interpretation per article (in greek) (2nd edn, Nomiki Bibliothiki 2017), 375.

[7] BL Fortson, JR Scotti, YC Chen, J Malone, K Del Ben, 'Internet use, abuse, and dependence among students at a south-eastern regional university' (2007) 56(2) J Am Coll Health 137-144 and K Young, 'Internet Addiction: A new clinical phenomenon and its consequences' (2004) 48(4) American Behavioural Scientist, 402-415.

[8] A Weinstein, M Lejoyeux, 'Internet Addiction or Excessive internet Use' (2010) 36(5) The American Journal of Drug and Alcohol Abuse, 277-283 <DOI: 10.3109/00952990.2010.491880> accessed 15 January 2024.

[9] M Reglitz, A Rudnick, 'Internet access as a right for realizing the human right to adequate mental (and other) health care' (2020) 49(1) International Journal of Mental Health, 97-103 <DOI: 10.1080/00207411.2020.1727019> accessed 15 January 2024.

emerging or disruptive, where complex military or security issues are involved. Concerns about privacy and relevant rights, such as the European Union's General Data Protection Regulation (GDPR), have been brought to the fore, reflecting heightened concerns about the protection of personal data online. Rights to personal freedom and individual choice have always been at the heart of democratic societies, and their adaptation to technology is a natural and ongoing process[10].

While for some jurisdictions, the protection of the right to privacy and autonomy can be interpreted as including the right to decide not to use the internet, the right to refuse education is mostly discussed in the framework of children's rights and compulsory education regulations, sometimes giving parents the possibility to choose alternatives to traditional education. Will it be possible to strike a global balance between individual freedom to refuse the internet and the imperatives of a digitally (technologically) transforming society? More explicit and appropriate regulation are expected, both in terms of the wider concerns about fundamental human rights in relation to digital security, data protection and access to offline information, and in terms of sustainability. The reasons are already part of reality and already discussed in theory, one example being that the internet is referred to symbolically as the 'Cyber ocean'[11] where do we find this expression? Footnote here or even Baobáxia. These terms reflect the global dimension of the internet, comparing it to a continent or a virtual ocean in which information flows freely. Baobáxia, as part of a wider discussion about the evolution of the internet and society as a whole, metaphorically it is seen as a social-technical-ecological network of diverse actors grown out of the earth, or a network of 'terrestrial' actors, operating as a decentralised autonomous network, regardless of nation-state and ethnic group boundaries. Baobaxia has also proved to be a cause of digital and geographical 'reterritorialisation'[12].

As an ecological approach, like Baobaxia, the internet precedes Latour's call to reterritorialize the earth for future life[13]. Comparison is the fruit of transdisciplinary methodologies. 'Baobaxia draws a new, or rather, reminds us of an old cartography of the world, from longer and non-Eurocentric historical

[10] See an intense analysis of the right to privacy under the new digital rules in K Konstantinos, I Serotila, *Privacy and Security in light of the European Digital Agenda* (Nomiki Bibliothiki, 2022).

[11] JP Castro, 'Sailing the Cyber Ocean: The CISO's Journey Through Digital Storms', is an article published by the author on April 5, 2024, on their LinkedIn page available here: link, accessed on May 14, 2024. The term "cyber ocean" is primarily used in the context of cybersecurity. It emphasizes the idea that the internet is a virtual sea where information flows and interactions take place in what appears to be an infinite manner. This metaphor highlights the fluid and dynamic characteristics of the internet.

[12] S Zhang, M Ribeiro Porto Araujo, AC de Assis Nunes, 'A terrestrial internet from the quilombos: the transatlantic evolution of baobab from colonial to digital capitalism' (2022) 5(1) Tapuya: Latin American Science, Technology and Society <DOI: 10.1080/25729861.2022.2037818> accessed 15 January 2024. 'Baobáxia' raises the question of the material resources that underpin the internet and digital capitalism. It is seen by the authors 'as a digital network for sharing community-produced content that emerged in the "quilombos" (communities of descendants of runaway slaves) of Brazil in the early 2000s and spread to other marginalized groups in South America, Africa and Europe'. The analysis developed by this article reveals 'the articulation of ancestral knowledge and new technologies in building Baobaxia, a network that adapts to local conditions-geographical, ecological and infrastructural-and supports community resilience, autonomy and sustainability'.

[13] See explanations in B Latour, *Down to Earth: Politics in the New Climatic Regime* (Polity Press, 2018).

perspectives that can guide academic understandings of the world'[14]. The internet, whether we call it Baobaxia or the virtual high street or the virtual village, is metaphorically materialized to emphasize its social aspects and human interaction online, comparing it to traditional community relations in familiar or visual contexts. Each metaphor highlights different features of the online experience and the impact of the internet on society. What is certain is that we are dealing with a new legal phenomenon because the internet is not just a technical entity or a communication medium, but it radiates a wide range of legal issues. A person's right not to use it is directly proportional to its formal and detailed recognition in law, societal awareness and adaptation.

If we were to draw the general lines of the arguments for or against the right not to use the internet, we could see how the 'pro' category could include: 1) the right to privacy as a way to protect that prerogative and avoid excessive exposure of personal information online; 2) the right to make personal choices – a general principle of democratic societies according to which refusing to use the internet is an expression of individual autonomy; 3) the preservation of mental health with a role in reducing the negative impact of excessive use, such as stress and anxiety online; 4) the avoidance of digital addiction and the negative impact of excessive time spent online; 5) the option for an 'offline' lifestyle; or 6) the protection of the individual for some personal religious or traditional values. The arguments here are presented through the lens of the individual.

On the other hand, several arguments 'against' the right not to use the internet can be identified, such as: 1) access to information and education (to educational resources), in which case refusing it may limit learning and personal development opportunities; 2) the internet facilitates communication and social interaction, and absence from online platforms may lead to social isolation and limited connections with other people; 3) problems for labour law in terms of workplace efficiency or even career opportunities, as most employers use the internet in the recruitment process, and absence online may limit professional and career opportunities; 4) exclusion from participation in the digital economy, affecting access to services and business opportunities; 5) the internet brings advantages in terms of efficiency in communication, quick access to information and solving everyday problems, and its denial can lead to the loss of these advantages; 6) social exclusion we also can have social exclusion in the excessive use of internet... Many of the 'against' arguments we note are along the lines of problems raised by public authorities.

Many of these were also stated in the case of home schooling for example when discussions on education versus human rights were ongoing. In theory the question was 'If the promise of human rights is individual freedom, then a system that justifies or supports state control of education for the purpose of cultural conformity can be considered to be far too statist for a free and

[14] S Zhang, M Ribeiro Porto Araujo, AC de Assis Nunes, 'A terrestrial internet from the quilombos: the transatlantic evolution of baobab from colonial to digital capitalism' *(*2022) 5(1) Tapuya: Latin American Science, Technology and Society <DOI: 10.1080/25729861.2022.2037818> accessed on 15 February 2024. See for a comprehensive analysis C Fujikane, *Mapping Abundance for a Planetary Future: Kanaka Maoli and Critical Settler Cartographies in Hawai'i* (Duke University Press, 2021).

democratic society?" [15] Home education, as a case example, highlighted features of the geography of education, taking into account cultural and enticing traditions[16], the collapse of communist totalitarian regimes in the former Eastern bloc, the spread of neoliberalism, the reaction of neolocalism to the standardising effects of globalisation, international immigration and the successful integration of immigrants[17]. At first glance, the right not to use the internet may lend itself to the same features. Last but not least, the question arises whether the assertion of new international human rights could lead to the very violation of the human rights they are intended to protect? Looking back, the affirmation of the right to education in the category of human rights has led to such violations[18], just as home schooling has not been recognised in all states. In the same way, the right to the internet or to new technologies, by its inclusion in the category of fundamental rights, may today defeat the protection of the right not to use the internet. For these reasons, the incorporation of the right to refuse the internet into the category of human rights requires great care and precision, especially as 'the life you save may be our own'. Certainly, all discourse about the internet and rights as citizens' rights generates ideological, economic and political debates that need to be addressed and guided on the road to the codification. Precision in legal regulation is meant to erect unscalable walls between the effective protection of these rights and any vulnerability. To all these guidelines is added to the need for a rapid pace of decision that moves the discourse beyond philosophical rhetoric to practical policy interpretations[19].

Not using the internet has a number of practical consequences, some of them with immediate effect. We can refer here, as we have reported above, to limited access to information, research and news online, which can influence knowledge and perspective on the world, reality itself. Social exclusion includes the inability to access online services such as e-banking, online shopping and other activities related to the digital economy. In the face of these problems, what economic, political, social and legal alternatives can be identified? How could we propose to make the whole system work, including the labour market? Will the functions of the future include intermediaries or even internet trustees between society (or the public interest of the state) and those who refuse to use it? Will they be civil servants who ensure the functioning of the internet, digitisation and new technologies for the state? Can we imagine institutional departments or physical offices dedicated to these new work occupations through which alternative sources will be made available to those who do not want to use the internet? Perhaps these new

[15] MP Donnelly, 'The Human Right of Home Education' (2016) 10(3) Journal of School Choice, 283-296 <DOI: 10.1080/15582159.2016.1202069> accessed 20 February 2024.
[16] See X Sheng, 'Confucian home education in China' (2019) 71(6) Educational Review, 712-729 <DOI: 10.1080/00131911.2018.1471665> accessed 20 February 2024.
[17] D Hána, Y Kostelecká, 'A comparison of home education legislation in Europe from the perspective of geography of education' (2022) 37(5) Research Papers in Education, 603-632 <DOI: 10.1080/02671522.2020.1864762> accessed 20 February 2024.
[18] EF Henderson, 'Education as a human right: principles for a universal entitlement to learning' (2015) 45(4) Compare: A Journal of Comparative and International Education, 658-660 <DOI: 10.1080/03057925.2013.861692> accessed on 20 February 2024.
[19] T Oyedemi, 'Internet access as citizen's right? Citizenship in the digital age' (2015) 19(3-4) Citizenship Studies, 450-464 <DOI: 10.1080/13621025.2014.970441> accessed on 20 February 2024.

professions or trades will balance situations such as those where, in a professional context, refusal to use the internet can lead to difficulties in communicating with colleagues, clients or business partners who use online technology. It seems correct and feasible. The truth is that, currently, in our opinion, achieving such a result has been impossible, as the almost sudden emergence of today's internet has not allowed room or time for a natural transition. The rapid dynamics of technologies exhibit these traits. Legal custom could solve a number of problems for example, but it has a very special character when we talk about the internet or new technologies. Here, custom does not take a long time to form as it spreads faster than any other custom. We find custom only if we know how to look at it, at the stage where it is required to correlate these customary rights to the same extent as others such as net neutrality (already codified in several jurisdictions) or others such as digital discouragement, etc. Even if we are party to or witness to the legal custom of the right not to use the internet, the ultimate goal is its codification.

In terms of social implications, we can identify, first of all, perceptions of the world, perceptions that can be either very different or very limited, depending on the pole in which the individual is situated. The protection of privacy is contrasted with the recognition of the benefits of the internet which enhances individual autonomy, decision-making, information and online engagement according to their values, preferences and needs. If we consider the arguments of this paper, we can say that the right not to use the internet is nevertheless necessary and contributes to maintaining a healthy balance between online and offline life, thus promoting a diverse lifestyle. If something here runs counter to the public interest, then we are moving towards appropriate changes within the already reforming labour market.

3. A legal perspective on the right to refuse education.

In this matter we believe that the relevant issues have been settled and clarified. Education is better regulated in international legal instruments. Examples include: The against Discrimination in Education (1960, CADE)[20], the International Covenant on Economic, Social and Cultural Rights (1966, ICESCR)[21], the Convention on the Elimination of All Forms of Discrimination Against Women (1979, CEDAW)[22], and the Convention on the Rights of the Child (1989, CRC)[23]. Our analysis pivots around education specifically chosen from the group of human rights, although another topic of discussion could be the relationship between human rights and consumer rights[24]. The possibility

[20] UNESCO Convention against Discrimination in Education (adopted 14 December 1960, entered into force 14 December 1960) 429 UNTS 93 (CADE).
[21] International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR).
[22] Convention on the Elimination of All Forms of Discrimination Against Women (adopted 18 December 1979, entered into force 3 September 1981) 1249 UNTS 13 (CEDAW).
[23] Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC).
[24] As it has been strongly indicated in the COST Action Report, 'Between human rights and consumer protection in the digital age or the rights of digital consumers in the European and international context – The Digital Services Act example' published online by COST in GDRH Net –: *We do not have a definition of*

is affirmed by analysis of relevant legislation, judicial decisions and the principles of individual rights and the education system. Among the general issues that can be considered are individual rights such as the right to education, recognition that may not be based on the obligation to participate in a traditional education system, regulations that address home education, giving those concerned the option to refuse traditional schooling in favour of home education (may impose certain requirements and standards to ensure that home education meets the objectives of traditional education), and the obligation of the state to provide education. Refusal of education may call into question the state's responsibility to monitor and intervene if the refusal affects the child's welfare, for example through intervention by the competent authorities. In many jurisdictions parents are recognised as having the right to conscientious objection, allowing them to refuse certain elements of traditional education, such as certain aspects of the curriculum or certain school activities. We can also learn some useful lessons from the case of the internet.

In general, the right to refuse education is found in various contexts in international conventions and in the domestic law of some states, especially regarding parental rights and the right to education in general. We consider, for example the Universal Declaration of Human Rights (1948) where Article 26 recognises the right to education and this right should ensure access to compulsory and free basic education[25]. As para 2 of this article states that 'education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms. It shall promote understanding, tolerance and friendship among all peoples and all racial or religious groups (…)', so too can these issues be seen through the prism of the use of the internet and even new technologies. At the same time, the Convention on the Rights of the Child (1989) in Article 28 emphasises the right of children to education, recognising and encouraging the diversity of modes of education, including home education[26]. Another example is The Convention relating to the Status of Refugees (1951, Refugee

users, implying that a user can even be a robot or that the user is usually based on a contractual relationship with the provider, which is also true for the consumer. This leads us to establish the following relationship: does the user group include consumers or does the consumer group include users? When we enter the consumer v. user field we are left with the same vulnerability that currently exists, namely not having a uniform international definition for either consumer or user. By following the international normative uniformity, the parallel with education appears more favourable to the present research. Also see CE Popa Tache, 'About the Human Rights and Consumer Protection in the Digital Age of Digital Services Act 2022 or What Aspects Interested Investors Should Pay Attention To' (2023) 3(2) International Investment Law Journal, 121-132.

[25] The Universal Declaration of Human Rights was adopted on 10 December 1948 by Resolution 217 A of the Third Session of the United Nations General Assembly. An inspiring element is the very preamble of this Declaration: 'On 10 December 1948, the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights. Following this historic act, the General Assembly recommended that Member States should spare no means at their disposal to publish the text solemnly of the Declaration and 'to ensure that it is distributed, displayed, read and commented upon, mainly in schools and other educational institutions, irrespective of the political status of countries or territories'.

[26] The Convention on the Rights of the Child was adopted by the United Nations General Assembly on 20 November 1989. The Convention was also assumed by Romania through the adoption of Law no. 18/1990 for the ratification of the Convention on the Rights of the Child, the text of which was published in the Official Gazette no. 109/28 September 1990.

Convention)[27], which is only applicable if the state in question has ratified the Protocol relating to the Status of Refugees (1967)[28], in Article 4 of the Convention guarantees the religious freedom of refugees and specifically 'freedom as regards the religious education of their children'. In practical terms, Article 4 places no obligations on the state to provide religious education, *but rather allows refugee parents to refuse religious education* (either entire institutions or religious classes that form part of the curriculum in a given school) if it conflicts with their own, and to choose between existing alternatives, provided by either the state or private institutions[29].

The right to education and the obligation of children to participate in an education system are generally recognized with certain limits and specific conditions. In this context, we mention the rights of parents to educate their children according to their own religious, philosophical, or pedagogical beliefs. Specifically, this refers to homeschooling established in several legislations, whereby parents can educate their children at home under certain conditions and standards, as well as the right of parents to object on conscientious grounds to certain aspects of education, such as participation in certain school activities. The principle of the best interests of the child is unanimously recognised and is related to making decisions for the best interests and development of the child. In general, legislation and judicial practice seek to strike a balance between the rights of parents to exercise their authority and the right of the child to receive an appropriate education. It is appropriate to note that freedom of belief and choice of education in accordance with one's own beliefs is recognised as part of fundamental rights.

The analysis of relevant case law and legal precedents on the right to refuse education focuses on how courts have interpreted and applied existing law. Consideration of ancillary means such as case law and doctrine supports the identification of the most appropriate solutions. For example, courts can assess the effects (consequences) of refusing to allow education on the child's best interests, taking into account the child's emotional, social and intellectual development, and could also consider the role of the state in supervising and providing appropriate education, even in situations where parents refuse traditional education. It is desirable for case law to take account of cultural specificities and local traditions when considering the denial of education in the context of a particular group or community, weighing both protection and neglect.

In recent years, homeschooling has gained popularity among parents and has been associated with various reasons, including concerns about the traditional school environment, educational freedom and religious values, and authorities have begun to worry about setting standards and assessments to provide sufficient assurance that homeschooled children are receiving an appropriate

[27] Convention Relating to the Status of Refugees (adopted 28 July 1951, entered into force 22 April 1954) 189 UNTS 137 (Refugee Convention).
[28] Protocol relating to the Status of Refugees (adopted 31 January 1967, entered into force 4 October 1967) 606 UNTS 267.
[29] See more details in E Murphy and others, *Right to Education Handbook*, United Nations Educational, Scientific and Cultural Organization 2019 <https://unesdoc.unesco.org/ark:/48223/pf0000366556?posInSet=11&queryId=N-bcae0510-a577-400f-a25a-416432a4837f> accessed 08 February 2024.

education. The initiatives have not been without a degree of tension between the rights of parents to decide on their children's education and the state's obligation to protect the best interests of the child. Interestingly, the rise of access to educational resources and technology has highlighted some differences in access to educational resources and technology, as well as socio-economic differences in online education. The phenomenon has expanded during the pandemic in recent years, when online education became the norm. On this occasion, a series of issues regarding unequal access to educational resources and technology have come to light. These refusal options generally come with societal changes and are highlighted by differential treatment, discrimination, or other safety issues in schools. We can provide an example from the pandemic when sanitary measures such as mask-wearing and social distancing in schools elicited diverse reactions from parents and students. These attitudes had an immediate impact at the administrative level (in the respective institutions) and then at the level of specific policies and so on. In terms of similarities, the same issues almost always arise when discussing the protection of privacy, mental health, or protection against cyberattacks, meaning that lessons learned yesterday can be helpful in finding solutions today.

Discourses on the nature of education as a right or obligation have demonstrated how the right to refuse education is perceived and treated at the legislative and jurisprudential level, including at the constitutional level. As we discuss education, we can also discuss the internet. We refer here to benefits, common criticisms of human rights, how these categories of rights are regulated in international law, in international human rights instruments, United Nations core human rights treaties, United Nations: Declarations, UNESCO normative instruments, international labour law, international refugee law, international humanitarian law, international criminal law, and also the right to education in regional human rights law[30]. Like education, the right to refuse the internet can also be based on: aims of the internet, non-discrimination and equality including the equal right to the internet, special protections of the right to the internet of marginalized groups, women and girls, people with disabilities, refugees, migrants, and other displaced persons.

Note that this right is not limited to children; adults also have the right to make decisions about their own education. In a democratic society, individual autonomy and freedom of choice are fundamental values. Adults therefore have the right to decide whether they want to participate in educational programmes and how they want to shape their own learning paths. Key issues include the right to educational autonomy which allows adults to choose their own learning programmes, to take courses or to participate in educational activities according to their interests, needs and goals, especially with regard to the alternatives: self-study, mentoring, online courses or participation in community programmes, depending on their preferences. Therefore, adults decide not to participate in certain educational programmes or activities without facing negative consequences or discrimination.

[30] See some theoretical considerations in I Calderón-Almendros, G Echeita-Sarrionandia, 'Inclusive Education as a Human Rights' (2022) OUP 19-32 <https://doi.org/10.1093/acrefore/9780190264093.013.1243> accessed 15 February 2024.

Like the right not to use the internet, while the right to refuse education is recognised, this must be balanced with recognition of the importance of education in personal and societal development.

4. Parallels between the right not to use the internet and the right to refuse education.

From the presentations provided so far, certain affinities can be discerned, which can now be examined from various perspectives, as outlined such as the following. Both rights are based on the principle of individual freedom and autonomy, whereby individuals have the right to decide how they live and shape their own lives, including their choices about their online environment and education. In this place these connections converge to make the internet a valuable tool for education[31]. The internet allied with education suffers from similar ills such as insufficient literacy or poor access and understanding of the infosphere[32].

These refusals may be motivated by a desire to protect privacy or to express conscientious objection, such as avoiding excessive online exposure or refusing to participate in certain aspects of education. Refusal or limitation of internet use and refusal of education may be caused by concerns about the impact on mental health, as some individuals prefer to avoid digital addiction or the stress associated with online life or to distance themselves from the traditional education system. Both rights offer the choice of alternatives to traditional systems such as home education and independent learning, while limiting internet use means seeking other means of communication and information. States must have very clear regulations to protect them from accusations such as the refusal by a state to guarantee access to a school or the internet, which could constitute a violation of the right. One of these possible regulations is precisely the recognition of these two rights, under certain well-defined conditions.

On a comparable level, the trend towards self-development and personal learning is common, adapted to individual needs and preferences. All of these emphasise a responsible assessment of benefits and risks. The right to refuse both only further reflect the need to balance advantages and disadvantages in order to create a lifestyle or educational trajectory in line with personal values and goals.

The legal justifications for the right not to use the internet and the right to withhold education have certain similarities within the principles of individual rights, because at the individual level, a restriction of access to valuable information and opportunities for learning and growth, social and relational

[31] D Nevická, M Mesarčík, 'Why are you offline? The issue of digital consent and discrimination of Roma communities during the pandemic in Slovakia' (2022) 22(2) International Journal of Discrimination and the Law,172-91. <DOI: 10.1177/13582291221096615> accessed 15 February 2024. Also see G Kecső, B Szentgáli-Tóth, B Bor, 'Emergency Regulations Entailing a Special Case of Norm Collision Revisiting the Constitutional Review of Special Legal Order in the Wake of the COVID-19 Pandemic' (2024) 14(1) Juridical Tribune - Review of Comparative and International Law, 5-26.

[32] GM Greco, L Floridi, 'The tragedy of the digital commons' (2003) 6 Ethics and Information Technology 73-81.

isolation can be installed. We have previously outlined how on a social level, the consequences of denial of education and internet use have the potential to influence diversity and inclusion within society. A society that encourages and supports education and technology is more likely to innovate and progress, but sufficient room must also be left for adequate protections for the full manifestation of human rights. In contrast, denials can contribute to a lack of diversity and less economic competitiveness, affecting collective efficiency and community development. Choices of this kind can also bring social pressures and judgements from the community, and those who reject certain social norms may be viewed with scepticism or criticism, in addition to the chance of losing connection with the changes and opportunities that derive from technology, so that they are not just individual choices but have a wider impact on society as a whole. All unless new jobs emerge to improve or address these dysfunctions through their remit. The public interest is all the more justified as the careful balancing of society's discontent against the discontent of individuals can inhibit some civil opposition (riots, strikes, etc.). Personal decisions shape the trajectory of collective progress, and the balance between individual freedom and responsibility towards the community can challenge contemporary society. Among possible solutions, the relevant government authorities should consider the emergence of new professions to bridge these gaps.

Digital rights in general are about ensuring that all individuals have fair access to resources and information available online, while educational rights are about ensuring access to quality education for all[33]. Their developments influence each other.

5. Conclusions.

The legal reaffirmation of the importance of individual rights in the context of technological transformations is a natural process and is fundamental to building the best protection for modern human rights. On the one hand, individuals who choose these rights seek alternatives that correspond to their needs and preferences, thus reaffirming the importance of diversity in the process of personal formation and development. On the other hand, states are seeking to find appropriate solutions to new technological metamorphoses, as there is no room for waiting. This equation of individual freedom, however, is not without a subtle tension between personal autonomy and social responsibility. One of the threats underlying the right not to use the internet is increasing dependence on technology. Alongside marginalisation and social isolation, a new type of perpetuation of social and economic inequalities has emerged until solutions are found to adapt to digitalisation in learning, for example. The principle of good guards overcoming bad guards leads individuals to avoid exposure to false information or invasion of privacy, at the sacrifice of

[33] Digital rights are intended to stimulate the development of technologies that facilitate educational processes, such as virtual reality, artificial intelligence or online learning platforms.

exclusion from certain aspects of modern life if necessary. States, based on the same principle, seek the best solutions.

From a legal point of view, the right not to use the internet and the right to refuse education are dealt with in a heterogeneous way, depending on the case law conferred by the national law of the States. However, on the line of parallelism, some advantages or disadvantages can be identified at the jurisdictional level and some lessons can be learned more easily. The most exposed cases are those concerning: access to certain services and information conditional on internet use affecting access to essential public services, regulations on online monitoring and surveillance of communications, the fact that in many states a certain period of compulsory education is imposed, the refusal of which conflicts with these laws and parents or legal guardians may be subject to sanctions or fines, individual rights in the face of state intervention, opposition against excessive or abusive collection of information online, or recognition of freedom of conscience and religion.

In communi sensu, a number of ideas have already been put forward which could be taken into account to ensure a balance between individual rights and the interests of society. I refer here to the introduction and strengthening of data protection and online privacy laws so that those who choose not to use the internet are not exposed to the risks associated with the unauthorised collection of personal information. As alternative solutions, we can discuss the creation of mechanisms to ensure that people who do not use the internet have fair access to public services and information through alternative means, such as printed documents or other non-digital forms of communication. The recommendations are for legislation to formally recognise alternative forms of education, such as home learning or flexible learning models, provided they meet legal quality standards and ensure adequate development of learners. This requires evaluating and, if necessary, reforming the compulsory education system to take into account the diversity of learning modalities and individual needs, thus facilitating adaptability to different learning styles. This is where the role of states comes in, the creation of new jobs (the emergence of the internet trustee or intermediary, e.g.), institutions and regulations designed to protect individual rights without compromising the general interests of society. All this can be achieved at the macro, meso or micro level. The latter includes the introduction of compulsory digital literacy courses in the school curriculum, while respecting the right to refuse certain aspects of the online environment.

In the perspective of future research and action, a point-by-point analysis is needed providing a detailed look at each of the ways in which individual choices can shape the dynamics of communities and, why not, the dynamics of law. For the field of education, promoting flexible education policy is a vital direction. In parallel, investment in digital literacy and digital education programmes becomes a priority in promoting responsible and effective use of the internet. The parallelism we seek in this material is a step towards developing strategies to reduce disparities.

Madi R, 'Protecting Consumer Privacy Under Resolutions on Marketing Through Phone Calls in the UAE' (2024) 1 EJPLT, 194-204.
DOI: https://doi.org/10.57230/EJPLT241MR

EJPLT
ISSN 2704-8012



Protecting Consumer Privacy Under Resolutions on Marketing Through Phone Calls in the UAE

Protezione della Privacy dei Consumatori secondo le Risoluzioni sul Marketing tramite Chiamate Telefoniche negli Emirati Arabi Uniti

RAMZI MADI
Full Professor of Commercial Law and Intellectual Property Law
Deputy Dean of College of Law
Al Ain University

Abstract
The UAE telecommunications market is rapidly expanding, prompting the issuance of Resolution No. 56 of 2024, which regulates marketing phone calls, and Resolution No. 57 of 2024, which addresses penalties for violations. Both resolutions take effect in mid-August 2024. Resolution No. 56 defines telemarketing and distinguishes between "marketing" and "unwanted marketing" calls. It establishes guidelines for licensed telemarketing companies and procedures to protect consumers, enhancing privacy and fair practices. Resolution No. 57 outlines administrative penalties for violations. This paper reviews the regulatory framework for telemarketing in the UAE.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Il mercato delle telecomunicazioni negli Emirati Arabi Uniti è in rapida espansione, portando all'emissione della Risoluzione n. 56 del 2024, che regola le chiamate di marketing, e della Risoluzione n. 57 del 2024, che affronta le sanzioni per le violazioni. Entrambe entreranno in vigore a metà agosto 2024. La Risoluzione n. 56 definisce il telemarketing e distingue tra chiamate di marketing e indesiderate, stabilendo linee guida per le società di telemarketing autorizzate e procedure per proteggere i consumatori, migliorando la privacy e garantendo pratiche eque. La Risoluzione n. 57 delinea le sanzioni amministrative. Questo documento esamina il quadro normativo per il telemarketing negli Emirati Arabi Uniti.

Keywords: marketing phone calls; unwanted marketing phone calls; telemarketing; resolution; UAE.

Summary: 1. Introduction – 2. What is telemarketing? – 3. Commitments for licensed companies in the UAE conducting telemarketing – 4. Regulations for telemarketing – 5. Consumer protection – 5.1. General principles of the Federal Law No. (15) of 2020 on consumer protection – 5.2. Procedures to shield the consumer from unwanted marketing calls – 6. Administration penalties – 7. Conclusions

1. Introduction

Telecommunications market is growing very fast in UAE; The UAE Telecom Market is projected to be valued at USD 9.08 billion in 2023, with an anticipated growth to USD 10.60 billion by 2028, exhibiting a Compound Annual Growth Rate (CAGR) of 3.15% from 2023 to 2028.[1]

Telecommunications and digital government services are regulated in UAE by the Telecommunications and Digital Government Regulatory Authority (TDRA). This Authority was established in 2003 by Federal Law by Decree No. 3 of 2003 Regarding the Organization of Telecommunications Sector, as amended.

The duties and responsibilities of TDRA is "to oversee the telecommunications sector in the State and all Licensees in accordance with this Federal Law by Decree, its Executive Order and the instructions of the Board. The Authority may provide to the Board any necessary proposals in relation to the general policy of such sector and shall, at the end of each financial year, submit to the Board a report on its activities and business performance during that year".[2] Moreover, the Authority is responsible for handling the subscriber complaints and disputes.[3]

[1] Mordor Intelligence, *UAE Telecom Market Size* <https://www.mordorintelligence.com/industry-reports/analysis-of-the-telecom-sector-in-the-united-arab-emirates-industry/market-size> accessed 07 July 2024.
[2] Article 12 of Federal Law by Decree No. 3 of 2003 Regarding the Organization of Telecommunications Sector, as amended.
[3] See Article 14 (3) of Federal Law by Decree No. 3 of 2003 Regarding the Organization of Telecommunications Sector, as amended.

According to Article 2 of the resolution[4] No. 56 year 2024 regulating marketing through phone calls,[5] telemarketing of products and services is regulated to maintain economic and social stability. The resolution ensure that companies follow the specified channels and times for marketing their offerings and aim to reduce unwanted marketing calls, prioritizing consumers' comfort and privacy. The resolution will apply to all licensed companies in the UAE, including those operating in the free financial and non-financial zones,[6] and will take effect in mid-August 2024.[7] Additionally, the Ministry of Economy will supervise the implementation of this resolution. This will be done in coordination with the Central Bank of the UAE concerning marketing phone calls for banking services, establishments, other financial institutions, and insurance companies. The Securities and Commodities Authority will handle marketing phone calls related to securities and commodities trading services in the country. Local authorities in each emirate will also be involved, each within their respective jurisdictions.[8]

[4] To understand the importance of resolutions, it is necessary to clarify the key legislative types in the UAE.
Federal Constitution: Establishes the fundamental legal framework and governance structure.
Federal Laws: Govern strategic matters, requiring proposal by the Cabinet, review by the Federal National Council, and approval by the President and Supreme Council.
Decrees by Law: Issued between Supreme Council sessions for urgent matters, requiring subsequent Council approval.
Ordinary Decrees: Issued by the President, this occurs after receiving approval from the Cabinet and ratification by either the President of the State or the Supreme Council of the Union, each according to their jurisdiction. It must be published in the official gazette after being signed by the President of the State.
Cabinet Resolutions: They address issues that do not require a law or decree, guiding the functions of ministerial and federal government entities.
Ministerial Decisions and Circulars: Issued by the minister, the undersecretary, or the director general of the federal authority for implementing laws and regulations. For more details, you can view the UAE Ministry of State for Federal National Affairs website accessed at https://www.mfnca.gov.ae/ar/media/altamkin-newsletter-content/types-of-federal-legislation-and-procedures-for-enactment/.

[5] For a comprehensive review of the current literature on consumer privacy and telemarketing, see: N Sholehuddin, S Miskam, FM Shahwahid, TNRA Aziz, and N Mansor, 'A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries: Analisis Perundangan Perbandingan Undang-undang Perlindungan Data Peribadi di Negara-negara ASEAN' (2024) 7(1) Journal of Muwafaqat 23-38; D Wilding, K Lee, K Lindsay, and V Kathirgamalingham, 'The Enforcement of Telecommunications Consumer Protections' (2024) Centre for Media Transition, University of Technology Sydney, Report, pp. 1-94; GE Omelagah, JE Ekpang, BE Odey, NO Egere, and EU Ogri, 'Users' Perception of Telemarketing as a Direct Marketing Technique by Selected Mobile Telecoms Operators in Nigeria' (2024) 11(1) IJRAR 851-866; M Bakhtiarvand and SMH Ghabooli Dorafshan, 'The Approach of Legal Systems Toward Unsolicited Commercial Messages (SPAM)' (2024) 30(24) Encyclopedia of Economic Law Journal 63-78; S Krishnamurthy, 'Spam: A Consumer Perspective' in R Pappu (ed), Revolution in Marketing: Market Driving Changes: Proceedings of the 2006 Academy of Marketing Science (AMS) Annual Conference (Springer International Publishing 2015) 107-107; PO Jonsson, 'The Economics of Spam and the Context and Aftermath of the CAN-SPAM Act of 2003' (2009) 2(1) International Journal of Liability and Scientific Enquiry 40-52; S Tladi, 'The Regulation of Unsolicited Commercial Communications (SPAM): Is the Opt-Out Mechanism Effective?' (2008) 125(1) South African Law Journal 178-192; DW Khong, 'The Problem of Spam Law: A Comment on the Malaysian Communications and Multimedia Commission's Discussion Paper on Regulating Unsolicited Commercial Messages' (2004) 20(3) Computer Law & Security Review 206-212; MY Schaub, 'Unsolicited Email: Does Europe Allow Spam? The State of the Art of the European Legislation with Regard to Unsolicited Commercial Communications' (2002) 18(2) Computer Law & Security Review 99-105; S Krishnamurthy, 'Spam Revisited' (2002) 1(4) Quarterly Journal of Electronic Commerce 305-321.

[6] Article 3 (1) and article 1 of the Resolution No. 56 year 2024 Regulating Marketing Through Phone Calls. Article 1 of the Federal Law No. 8 of 2004 concerning Financial Free Zones defines "Financial Free Zone" as: "A free zone, that is established in any Emirate of the State, in which Financial Activities are carried out".

[7] Article 11 of the Resolution No. 56 year 2024 Regulating Marketing Through Phone Calls.

[8] Article 9 of the Resolution No. 56 year 2024 Regulating Marketing Through Phone Calls.

2. What is telemarketing?

Article 1 of the resolution distinguishes between “marketing phone calls” and “unwanted marketing phone calls”. It defines the former as calls made by a company or an individual to a consumer for the purpose of marketing, advertising, or promoting the products or services they offer, or on behalf of those who authorize them, using a fixed or mobile phone number. This includes marketing text messages and marketing messages through social media applications.

As for “unwanted marketing phone calls”, they are defined as marketing phone calls made in violation of the provisions of this resolution and do not include marketing phone calls made at the consumer’s request.

It should be noted that, in general, “calls” refers to voice calls. However, according to Article 1 of the resolution, telemarketing calls encompass both voice calls and text messages. The resolution includes marketing text messages and marketing messages through social media applications. Furthermore, the article covers both fixed and mobile phone numbers, whether the calls are initiated by the company or its employees.

There is no justification for broadening the definition of telemarketing calls to encompass marketing text messages and promotional messages sent via social media applications. Because, in addition to the resolution regulating marketing through phone calls, the TDRA issued a Mobile Spam Policy, which focuses specifically on marketing text messages rather than voice calls.

Article 1 of the Mobile Spam Policy differentiate between the “licensee’s own marketing text messages” and the “unsolicited electronic communications (spam)”.

Article 1 (9) of the Mobile Spam Policy defines “licensee’s own text messages marketing licensee’s own marketing text messages” as a “marketing text messages sent by a licensee to a mobile customer for marketing services provided by that licensee or its affiliate”. However, Article 1 (10) of the Mobile Spam Policy defines “unsolicited electronic communications (spam)” as “marketing electronic communications sent to a recipient without obtaining that Recipient’s Consent”.

The intent behind the marketing text messages should be to provide goods, services, or business opportunities; advertise goods, services, or business opportunities; solicit donations by charities; or serve any other purpose designated by the TRA. [9]

Moreover, the Mobile Spam Policy did not mention text messages sent by governmental entities and official organizations. However, it is covered by Article 1 (8) of the Policy; as it stated “or any other purpose designated by the TRA”.

Furthermore, the Mobile Spam Policy did not mention “political spam” which is used by candidates to promote their programs to reach the electorate. According to the Article 33 (14) of the Resolution No.25 of 2023 concerning the executive regulations of the 2023 Federal National Council (FNC) elections it is

[9] Article 1 (8) of Mobile Spam Policy.

not allowed to communicate with voters via using text messaging services or digital application messages of all kinds, provided by commercial companies.

Several countries, UK for example, allows Political advertising. Section 7.1 of the UK Code of Non-Broadcast Advertising and Direct & Promotional Marketing (CAP Code) states that: "Claims in marketing communications, whenever published or distributed, whose principal function is to influence voters in a local, regional, national or international election or referendum are exempt from the Code".

Furthermore, Article 1 of the resolution defines a "consumer" as a "natural person (individual)". This narrow definition contradicts Article 1 of Federal Law No. (15) of 2020 on Consumer Protection, which defines a "consumer" as: "Any natural or legal person obtaining a commodity or service for or without a fee to satisfy their own or another person's needs, or who is dealt with or contracted in this regard." Additionally, it is problematic that "marketing phone calls" and "unwanted marketing phone calls" are limited to natural persons, despite the reality that legal persons can also receive such calls.

3. Commitments for licensed companies in the UAE conducting telemarketing

Article 4 of the resolution outlines several commitments for licensed companies in the UAE conducting telemarketing. These include obtaining prior approval from the competent authority to engage in phone marketing, providing thorough training for the company's marketers on professional behavior and ethics in marketing calls, and the basics of using the Do Not Call Registry (DNCR). Marketers should only use local phone numbers issued by authorized telecommunications companies in the UAE and registered under the company's commercial license.

It should be noted that the UAE telecom providers Etisalat, Du, and Virgin Mobile offer the DNCR, a directory of phone numbers of consumers who do not wish to receive telemarketing calls. This directory has been in effect since September 2022. The UAE telecom providers explain how individuals can register and unregister their numbers with the DNCR, how to check if their number is registered in the DNCR, and how to file a complaint about unwanted marketing phone calls.

The process outlined by UAE telecom providers clearly explains how individuals can register and unregister their numbers with the DNCR, and how to file a complaint about unwanted marketing phone calls. However, the definition of "marketing phone calls" also includes marketing messages sent through social media applications. The current complaint forms are designed solely for local mobile, landline, or international numbers. There is no guidance on how individuals can raise a complaint regarding marketing messages received through social media applications, leaving this issue unaddressed.

Additionally, Article 4 of the resolution requires companies to provide a communication channel for consumers who want to receive marketing information, make marketing calls only to those consumers, and avoid calling consumers listed in the DNCR. Companies must keep a record of all marketing

phone calls using the form provided by the competent authority to ensure they have the minimum required data about their marketing activities and retain these records until the specified period ends.

Companies should also record marketing calls and notify the consumer at the beginning of the call that it is being recorded. Additionally, submit periodic reports as required by the competent authority, detailing all marketing calls made within the specified month after the report's due date. They should also sign a code of professional conduct according to the model prepared by the competent authority if deemed necessary to ensure ethical business practices in their marketing activities through phone calls.

Furthermore, companies should only make marketing phone calls between 9:00 AM and 6:00 PM. The caller should identify the company and the purpose of the call at the beginning of the marketing phone call. Companies have to tell where they got people's phone numbers and data if the authorities ask. They also cannot use phone numbers that are not registered or allowed for marketing calls.

4. Regulations for telemarketing

Article 5 of the resolution includes important rules. It bans the use of high-pressure sales tactics and requires that all information given about a product or service must be true and not misleading. Marketing phone calls should only be made between 9:00 AM and 6:00 PM, as mentioned earlier. If the consumer refuses the product or service during the first call, companies must not call them again. Additionally, if the consumer does not answer or ends the call, companies are limiting calls to only once a day and no more than two times a week.

The resolution allows companies to use automated dialing systems to market their products or services. It also requires companies to ask the consumer if they wish to proceed with the call before beginning any marketing or advertising. Companies must adhere to any other regulations issued by the Minister of Economy after coordination with the competent authority and relevant entities, as well as any additional regulations set by the competent authority.

It should be noted that the article specifies that marketing phone calls should only be made between 9:00 AM and 6:00 PM, without distinguishing between working days and off days. In the federal government sector, Saturdays and Sundays are the official weekends, and Fridays are considered a half-day. Additionally, the article does not prohibit marketing phone calls during holidays and public holidays.

Other jurisdiction such as South Africa, specifies the days, holidays and public holidays clearly. Clause 16.8. of the Wireless Application Service Providers' Association (WASPA) Code of Conduct, version 17.6, effective as of August 24, 2023, states: "Unless a consumer has expressly or implicitly requested or agreed otherwise, a member may not engage in any direct marketing directed to a consumer on:

(a) Sundays, public holidays contemplated in the Public Holidays Act, 1994;

(b) Saturdays before 09:00 and after 13:00; and
(c) all other days between the hours of 20:00 and 08:00 the following day.”.

5. Consumer protection

Consumer protection in the UAE is guided by Federal Law No. (15) of 2020, which establishes key principles to uphold consumer rights.[10] In addition to this, Resolution No. 25 of 2023 concerning the executive regulations of the Federal National Council (FNC) outlines procedures to protect consumers from unwanted marketing calls and ensure their privacy.

5.1. General principles of the Federal Law No. (15) of 2020 on consumer protection

The fundamental law protecting consumers in the United Arab Emirates is Federal Law No. (15) of 2020 on Consumer Protection. This law repeals Federal Law No. (24) of 2006.

Alongside the Federal Law, the legislator enacted Cabinet Resolution No. (66) of 2023 Concerning the Executive Regulations of Federal Law No. (15) of 2020 Concerning Consumer Protection, which brought forth the highly anticipated Executive Regulations for the Consumer Protection Federal Law. These regulations came into force in October 2023.

The significance of this law lies in the fact that most of the obligations and penalties outlined in the Consumer Protection Regime were absent in previous legislation. This underscores the UAE’s heightened emphasis on strengthening consumer rights and regulating fair trade practices.[11]

According to Article 2 of the law, its objectives are to safeguard all consumer rights, particularly the following:

1. Quality of Commodities and Services: Ensuring commodities and services are of high quality and available at the advertised price.

2. Health and Safety: Maintaining the health and safety of consumers when acquiring commodities or receiving services, without causing harm from their use.

3. Promoting Sound Consumption Patterns: Encouraging healthy and safe consumer habits.

According to Article 3, the law covers a wide scope[12] and applies not only to commodities and services within the country but also extends to free zones. It governs transactions involving suppliers, advertisers, or commercial agents, whether conducted traditionally or through electronic commerce, if the supplier is registered within the state. This is without prejudice to the treaties and international agreements to which the state is a party.

It is important to note the consumer rights outlined in Article 4 of the law,

[10] W Hussam Al-Din Al-Ahmad, *Explanation of the UAE Federal Consumer Protection Law* (Dar Al Hikma, 2023).
[11] I Shah and J Moussa, ‘Understanding the UAE’s Enhanced Consumer Protection Law’ (2024) Hogan Lovells, accessed at https://www.lexology.com/library/detail.aspx?g=a321eb0c-e620-4f7d-8067-3ada07d53374.
[12] A Lester, ‘Changes to the UAE Consumer Protection Law: What You Need to Know’ (2023) Clyde & Co, accessed at https://www.clydeco.com/en/insights/2023/10/changes-to-the-uae-consumer-protection-law-what-yo.

which include:

1. Safe Environment: The right to a suitable and safe environment when purchasing commodities or receiving services.
2. Accurate Information: The right to receive correct information about the commodities and services purchased, used, or consumed.
3. Education and Awareness: The right to be educated and informed about consumer rights and obligations.
4. Freedom of Choice: The right to choose the most suitable product and service available in the market according to personal preferences.
5. Privacy Protection: The right to privacy and security of personal data, ensuring it is not used for promotional and marketing purposes.
6. Safeguarding consumers' cultural and religious values: The right to have commodities and services provided in a manner that respects religious values, customs, and traditions.
7. Dispute Resolution: The right to fair and swift resolution of disputes.
8. Compensation: The right to fair compensation for damages to oneself or one's property due to the purchase, use, or receipt of commodities and services.
9. Additional Rights: Any other rights established by applicable legislation in the country.

It should be noted that various entities in the UAE are concerned with consumer protection, including the Ministry of Economy through the Supreme Committee for Consumer Protection and the Economic Development Departments in each emirate: Department of Economic Development – Abu Dhabi, Department of Economic Development – Dubai (Consumer Rights Site), Department of Economic Development – Sharjah, Department of Economic Development – Ajman, and Department of Economic Development – Umm Al Quwain. Additionally, the UAE Central Bank, Abu Dhabi Quality and Conformity Council, Abu Dhabi Agriculture and Food Safety Authority (ADAFSA), and the Emirates Society for Consumer Protection also play roles in this regard.

The law includes strict penalties in Articles 29 to 32, imposing imprisonment for up to two years and fines ranging from a minimum of AED 10,000 to a maximum of AED 2,000,000, or either of these penalties, for anyone violating certain legal provisions. Penalties may be doubled for repeat offenses.

In other cases, imprisonment of up to six months and fines ranging from AED 3,000 to AED 200,000, or either of these penalties, may apply, with doubled penalties for repeat offenses.

In addition to imprisonment and fines, the competent court may also order the confiscation or destruction of commodities, materials, and tools used, at the expense of the convicted person. It may also order the closure of the premises where the offense occurred for up to three months and publish the conviction in two local daily newspapers, one of which must be in Arabic, at the convicted person's expense.

If commodities and tools seized by the competent authority are disposed of unlawfully, the penalty is imprisonment for up to two months and a fine equal to twice the market value of the seized commodities and tools, or either of these penalties

5.2. Procedures to shield the consumer from unwanted marketing calls

Article 6 of the resolution specifies procedures to protect consumers from unwanted marketing calls. However, these procedures do not apply to marketing phone calls started upon the consumer's request. Consumers have the right to submit a complaint to the competent authority about unwanted marketing calls. The complaint should include the complainant's name, phone number, the respondent's name and phone number, and any supporting documents, if available. The competent authority will establish regulations and procedures for receiving and resolving complaints according to its practices and may investigate and inquire about unwanted marketing phone calls.

The resolution emphasizes the prohibition of disclosing the consumer's personal data[13] without obtaining their permission or selling it to companies that intend to use it for marketing their products or services through telemarketing calls. Additionally, consumers have the right to register in the DNCR to stop receiving marketing phone calls and to file complaints about them, in accordance with the prevailing legislation and procedures.

6. Administration penalties

Article 3 of the resolution No. 57 of 2024 regarding violations and administrative penalties for actions that occurred in violation of the provisions of Resolution No. 56 of 2024 distinguishes between the administrative penalties imposed by the competent authorities on companies and the penalties imposed by the TDRA on individuals, as well as the administrative penalties imposed by the Central Bank of the UAE on companies and individuals, as stated in article 3 of the resolution.

When it comes to the administrative penalties imposed by the authorities on companies, the competent authority can impose one or more penalties for any actions committed by the companies. The resolution outlines a range of penalties starting with a warning, followed by an administrative fine (according to table No. 1 attached to the resolution),[14] suspension of activity (partially or fully) for a period of 7 to 90 days, license cancellation, removal from the commercial register, disconnection of telecommunications services, and removal of the phone number. Additionally, the administrative decision that imposes the penalty specifies the time frame for the company to fix or remove

[13] Article 1 of the Federal Decree by Law No. 45 of 2021 Concerning the Protection of Personal Data defines "Personal Data" as : "Any data related to a specific natural person or related to a natural person that can be identified directly or indirectly by linking the data, through the use of identification elements such as his/her name, voice, image, identification number, his/her electronic identifier, his/her geographical location, or by one or more physical, physiological, economic, cultural or social characteristics. It includes Sensitive Personal Data and Biometric Data."

[14] The resolution lists 18 types of violations and penalties for companies that break the rules. These include not getting approval from the authorities for phone marketing, with fines of AED 75,000 for the first time, AED 100,000 for the second, and AED 150,000 for the third. There is also a fine of up to AED 150,000 for marketing to consumers on the DNCR, and a fine of up to AED 75,000 for marketers who do not use local phone numbers from authorized telecom companies in the UAE. Additionally, there are fines from AED 25,000 to AED 75,000 for deception and misleading consumers during phone marketing, and other fines ranging from AED 10,000 to AED 150,000 for any other violations of these resolutions.

the violation. If the company fails to do so, the decision also specifies the penalty to be applied, following the previously mentioned gradation. The competent authority may skip the step-by-step penalties and directly impose the most severe penalty if the company repeats the same violation within 6 months of the previous penalty.

Regarding the penalties imposed by the TDRA on individuals, the TDRA, along with authorized telecommunications companies in the country, can impose one or more penalties on a person who makes marketing phone calls that break the rules of the resolution. These penalties are listed in table no. 2 attached to the resolution.[15]

TDRA, along with authorized telecommunications companies, can skip the step-by-step penalties listed in table no. 2 of the resolution and directly impose the most severe penalty if the individual repeats the same violation for the third time.

The Central Bank of the UAE sets out a list of violations and administrative penalties imposed on companies and individuals that violate the resolution, after obtaining the approval of the Cabinet. Consequently, it is noted that the resolution did not include any attached table for these penalties, unlike the administrative penalties imposed by the competent authorities on companies and the penalties imposed by the TDRA on individuals. The resolution also did not address any gradation of penalties, nor the imposition of the most severe penalty in case of repetition, leaving the organization of this matter to the regulation.

It should be noted that the Cabinet has the right to modify the aforementioned fines, whether by addition, deletion, or amendment.[16]

It is important to note that these administrative penalties are not final, as any person with an interest in the matter has the right to appeal. The appeal can be submitted either in writing or electronically to the head of the competent authority or the head of the commission within 15 days from the date of notification of the administrative penalty being appealed. When submitting the appeal, all supporting documents and evidence must be attached. The appeal will be reviewed within 30 days from the date of submission. If there is no response from the receiving authority, the lack of response is considered a rejection. The authority must inform the appellant of the decision and the reasons for the rejection, whether explicitly or implicitly. This process does not apply to the Central Bank of the UAE, which sets its own procedures for appeals.[17]

[15] If an individual makes marketing phone calls for products or services using a landline or mobile phone number licensed in their name, they will be fined AED 5,000 and all their phone numbers will be disconnected until the fine is paid. If they commit the same violation within 30 days, the fine increases to AED 20,000, and their phone numbers will be disconnected for three months. If they repeat the violation again within 30 days of the second penalty, they will be fined AED 50,000 and banned from getting any services from licensed telecommunications companies in the country for 12 months.

[16] Article 4 of the resolution No. 57 of 2024 regarding violations and administrative penalties for actions that occurred in violation of the provisions of Resolution No. 56 of 2024.

[17] Article 6 of the resolution No. 57 of 2024 regarding violations and administrative penalties for actions that occurred in violation of the provisions of Resolution No. 56 of 2024.

7. Conclusions

The resolution makes a clear distinction between “marketing phone calls” and “unwanted marketing phone calls,” with “calls” generally referring to voice calls. However, according to Article 1, telemarketing calls also include text messages and marketing messages via social media applications, covering both fixed and mobile numbers. There is an unnecessary expansion of the definition of telemarketing calls to include text and social media messages, given the TDRA’s Mobile Spam Policy already regulates marketing text messages specifically.

The Mobile Spam Policy excludes text messages from governmental entities but is addressed in Article 1(8) of the Policy, and it does not cover “political spam” used by candidates, which is restricted under Article 33(14) of Resolution No. 25 of 2023 for FNC elections.

Article 1 of the resolution narrowly defines a “consumer” as an individual, conflicting with Federal Law No. 15 of 2020, which includes both natural and legal persons. This limitation is problematic as legal persons also receive marketing calls.

The UAE’s DNCR process guides individuals on registering and unregistering numbers and filing complaints about unwanted calls but lacks guidance on complaints regarding marketing messages through social media. Additionally, marketing phone calls are allowed between 9:00 AM and 6:00 PM without distinguishing between working days and holidays, unlike jurisdictions, which clearly specifies permissible days and times for marketing calls.

Eventually, the resolution No. 57 of 2024, which deals with violations and administrative penalties for actions against the rules of Resolution No. 56 of 2024, mentions strict administrative penalties. It also gives the Central Bank of the UAE the authority to create a list of violations and penalties for companies and individuals who break the rules, after getting approval from the Cabinet.

Santoni G, 'Un approccio comparatistico all'interpretazione degli obblighi dei gatekeepers nel Digital Markets Act' (2024) 1 EJPLT, 205-218.
DOI: https://doi.org/10.57230/EJPLT241GS

EJPLT
ISSN 2704-8012



Un approccio comparatistico all'interpretazione degli obblighi dei gatekeepers nel Digital Markets Act

A comparative approach to the interpretation of gatekeepers' obligations in the Digital Markets Act

GIULIO SANTONI
Dottore di ricerca, Università degli Studi Roma Tor Vergata

Abstract
L'articolo analizza gli obblighi dei gatekeepers come definiti nel Digital Markets Act. Particolare attenzione è prestata all'influenza dei vari ordinamenti europei, precisamente di quello tedesco, nell'evoluzione della materia. La nutrita schiera di obblighi che il DMA impone ai gatekeepers è suddivisa in due macrocategorie al fine di razionalizzarne la trattazione. Così da un lato si descrivono i profili anticoncorrenziali collegati al controllo dei dati personali da parte dei gatekeepers e, dall'altro si riuniscono quelli riconducibili ad'idea di neutralità della piattaforma. Per definire quest'ultimo ambito, si attinge nuovamente ad una metodologia comparativa, anche fuoriuscendo dagli schemi del diritto europeo, per meglio definire il concetto di neutralità della piattaforma.

This article analyses the obligations of gatekeepers as defined in the Digital Markets Act. Particular attention is paid to the influence of the various European legal systems, especially the German one,, in the evolution of the subject matter. The extensive array of obligations that the DMA imposes on gatekeepers is subdivided into two macro-categories to rationalize their conceptualization. Thus, on the one hand, the anti-competitive profiles connected to the control of personal data by gatekeepers and those related to the idea of platform neutrality are described. In the latter area, a comparative methodology is once again drawn upon, even outside the framework of European law, to better define the concept of platform neutrality.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: digital markets act; gatekeepers; platform neutrality; comparative law.

Summary: 1. Premesse metodologiche. – 2. Obblighi che hanno ad oggetto il particolare vantaggio competitivo collegato al controllo di dati personali da parte del gatekeeper. – 3. Obblighi riconducibili all'espansione del concetto di neutralità della rete all'idea di neutralità della piattaforma. – 4. Neutralità della rete su più livelli: spunti comparativi. – 5. Dei limiti applicativi concreti.

1. Premesse metodologiche.

Gli obblighi dei *gatekeepers* sono enumerati agli artt. 5, 6 e 7 del Regolamento UE 2022/1925 "relativo a mercati equi e contendibili nel settore digitale", noto come *Digital Markets Act* (DMA) [1]. Nel prevedere misure che di fatto limitano la libera iniziativa economica dei *gatekeepers*, il legislatore europeo si serve di un lungo elenco, che contiene oltre 20 obblighi diversi, senza tenere conto degli obblighi accessori all'applicazione di tali obblighi principali. Questo non facilita l'organizzazione di una trattazione delle norme in esame. La tentazione di descrivere ogni obbligo in dettaglio deve essere respinta, perché rischierebbe di svilire il lavoro in un mero approfondimento dell'elenco offerto dal legislatore europeo. Il primo sforzo che l'interprete deve allora affrontare è di raggruppare gli obblighi in categorie di obblighi simili o funzionalmente collegati, legandoli eventualmente ad obblighi preesistenti, in particolare quelli derivanti dall' art. 102 TFUE, dal GDPR e dal meno noto Regolamento 2019/1150, cosiddetto Platform-to-business ("P2B").

Prima di avviare la trattazione, occorre svolgere alcune premesse di carattere metodologico e terminologico. Quanto alle prime, il DMA prevede degli obblighi di condotta ulteriori rispetto a quelli elencati agli art. 5, 6, e 7, rubricati con la dicitura "obblighi dei g*atekeepers"*. Ad esempio, l'art. 14 impone ai *gatekeepers* ad informare la Commissione degli eventuali progetti di concentrazione ai sensi della normativa euro-unitaria vigente in materia, mentre l'art. 15 impone al soggetto designato come *gatekeeper* di trasmettere, entro sei mesi, una descrizione sottoposta ad audit indipendente delle tecniche di profilazione dei consumatori applicate dal *gatekeeper* ai suoi *core platform services*. Si tratta di obblighi strumentali a garantire l'efficace applicazione degli obblighi primari, quelli previsti dagli artt. 5, 6 e 7, che si caratterizzano invece per essere in larga parte obblighi *ex ante,* che tengono conto di profili specifici del mercato digitale e che si applicano al *gatekeeper* in quanto tale e, pertanto, a prescindere dall'esistenza di un abuso di posizione dominante[2]. È opportuno

[1] Sui limiti dei tradizionali strumenti di analisi dei mercati, che hanno portato l'UE ad adottare una normativa ad hoc, si v. M. LIBERTINI, *Digital Markets and the competition policy. Some remarks on the suitability of the antitrust toolkit, in Rivista Orizzonti del Diritto Commerciale*, 2021, 339 e G. Ferrari, M. Maggiolino, Il potere across markets delle GAFAM: come reagire? In *Rivista Orizzonti del Diritto Commerciale*, 469.

[2] v. in questo senso A. IANNOTTI DELLA VALLE, *Il Digital Markets Act e il ruolo dell'Unione Europea verso un costituzionalismo digitale*, in *Giurisprudenza Costituzionale*, 2022, 1873 – 1874. Cfr. anche con S. SCALZINI, *Dipendenza economica e regolazione «asimmetrica» dell'attività d'impresa. Prime osservazioni sul novellato art. 9 l. n. 192/1998*, in *Analisi Giuridica dell'Economia, Studi e discussioni sul diritto dell'impresa* 2/2022, 570 e A.

spendere altresì qualche parola sull'utilità di un approccio comparatistico. Non solo, come si vedrà a breve è dal confronto con il diritto statunitense che emergono le insidie insite nella nozione stessa di *gatekeeper*. La stessa formulazione di alcuni degli obblighi di cui al Digital Markets Act attinge all'esperienza maturata nei diversi ordinamenti nazionali europei ed, in particolare, alle decisioni del *Bundeskartellamt*, che molto hanno attirato l'attenzione della dottrina, anche italiana (v. *infra*) [3].

L'altra premessa, di carattere terminologico, riguarda l'utilizzo che nel DMA viene fatto del termine *gatekeeepers*, mantenuto in inglese anche nella versione italiana del regolamento. Il concetto di *gatekeeper* è infatti stato utilizzato in dottrina, in particolare negli Stati Uniti, fin dagli anni 80, per definire il soggetto privato che, offrendo sul mercato un servizio potenzialmente utilizzabile per la realizzazione di illeciti, può essere coinvolto dall'autorità, allo scopo di regolare il mercato o un soggetto che si trovi altrimenti in una posizione di garanzia [4]. L' esempio classico di *gatekeeper*, nell'accezione qui riportata, sono gli intermediari finanziari, assoggettati ad obblighi di informazione particolari, allo scopo di rafforzare la sicurezza del mercato finanziario. Il concetto è stato riadattato al tema della responsabilità dei prestatori di servizi in rete, detta anche *gatekeeper liability*[5]. La materia della *gatekeeper liability* è stata accolta nel diritto europeo attraverso la direttiva 2000/31, in parte ispirata dal Digital Millennium Copyright Act statunitense ed ora sfociata nel provvedimento gemello al *Digital Markets Act,* il Regolamento 2022/2065, o *Digital Services Act* [6]. Trattasi pertanto di un'ipotesi particolare di responsabilità aquiliana, concettualmente distinta dal tema di diritto della concorrenza affrontato dalla disciplina contenuta nel Digital Markets Act, rubricata "obblighi dei *gatekeepers*" (in inglese, *gatekeepers' obligations*). È doveroso aggiungere che questo nuovo utilizzo del termine trova una corrispondenza anche nel diritto statunitense, dove appare nel c.d. Open App Markets Act.

Dato il gran numero di obblighi che il DMA prevede, allo scopo di facilitare la trattazione e di evitare di limitarsi a riprodurre l'elenco contenuto nel DMA, si suddividono gli obblighi in due macrocategorie: a) obblighi che hanno ad oggetto il particolare vantaggio competitivo collegato al controllo di dati da parte del *gatekeeper*; b) obblighi riconducibili all'espansione del concetto di neutralità della rete all'idea di neutralità della piattaforma.

MANGANELLI, *Il regolamento per i mercati digitali: ratio, criticità e prospettive di evoluzione*, in *Mercato Concorrenza Regole*, 2021, p. 484, i quali sottolineano altresì l'asimmetricità degli obblighi imposti dal DMA, nel senso che non si applicano in seguito o a causa di un abuso di posizione dominante, ma al *gatekeeper* in quanto tale.

[3] Non meno rilevante l'attività dell'autorità per la concorrenza italiana, sulla quale, tuttavia, non si è arrivati a pronunce della CGUE. Si v. C. CALINI, E. IOSSA, *Multiplicity of Tools for Antitrust and Consumer Protection in Digital Markets: the Italian Experience and the Road Ahead*, in European Competition Journal, 2023, disponibile anche presso https://drive.google.com/file/d/16lfcgvnn04VKJ3n52eHZUf5m31Tr8PpH/view.

[4] Si v., su tutti, R.KRAAKMAN,, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy* in *The Journal of Law, Economics, and Organization,* 1986.

[5] v. ad es., tra i primi, , A. HAMDANI, *Gatekeeper liability*, in *South California Law Review*, 2004.

[6] Sul problema della sovrapposizione di alcuni profili dei due regolamenti europei, v. G.M. RUOTOLO, *Digital Services Act e Digital Markets Act tra responsabilità dei fornitori e rischi di bis in idem*, in S*idiblog*, 2021, passim.

2. Obblighi che hanno ad oggetto il particolare vantaggio competitivo collegato al controllo di dati personali da parte del gatekeeper.

Rientrano nella categoria qui trattata gli obblighi di cui all'art. 5, c. 2, 5, c. 9, 5 c. 10 e 6, c. 2, 6, c. 8 e, 6, c. 9, 6, c. 10[7], che si incardinano sul diffuso meccanismo economico che vede numerosi *gatekeepers* offrire servizi apparentemente gratuiti a persone fisiche, che in cambio acconsentono al trattamento dei dati personali da parte del *gatekeeper* stesso[8]. L'immensa mole di dati personali raccolti dai *gatekeeper* assicura un incremento esponenziale dell'efficienza dei processi di profilazione delle preferenze degli utenti, che si traduce in un vantaggio concorrenziale in termini di accuratezza dei sistemi di raccomandazione[9].

Un tema che le Autorità della concorrenza e la Corte di Giustizia Europea hanno già affrontato riguarda il vantaggio concorrenziale che i servizi il *gatekeeper* trae incrociando e combinando i dati raccolti attraverso diversi servizi[10]. Per superare il rischio per il mercato comportato dall'incrocio e dalla combinazione di dati personali da parte di Facebook, il *Bundeskartellamt* tedesco ha utilizzato strumenti propri del diritto alla protezione dei dati personali[11]. Ha sanzionato l'azienda poiché riuniva gli account relativi a servizi diversi (Facebook, Instagram, Oculus, Whatsapp, Masquerade), così inducendo gli utenti a prestare un consenso orizzontale al trattamento dei dati personali. Era contestato, in altre parole, che la riunione degli account relativi a diversi servizi non fosse necessaria ad esigenze legate ad un'ottimale fornitura dei servizi, bensì a fondare giuridicamente la condivisione di dati tra servizi diversi, riferibili alla stessa realtà aziendale, così violando il principio di limitazione del trattamento di cui all'art. 5 del GDPR[12].

Non sorprende allora che l'elenco di obblighi previsto dal DMA si apra, all'art. 5, c.2, con un quartetto di divieti che dovrebbero limitare la possibilità del *gatekeeper* di avvantaggiare i propri servizi secondari con i dati raccolti attraverso il servizio di piattaforma di base alle ipotesi in cui l'utente finale abbia prestato consenso "granulare" ed espresso al trattamento[13]. E così, il *gatekeeper* non può utilizzare i dati personali, quindi i dati identificativi di persone fisiche, provenienti dall'uso fatto di servizi commerciali che operano

---

[7] Laddove ai fini del DMA si intende per dato "qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva" (art. 2, c. 24 del DMA). Che il controllo di grandi quantità di dati rappresenti di fatto un fondamentale vantaggio per i *gatekeepers* è evidenziato dal fatto che il considerando 3 del DMA cita "l'accesso a grandi quantità di dati" come il primo dei fattori cruciali che consentono al *gatekeeper* di trasferire i vantaggi acquisiti attraverso una determinata attività in un altro settore

[8] Si vedano, su tutti, gli scritti di V.Ricciuto, e, in particolare, *L'equivoco della privacy*, 2022, 101 e ss.

[9] Cfr. A. Manganelli, *op. cit.*, 479.

[10] Decisione no B6-22/16 del 6 febbraio 2019. Per una comparazione di carattere generale e critico tra l'approccio del Bundeskartellamt e quella dell'AGCM, si rinvia a G. Olivieri, *Sulle relazioni pericolose tra antitrust e privacy*, in *Orizzonti di diritto commerciale*, 2021, 365.

[11] Come correttamente osservato in G. Buttarelli, *This is not an article on data protection and competition law,* in *Competition Policy International*, 2019, 3.

[12] La questione è stata successivamente portata alla Corte di Giustizia Europea (causa C-252/2021), che ha sostanzialmente confermato la lettura del BKA v. *amplius*, E. Prosperetti, D. Tuzzolino, *Abuso di dati personali? La Corte di Giustizia ammette il sindacato antitrust sul trattamento dei dati personali,* in *Diritto di Internet*, 2023, 643.

[13] Sul tema del consenso granulare, si è soffermato in dettaglio l'European Data Protection Board, nelle linee guida 05/2020 sul consenso ai sensi del GDPR, nonché E. Prosperetti, D. Tuzzolino, *op. cit.*, 643.

sul servizio di piattaforma di base per fornire pubblicità online (lett. a)); non può combinare i dati personali degli utenti del proprio servizio di piattaforma di base con i dati provenienti da altri servizi forniti dal *gatekeeper* (lett. b))*;* non può utilizzare in modo incrociato i dati personali provenienti dal servizio di piattaforma di base in altri servizi forniti separatamente dal *gatekeeper* e viceversa (lett. c)); e, infine, non può costringere gli utenti finali del suo servizio di piattaforma di base a registrarsi ad altri servizi del *gatekeeper* (lett. d)).

Quest'ultimo aspetto riporta al cosiddetto *bundling of consent* che è già stato al centro della già citata decisione del *Bundeskartellamt* del 2019 e che nella prassi è frequentemente collegato alle operazioni di cui alla lett. b)) dell'elenco di cui all'art. 5, comma 2. Il fatto che il mercato delle informazioni favorisca le economie di scala, vale a dire il confluire dei consumatori verso i medesimi servizi, fa sì che in alcuni casi possa essere particolarmente difficile per i consumatori rinunciare ad utilizzare un particolare servizio[14]. Pertanto, la lett. d) dell'art. 5, comma 2, ha la funzione di impedire che il costo opportunità che il mancato utilizzo di un *core platform service* di un importante *gatekeeper* (si pensi ad esempio al *core plaform service* Google Search del *gatekeeper* Alphabet) porti il consumatore a registrarsi in blocco a tutti i servizi del *gatekeeper* attraverso un account unico.

L'art. 5 comma 2 del DMA lambisce il vantaggio competitivo dei *gatekeepers*, dato dal combinare ed incrociare i dati personali dei propri utenti, ma non lo intacca in modo significativo. La previsione non vieta in toto le condotte elencate, ma le condiziona a requisiti di specificità e granularità del consenso e, pertanto, si pone in linea di continuità con un orientamento seguito sia dalle Autorità sulla concorrenza, su tutte il *Bundeskartellamt*, sia dalla Corte di Giustizia dell'Unione Europea. E con riferimento a tale orientamento, la difficoltà di "disarticolare" servizi complessi come quelli offerti dalle grandi piattaforme, per così isolare i trattamenti essenziali da quelli accessori, è stata già osservata in dottrina[15]. Ma il problema non si limita ad un tema di validità del consenso prestato dal soggetto interessato dal trattamento: nella prospettiva della tutela del mercato, il fatto che una condotta anticoncorrenziale, o comunque lesiva per il mercato, sia fondata su un consenso valido o meno, in realtà, è irrilevante. Suggestiva dottrina ha argomentato l'insufficienza degli strumenti di diritto della concorrenza tradizionale e di tutela dei dati personali ad arginare i fallimenti di mercato causati dalle piattaforme online di grandi dimensioni [16]. I consumatori difficilmente riescono ad evitare di utilizzare i servizi delle grandi piattaforme e questo consente alle grandi piattaforme online di far accettare agli utenti delle condizioni contrattuali particolarmente svantaggiose in termini di tutela dei dati personali [17]. Secondo l'orientamento riportato, ciò permette alle

[14] W. KERBER, K. K. ZOLNA, *The German Facebook case: the law and economics of the relationship between competition and data protection law*, in *European Journal of Law and Economics*, 2022, 224.
[15] E. PROSPERETTI, D. TUZZOLINO, *op. cit.*, 646.
[16] v., su tutti, W. KERBER, K. K. ZOLNA, *op. cit.*, 219.
[17] Cfr., nuovamente, con W. KERBER, K. K. ZOLNA, *op. cit.*, 225 Il riferimento riguarda, in particolare, il diritto alla portabilità dei dati del GDPR, che, per via della difficoltà tecnica di esportare i dati da un servizio all'altro, non ha avuto un impatto decisivo. v. *amplius*, sul tema, C. CARLI, *Accesso ai dati tra GDPR, tutela della concorrenza e DMA: un gioco di specchi?*, in *Mercato Concorrenza Regole*, 2022, 642, che sottolinea correttamente come un importante limite del diritto alla portabilità sia la mancata previsione di un diritto in capo al terzo di ottenere l'interoperabilità del dato.

piattaforme di rafforzare ulteriormente il proprio dominio nei mercati dei dati e, di contro, di proporre ai propri utenti condizioni contrattuali ancora più svantaggiose[18]. Il fatto che l'art. 5 comma 2 consenta al *gatekeeper* di superare i divieti raccogliendo il consenso dell'interessato ha l'indubbio pregio di coordinare la normativa in tema di tutela della concorrenza con il principio di libera circolazione dei dati personali previsto dal GDPR. Allo stesso tempo, comporta l'assorbimento nel diritto della concorrenza della contraddizione che si è appena descritta: l'applicabilità dei divieti può essere superata con il consenso di un soggetto, il consumatore/ interessato dal trattamento dei dati personali, che ha un margine di manovra estremamente ristretto nei confronti del *gatekeeper*. L'armonia del sistema è ulteriormente turbata dal fatto che il consumatore non è portatore dell'interesse pubblico alla concorrenza sul mercato, bensì del suo interesse, individuale e immediato, ad ottenere il servizio in rete nel momento in cui ne ha bisogno, il che rischia di indebolire eccessivamente tutele del mercato fondate sul consenso del soggetto del trattamento[19].

I successivi commi 9 e 10 dell'art. 5 obbligano il *gatekeeper* a fornire ai suoi inserzionisti informazioni utili a valutare l'impatto dell'inserto pubblicitario, in questo modo appianando il deficit informativo che caratterizza i rapporti contrattuali che intercorrono tra questi soggetti. I commi 8, 9, e 10 dell'art. 6, impongono invece vari obblighi volti a rendere effettivo l'accesso dei soggetti terzi ai dati raccolti dai gatekeeper.

Il comma 2 dell'art. 6, prevede invece una situazione speculare, perché vieta al *gatekeeper* di utilizzare le informazioni raccolte attraverso le operazioni dei propri utenti commerciali concorrenti, allo scopo di competere con essi (c.d. *sherlocking*) [20]. Solo nel caso in cui i servizi di piattaforma di base coinvolti siano servizi di intermediazione online (ad esempio siti di e-commerce) tale divieto si lega alle previsioni di cui all'art. 9 del Regolamento P2B, che impone a tali fornitori di servizi di chiarire, nei propri termini e condizioni, quali siano le modalità di accesso ai dati generati dagli utenti commerciali (i negozi virtuali nel sito di e-commerce). Ciò anticipa in parte lo stretto legame funzionale che intercorre tra gli obblighi di trasparenza di cui al Regolamento P2B e le previsioni del DMA (v. *infra*, sub par. 3, lett. b)).

3. Obblighi riconducibili all'espansione del concetto di neutralità della rete all'idea di neutralità della piattaforma.

Il DMA individua il *gatekeeper* da un punto di vista funzionale, in quanto esso è il soggetto in grado di operare come un portiere sito all'ingresso del mercato

[18] Cfr. con W. KERBER, K. K. ZOLNA, *op. cit.*, 225, i quali concludono la loro analisi osservando che l'inefficacia dei rimedi tradizionali nel settore dell'economia digitale è aggravata dal fatto che l'utilizzo di strumenti a tutela del mercato, come potrebbero essere ad esempio obblighi in capo alle piattaforme di condividere alcuni dati con i propri concorrenti possono avere effetti negativi sugli obiettivi perseguiti dalla normativa in materia di tutela dei dati personali.
[19] Cfr. con M. BETZU, *I poteri privati nella società digitale: oligopoli e antitrust*, in *Diritto pubblico*, 2021, 751-753.
[20] Cfr. con S. SCALZINI, *op. cit.*, 570.

delle informazioni[21]. Il concetto si impernia sulla vitale importanza del ruolo di alcuni fornitori di servizi in rete nel contesto dell'economia di rete. Quando raggiunge una certa massa critica, il fornitore di cosiddetti servizi di piattaforma di base, o *core platform services*, diventa un collo di bottiglia dell'informazione che, in quanto tale, deve essere regolato. A prescindere dalle loro dimensioni e dalla rilevanza sul mercato, non tutti i servizi online possono essere soggetti all'applicazione della normativa in esame, ma solo i cosiddetti servizi di piattaforma di base. Questi non sono oggetto di una definizione di carattere generale, poiché l'art. 2 comma 2 del Regolamento 2022/1925 elenca dieci tipologie di servizi che costituiscono *core platform services*, che spaziano dai motori di ricerca ai servizi di comunicazione interpersonale indipendenti dal numero, ai *browser web,* ai *social netroweks,* ai servizi di cloud, ecc. Si tratta di servizi disomogenei, accomunati non dall'oggetto delle prestazioni svolte, ma dal fatto che il soggetto che li fornisce può incidere sulla frequenza con cui gli utenti vengono a contatto con servizi offerti da soggetti terzi [22]. Una trattazione dettagliata di tutte le previsioni applicabili ai *gatekeepers* rischierebbe di fuoriuscire dal raggio di questo breve scritto. Giova in ogni caso ricordare che il DMA si concentra (a) in particolar modo sulla posizione degli app store; (b) sui servizi di intermediazione in rete; (c) sull'interoperabilità dei servizi di messaggistica[23].

a) Obblighi relativi agli app stores

Il DMA prevede obblighi collegati alla particolare posizione degli app store e dei gestori di sistemi operativi (artt. 6, c. 3, 6, c. 4, 6, c. 6, c. 12), che si caratterizzano per il fatto di essere applicabili ad una specifica categoria di servizi di piattaforma di base, gli *app store*[24]. Con essi, in quanto ispirato alla medesima *ratio*, può essere raggruppato anche l'art. 6, c. 7 che non si applica ai fornitori di app store, ma a fornitori di software e hardware necessari per il funzionamento di servizi terzi, cui è imposto un obbligo di garantire l'effettiva interoperabilità tra le componenti hardware e software fornite e componenti software e hardware fornite da soggetti terzi. La previsione è volta ad impedire al *gatekeeper* di favorire i propri servizi verticalmente integrati, ostacolando o

---

[21] Nell'espressione inglese *gatekeeper,* immediato è il riferimento biblico a Cronache, 9: 23-33, dove i *gatekeepers* sono i guardiani del Tempio di Dio:
"The gatekeepers and their descendants had to guard the gates of the Temple of the Lord. ...
There were gatekeepers on all four sides of the Temple: east, west, north, and south.
The gatekeepers' relatives who lived in the villages had to come and help them at times".

[22] Qualche chiarimento in merito è offerto dalla lettura congiunta dei considerando 2 e 5 del DMA, che, pur limitandosi ad esemplificare gli elementi che rendono un servizio in rete un servizio di piattaforma di base, evidenziano che si tratta di servizi che possiedono caratteristiche intrinseche che possono essere sfruttate dal fornitore del servizio, in modo tale da compromettere la contendibilità dei mercati e caratterizzati dal fatto che gli strumenti tradizionali di tutela della concorrenza sono esplicitamente ritenuti inadeguati.

[23] Ne consegue che occorre inoltre fare i conti con un gran numero di regolamenti settoriali applicabili alle singole tipologie di servizi inclusi nell'elenco. Così i fornitori di servizi di motore di ricerca (art. 2, c.2, lett. a) del Regolamento) devono confrontarsi con la complessa disciplina del Regolamento 2019/1150, i social networks con la disciplina in materia di piattaforme di cui al *Digital Services Act*, e così via. Peraltro, i regolamenti appena citati non sono a loro volta che il perno attorno al quale ruotano ulteriori provvedimenti settoriali, come, per restare in tema di *social networks*, il Codice di condotta per lottare contro le forme di incitamento all'odio online, redatto dai principali social networks su impulso della Commissione europea nel 2016. É evidente, in breve, che una ricostruzione comprensiva degli obblighi dei *gatekeepers* non potrebbe essere svolta in queste brevi pagine e richiederebbe un'analisi estensiva non solo del Regolamento in esame, ma di un gran numero di altre previsioni disseminate nella copiosa normativa in materia.

[24] v. G. COLANGELO, *The European Digital Markets Act and antitrust enforcement, a liaison dangereuse*, in *European Law Review*, 2022, 608.

non rendendo comunque possibile la compatibilità tecnica di prodotti con i propri servizi di piattaforma di base.

Le previsioni applicabili ai negozi di applicazioni online sono ispirate alla medesima logica di favorire la neutralità del negozio. E così i commi 3, 4 e 6 dell'art. 6 del DMA stabiliscono rispettivamente l'obbligo in capo al gestore del sistema operativo di consentire, anche a livello tecnico, che il consumatore disinstalli le app preimpostate, modifichi le opzioni preimpostate che lo indirizzano verso le app del gestore, ed in particolare di modificare il negozio di app preimpostato, di installare app di terzi e di renderle app preimpostate.

Si tratta evidentemente di novità che, se efficacemente implementate, potrebbero avere un effetto potenzialmente dirompente sul mercato dei servizi in rete, posto che i sistemi operativi e gli app store possono in un certo modo essere immaginati come catalizzatori di *gatekeepers*[25].

b) Norme sui servizi di intermediazione in rete (in parte applicabili ai motori di ricerca).

I servizi di intermediazione online sono servizi della società dell'informazione ai sensi del Regolamento 2015/1535, che, sulla base di una relazione commerciale tra il fornitore del servizio stesso ed un utente commerciale, consentono a quest'ultimo di offrire beni o servizi ai consumatori. Un fenomeno frequente in questo particolare ambito dell'economia digitale è detto integrazione verticale e consiste nel fatto che lo stesso fornitore del servizio offre beni e servizi ai consumatori sul servizio stesso, in concorrenza con gli utenti commerciali. In questi casi, è necessario impedire al fornitore di servizi di favorire i propri prodotti a danno dei concorrenti.

La definizione di servizi di intermediazione online sopra riportata è contenuta nel Regolamento 2019/1150, cosiddetto Regolamento P2B art. 2, c.2, espressamente richiamato dal DMA, che ha in parte aperto la strada alle innovazioni del DMA, introducendo dei requisiti di trasparenza delle condizioni contrattuali dei fornitori di servizi di intermediazione. In particolare, il Regolamento P2B, oltre ad imporre un generico principio di chiarezza dei termini e condizioni contrattuali (art. 3), prevede un obbligo di comunicazione in caso di cessazione della fornitura di servizi (art. 4), un obbligo di trasparenza dei criteri di posizionamento dei risultati di ricerca (art. 5), un obbligo di trasparenza in virtù del quale il fornitore di servizi deve chiarire eventuali trattamenti differenziati (art. 7), un obbligo di trasparenza sull'accesso ai dati degli utenti commerciali (art. 9), nonché l'introduzione di un meccanismo di reclamo interno al servizio di intermediazione online.

Tali norme non hanno una particolare efficacia dissuasiva, poiché possono condurre a sanzioni solo dopo che le Autorità nazionali abbiano rilevato ripetute violazioni da parte del soggetto, ma svolgono un'importante funzione con riferimento all'obbligo di cui all'art. 6, c. 5. La norma in esame, a differenza di altre previsioni contenute nell'elenco di cui agli artt. 5-7 del DMA, non è esplicitamente indirizzata ai servizi di intermediazione online, e si applica anche ai motori di ricerca di tipo generalista. Vieta ai *gatekeepers* di garantire un trattamento più favorevole, in termini di posizionamento e *crawling* ai servizi e prodotti offerti dal *gatekeeper* stesso rispetto a prodotti e servizi analoghi di

[25] v. O. BORGOGNO, G. COLANGELO, *Platform and device neutrality regime: the transatlantic new competition rulebook for app stores?* in *The antitrust Bulletin*, 2022.

terzi[26]. Ad esempio, un motore di ricerca non può posizionare un servizio di proprietà dello stesso fornitore, potrebbe trattarsi di una mappa o di un servizio di traduzione, in modo più favorevole rispetto ai concorrenti, pratica che attualmente è frequente, come ammesso dal considerando 51 del DMA, che rileva una posizione di conflitto di interesse.

Il secondo capoverso della norma, secondo cui il *gatekeeper* applica condizioni trasparenti eque e non discriminatorie al posizionamento, si lega, qualora il *gatekeeper* sia una piattaforma di e-commerce o un motore di ricerca, agli obblighi di trasparenza di cui all'art. 5 del Regolamento P2B, che impongono a tali soggetti di fornire informazioni sul funzionamento dei meccanismi algoritmici che determinano il posizionamento delle informazioni nei propri servizi. Un problema discusso in dottrina ed in giurisprudenza, con riferimento all'equità dei sistemi di raccomandazione di contenuti in rete, quali sono i criteri di posizionamento dei servizi di intermediazione online, riguarda il problema dell'analisi controfattuale, che si preoccupa di come misurare una discriminazione a danno di un utente commerciale quando non esiste uno standard minimo di visibilità garantita alla singola informazione o, nel caso dei servizi di informazione, alla singola offerta commerciale[27].

È bene chiarire fin da subito che non si tratta di un problema meramente teorico. In numerosi passaggi ripresi dalla CGUE, nel noto caso Google Shopping, Google si difendeva dall'accusa di aver favorito i servizi verticalmente integrati a danno dei concorrenti, opponendo che la Commissione non era riuscita a identificare uno standard minimo di visibilità che Google avrebbe dovuto garantire ai propri concorrenti[28]. Ciò evidenzia come, in assenza di un criterio controfattuale, è impossibile determinare se vi sia stata una violazione e quale sia l'ammontare. Un suggestivo orientamento suggerisce invece che dei criteri oggettivi di visibilità delle informazioni in rete, tali da consentire l'analisi controfattuale necessaria a valutare *an* e *quantum* delle violazioni delle norme in tema di posizionamento, possono essere ricavati scomponendo l'algoritmo che determina i risultati delle ricerche effettuate attraverso servizi di intermediazione nei suoi diversi elementi[29]. Infatti, gli algoritmi che determinano il posizionamento delle informazioni in rete non sono concepiti come formule monolitiche, ma si compongono ~~invece~~ di diversi elementi. Secondo la dottrina citata, pur nella loro complessità, è possibile identificare degli elementi che attribuiscono un punteggio di base alle informazioni, al fine di favorire le informazioni che hanno una maggiore probabilità di attirare l'attenzione di un utente. Altri elementi si innestano su

[26] Il posizionamento è definito al considerando 24 del Regolamento 2019/1150: "Il posizionamento si riferisce alla rilevanza relativa delle offerte degli utenti commerciali o alla rilevanza attribuita ai risultati della ricerca come presentati, organizzati o comunicati dai fornitori di servizi di intermediazione online o dai fornitori di motori di ricerca online, risultante dall'utilizzo di meccanismi algoritmici di ordinamento in sequenza, valutazione o recensione, dalla messa in evidenza visiva o da altri strumenti di messa in rilievo, o da una combinazione tra questi".

[27] Così, con riferimento alla moderazione di contenuti nei social media, in T. GILLESPIE, *Do not recommend? Reduction as a form of content moderation*, in *Social Media + Society*, 2022.

[28] Causa T-612/17, Google LLC c. Commissione, § 359, § 374.

[29] Di nuovo, con riferimento alla moderazione di contenuti nei canali social media, ma applicabile in toto anche al posizionamento di annunci online o altre informazioni commerciali, v. P. LEERSEN, *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, in *Computer Law& Security Review*, 2023, 8-9.

tale punteggio di base in un momento successivo, attribuendo *bonus* e *malus* che possono ulteriormente aggiustare il posizionamento ai criteri preimpostati dal fornitore del servizio. Emerge allora l'importanza degli obblighi di trasparenza di cui al Regolamento P2B ed in particolare degli obblighi di cui agli artt. 5 e 7. In particolare, l'art. 5 stabilisce, utilizzando formule leggermente diverse per servizi di intermediazione e motori di ricerca, che devono essere chiariti i parametri che determinano il posizionamento, nonché i motivi per cui a determinati parametri è data importanza. Quando è data la possibilità di influire sul posizionamento dietro un corrispettivo, gli effetti di questo sul posizionamento devono essere trasparenti.

Si profila allora una tensione tra l'interesse del fornitore di servizi di intermediazione a mantenere il segreto industriale sul funzionamento del suo meccanismo di raccomandazione algoritmica e le previsioni del Regolamento P2B, che impongono la pubblicazione nei termini e condizioni di criteri di posizionamento sufficientemente dettagliati da consentire all'utente commerciale di conoscere i diversi elementi costitutivi che compongono il risultato della ricerca[30]. Un tentativo di bilanciare i due interessi appena abbozzati è stato formulato dalla Commissione europea, che pur riconoscendo che "il funzionamento dettagliato dei metodi di posizionamento può costituire un segreto commerciale (del prestatore di servizi di intermediazione online o del motore di ricerca)", ha altresì riconosciuto altrettanta meritevolezza nell'interesse degli utenti commerciali a poter conoscere i motivi del proprio posizionamento per migliorarlo[31]. La tutela di tale interesse giustifica allora l'obbligo in capo ai fornitori di servizi di intermediazione e motori di ricerca di pubblicare quantomeno tutti i parametri utilizzati per determinare il posizionamento di un'informazione, nonché i motivi della loro rilevanza, in modo da attribuire all'utente commerciale un certo livello di comprensione[32]. Ciò che qui preme sottolineare è che parametri sufficientemente precisi da consentire un certo livello di comprensione all'utente commerciale possono anche essere utilizzati dalla Commissione per valutare se il posizionamento effettivamente implementato dal fornitore di servizi corrisponda ai criteri pubblicati, superando così la questione degli elementi controfattuali nell'analisi del posizionamento.

La previsione di cui all'art. 6, comma 5, non esaurisce il novero delle disposizioni applicabili ai servizi di intermediazione. Queste includono anche i commi 3 e 4 dell'art. 5 che, rispettivamente, vietano ai *gatekeeper* di impedire agli utenti commerciali di offrire gli stessi prodotti o servizi agli utenti finali attraverso servizi di intermediazione di terzi; e l'obbligo di consentire agli utenti commerciali, a titolo gratuito, di promuovere e comunicare offerte, anche a condizioni diverse, agli utenti finali acquisiti attraverso il proprio servizio di piattaforma di base.

c) Obblighi di interoperabilità in capo ai servizi di messaggistica indipendenti dal numero

[30] Ciò sembra essere confermato dagli Orientamenti sulla trasparenza del posizionamento a norma del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio

[31] Comunicazione 2020/C 424/01, contenente Orientamenti sulla trasparenza del posizionamento a norma del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio.

[32] v. il §22 della stessa Comunicazione della Commissione.

Tutto l'art. 7 del DMA è dedicato a obblighi specifici in capo ai servizi di comunicazione interpersonale indipendenti dal numero, già definiti nel codice europeo delle comunicazioni elettroniche (direttiva UE 2018/1972) come servizi di comunicazione interpersonale che non si connettono a risorse di numerazione assegnate pubblicamente. L'art. 7, c. 1 del DMA modifica il contenuto della direttiva, che liberava dalla maggior parte degli obblighi applicabili agli altri servizi di comunicazione, come ad appunto gli obblighi di interoperabilità.

La norma obbliga infatti i *gatekeeper* che siano fornitori di servizi di comunicazione interpersonale indipendenti dal numero a rendere le proprie funzionalità di base compatibili con le funzionalità di base di altri fornitori di servizi. Cosa si intenda per funzionalità di base si ricava dal successivo art. 7, c. 2 del DMA, che prevede un vero e proprio piano di realizzazione dell'interoperabilità tra servizi di messaggistica indipendenti dal numero, scaglionando una serie di obblighi, che devono portare i servizi in esame ad essere pienamente interoperabili entro 4 anni dalla designazione. Funzionalità di base sono allora i messaggi, sia tra utenti singoli, sia nelle chat di gruppo, la condivisione di messaggi vocali, video e file allegati, le chiamate e le video chiamate sia tra utenti singoli, sia tra utenti singoli e chat di gruppo.

4. Neutralità della rete su più livelli: spunti comparativi.

Si è deciso di raggruppare gli obblighi elencati alle lett. a), b) e c) di questo paragrafo sotto la categoria unitaria della neutralità della piattaforma, poiché tutte le previsioni trattate qui hanno la finalità di impedire che il controllo da parte di *gatekeeper* dei colli di bottiglia dell'informazione rappresentati dai servizi di piattaforma di base possa consentire al *gatekeeper* di favorire i propri servizi verticalmente integrati o di escludere servizi concorrenti. L'applicazione del concetto di neutralità della rete alle piattaforme è stata già discussa in dottrina, sia, diffusamente, in materia di criteri di attribuzione della responsabilità della piattaforma[33], sia, più recentemente, in materia di tutela del mercato digitale, con riferimento ai *gatekeepers*[34]. In questa sede non si ha la pretesa di contribuire al dibattito, posto che il concetto stesso di neutralità della rete e la sua applicabilità ai *gatekeepers* in linea teorica meriterebbero e richiederebbero un'autonoma trattazione, ma solo di introdurre il tema.

Il fondamento dei meccanismi legislativi volti a favorire la neutralità di qualsiasi rete rispetto alle applicazioni periferiche che operano sulla rete si fonda sulla convinzione che i divieti di discriminazione delle applicazioni periferiche finiscano a lungo termine per favorire sia l'innovazione, sia i

[33] In particolare, in seguito alla discussa decisione della CGUE, *Google France* (C-236/08 - C-238/08). Con riferimento alla dottrina, si v. su tutti, l'ampio studio a cura di G. FROSIO, *The Oxford Handbook of online intermediary liability*, Oxford, 2020.

[34] Sebbene risalire alla paternità delle dottrine non sia facile, né utile, giova ricordare che il tema della neutralità della piattaforma in materia di concorrenza è stato sollevato dalla CGUE nel noto e già citato caso "Google Shopping", (Causa T-612/17, Google LLC c. Commissione), §180, oltre ad essere stato discusso in dottrina, si v. nuovamente O. BORGOGNO, G. COLANGELO, *op. cit.*

consumatori[35]. Nel breve termine, infatti, l'integrazione verticale di servizi a danno dei concorrenti può essere giovevole per i consumatori, che beneficiano dell'effetto di rete generato dagli ecosistemi di servizi[36]. Nel lungo periodo, tuttavia, un mercato dominato dalla presenza di poche grandi aziende, finisce per limitare le possibilità di innovazione, intesa come fenomeno serendipico e dirompente: la natura aperta e neutrale della rete non impedisce a privati che intendano competere con i soggetti che controllano le infrastrutture di avere la possibilità di prevalere. Il vantaggio principale della competizione su un mercato innovativo, in questo ordine di idee, non è di incentivare le scelte ottimali e quindi una corretta allocazione delle risorse, come suggeriscono le teorie economiche ortodosse. Data l'imprevedibilità delle risposte delle imprese agli stimoli del mercato innovativo, quest'ultimo assurge a laboratorio di sperimentazione economica e sociale[37]. La competizione nel mercato innovativo consente agli operatori di mercato di sperimentare le diverse applicazioni commerciali della tecnologia innovativa e, di converso, ai consumatori di selezionare le migliori, intese come quelle più commercialmente utili[38].

Può essere utile, per svolgere un breve approfondimento sul tema della neutralità della rete, riprendere la distinzione tra servizi essenziali (*basic*) e avanzati (*enhanced*), operata negli anni '80 dalla Federal Communications Commission statunitense[39]. Sono fornitori di servizi essenziali quelli il cui compito si limita alla trasmissione di pacchetti di dati attraverso la rete

[35] Il tema è discusso con grande chiarezza, con riferimento alla neutralità degli Internet Service Providers, in T. WU, *Network Neutrality, Broadband Discrimination,* in *Telecomm. & High Tech.* L. 141, 2003, p. 141. L'A. osserva peraltro come il tema della neutralità della rete sia stato al centro del dibattito statunitense in tema di concorrenza, fin da prima dell'invenzione di Internet. Il noto caso *Hush-A-Phone c. Stati Uniti,* 238 F.2d 266 (D.C. Cir. 1956), vide contrapporsi una linea telefonica nazionale, AT&T, che aveva un monopolio di fatto sugli apparecchi telefonici e Hush-A-phone, una società fondata da un professore del MIT di Boston, che si affacciava sul mercato, offrendo apparecchi telefonici innovativi compatibili con la rete AT&T. AT&T forte del suo controllo della rete, imponeva a Hush-A-phone di pagare una tariffa, asseritamente giustificata dal rischio causato da apparecchi non compatibili con la rete. Il giudice statunitense decise in questo caso che le tariffe sui dispositivi Hush-A-Phone erano un'interferenza ingiustificata con il diritto dell'abbonato di usare il suo telefono in modi che sono vantaggiosi per il privato senza essere dannosi per il pubblico.

[36] Cfr. con F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge, Massachussetts, 2015, 66.

[37] Cfr. con R. NELSON, *Understanding Technical Change As An Evolutionary Process*, New Holland Amsterdam (1987), 450 - 453.

[38] Visione che il legislatore euro-unitario sembra aver fatto propria, nel parlare di "corretto funzionamento del mercato interno stabilendo norme volte a garantire la contendibilità e l'equità per i mercati nel settore digitale in generale e per gli utenti commerciali e gli utenti finali dei servizi di piattaforma di base forniti dai *gatekeeper* in particolare" (considerando 7).

[39] Più precisamente, fu introdotta nel nel Amendment no. 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), Docket No.20828, Final Decision, 77 FCC 2d 384, 420, para. 97 (1980) (Computer II Final Decision), anche conosciuto come "Computer II Order". Con una serie di decisioni prese negli anni '80 e conosciute come *Computer Inquiries*, la FCC ha creato una distinzione tra servizi *basic* (essenziali) ed *enhanced* (avanzati). I primi sono i servizi che offrono una mera capacità di comunicazione che è virtualmente trasparente in termini di interazione con le informazioni (i dati) inserite dagli utenti. Questi consistono ad esempio nei servizi di connessione alla banda larga o anche nei servizi telefonici, che normalmente prevedono la corresponsione di un canone. L'accesso al mercato dei servizi *basic* è soggetto a regole particolarmente stringenti. Trattandosi di un'attività che per sua stessa natura è soggetta a monopoli od oligopoli, le autorità regolatrici devono impedire agli operatori di questo mercato di sfruttare il controllo della rete per escludere potenziali concorrenti o esercitare altre forme di controllo sul flusso di dati. È quindi evidente che un mezzo di comunicazione che si serva del protocollo TCP/IP sia architettonicamente predisposto a creare una rete semplice e neutrale rispetto ai contenuti trasmessi. I servizi *enhanced*, che invece hanno finito per evolversi nelle cosiddette piattaforme Internet, ben possono caratterizzarsi per una maggiore complessità, ovvero per il fatto di gestire i dati trasmessi dal prestatore di servizi *basic*.

Internet. In quanto fornitori di servizi essenziali, hanno limitate possibilità di comprimere le attività dell'utenza entro dei confini prestabiliti. La normativa riguardante tali servizi si preoccupa in sostanza di assicurare la neutralità della rete, in modo da garantire che i fornitori di servizi avanzati possano competere in un mercato aperto [40]. I fornitori di servizi avanzati sono prestatori di applicazioni periferiche che operano sulla rete, come a esempio i siti Internet, e accedono al mercato aperto che la regolazione dei servizi essenziali consente. Possono essere immaginati come delle sovrastrutture che si agganciano all'architettura di base della rete. Tradizionalmente, la legislazione sui fornitori di servizi *enhanced* non ha imposto la neutralità rispetto alle informazioni trasmesse. Il tentativo operato dalla CGUE di distinguere tra fornitori di servizi sulla rete che operano un ruolo meramente tecnico e neutrale e quelli che operano un ruolo attivo[41], per discriminare i casi in cui al fornitore di servizi in rete possa essere ascritta la responsabilità per gli illeciti causati dal comportamento illecito per l'utente è stato giustamente criticato per essere incappato nel *gatekeeper paradox* individuato dalla dottrina statunitense fin dagli anni '90, oltre che per essere fondato su un'interpretazione forzata del considerando 42 della direttiva 2000/31[42].

Al fornitore di servizi *enhanced*, quale è una piattaforma social, un sito di e-commerce o un motore di ricerca, non si è tradizionalmente richiesta la neutralità perché il ruolo di questi soggetti è proprio di ordinare le informazioni create dagli utenti della rete, al fine di renderle fruibili[43]. È su questo principio che il DMA interviene, poiché i grandi *gatekeepers* della rete, fornitori di servizi *enhanced* che dominano il mercato, hanno acquisito la capacità di attuare le stesse pratiche discriminatorie che la neutralità della rete mirava a prevenire[44].

La neutralità del fornitore di servizi *enhanced* non viene più intesa, come faceva la CGUE nei casi citati, come l'astenersi dall'avere un ruolo attivo nella trasmissione di informazioni, cosa che evidentemente esclude la neutralità di qualsiasi fornitore, ma come la trasmissione di informazioni secondo criteri per quanto possibile trasparenti e oggettivi, tali da assicurare ex ante che il gatekeeper non favorisca i propri servizi verticalmente integrati.

5. Dei limiti applicativi concreti.

Tornando a questioni più immediate, problema centrale per i meccanismi di cui alle lett. a), c) e d) è quando possa parlarsi di due diversi servizi forniti dal *gatekeeper* e quando invece due funzioni distinte siano riferibili ad un unico servizio. La nozione di "diversi servizi" è utilizzata per delimitare soggetti diversi, che non possono combinare dati personali, né utilizzarli in modo incrociato, né favorire i risultati. La definizione di servizio della società dell'informazione contenuta nel Regolamento 2015/1535, cui rinvia il comma 3

[40] Nel diritto europeo, la normativa sulla neutralità della rete si rinviene nella direttiva 2015/1535.
[41] Caso c.d. Google France, C-238/08, 23/03/2010 *Google France SARL, §114.*
[42] Per un'esaustiva rassegna di tale risalente dottrina, non si può che rimandare a G.M. RICCIO, *La responsabilità civile degli Internet providers*, Torino, 2002, 108 e ss.
[43] J. GOLDSMITH, T. WU, *Who controls the Internet? Illusions of a borderless world*, Oxford, 2006, passim.
[44] I. COMEIG,K. KLASER, L.D. PINAR, *The paradox of (Inter)net neutrality: an experiment on antitrust regulation*, in *Technological Forecasting and Social Change*, 2022, 2.

dell'art. 2 del DMA, non fornisce alcuna indicazione utile a separare concettualmente i servizi digitali forniti da un medesimo prestatore[45]. Il DMA elenca e definisce alcuni tipi di servizi ai commi 6 – 19 dell'art. 2, quali ad esempio i motori di ricerca, i social networks ed i servizi di piattaforma per la condivisione video. Tali definizioni mantengono tuttavia un tenore troppo vago per consentire di inquadrare quale servizio unico o pluralità di servizi fattispecie concrete che sono sempre più complesse. Si pensi, per restare agli esempi appena riportati, a social networks che consentono anche la condivisione video. Maggiori indicazioni provengono in alcuni casi dalle discipline settoriali cui il DMA non manca di rinviare. Così, in tema di motori di ricerca, il rinvio è al Regolamento 2019/1150, che fornisce una più ampia definizione di motore di ricerca, dalla quale è possibile ricavare dei tratti distintivi del motore di ricerca e così considerare servizio separato ciò che fornisce funzionalità ulteriori rispetto a quelle proprie del motore di ricerca[46]. Sotto questo fondamentale profilo, la scelta del legislatore comunitario di non fornire criteri generali di delimitazione dei servizi diversi rimane in ogni caso criticabile. Innanzitutto, non tutti i servizi elencati nel DMA sono oggetto di definizioni specifiche in altri regolamenti euro-unitari, come avviene per i motori di ricerca. D'altra parte, i servizi in rete sono in costante evoluzione, il che rende l'utilità di un elenco tassativo di servizi come quello previsto all'art. 2 del DMA relativa e circoscritta nel tempo.

[45] L'art. 1, c. 1, lett. b) definisce "servizio qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi".

[46] Si riporta qui la definizione di cui all'art. 5, comma 2 del Regolamento P2B: "motore di ricerca online": un servizio digitale che consente all'utente di formulare domande al fine di effettuare ricerche, in linea di principio, su tutti i siti web, o su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto.

Izzo L, 'Satellite Data Management and Privacy Law' (2024) 1 EJPLT, 219-230.
DOI: https://doi.org/10.57230/EJPLT241LI

EJPLT
ISSN 2704-8012



EO Satellite Data Management and Privacy Law*

La gestione dei dati satellitari nell'osservazione della Terra e la tutela della privacy

LUIGI IZZO
Ph.D.(s) in Humanities and Technologies: an integrated research path
Università degli Studi Suor Orsola Benincasa

Abstract

The relevance of the space sector is increasing, with reference not only to the traditional telecommunications satellites but also to Earth Observation satellites, equipped with increasingly sophisticated electro-optical, radar and spectrographic payloads capable of collecting increasingly precise and well-defined data. This space race sees the participation above all of private entities that carry out extensive data collection, with the sole aim of making it profitable. In this light, the aim of the paper is to specifically analyze the issue of personal data processing, also with regard to the latest advances in the field of sensors and access to space.

La rilevanza del settore spaziale sta aumentando, con riferimento non solo ai tradizionali satelliti per le telecomunicazioni ma anche quelli per l'Osservazione della Terra, dotati di payload elettro-ottici, radar e spettrografici sempre più sofisticati e in grado di raccogliere dati sempre più precisi e definiti. Questa corsa allo spazio vede la partecipazione soprattutto di soggetti privati che effettuano un'ampia raccolta di dati, con l'unico scopo di renderla redditizia. In quest'ottica, l'obiettivo del documento è quello di analizzare nello specifico la questione del trattamento dei dati personali, anche in relazione agli ultimi progressi nel campo dei sensori e dell'accesso allo spazio.

* The paper is the result of the work of a researcher of the Research Centre of European Private Law (ReCEPL) at Università degli Studi Suor Orsola Benincasa, with the collaboration of PhD(s) Alessandra Fabrocini and PhD Anna Anita Mollo, and the coordination of the ReCEPL Director Prof. Lucilla Gatt and the ReCEPL Vice-Director Prof. Ilaria A. Caggiano.
The work was presented at the IEEE International Conference 'MetroAeroSpace', held in the Bovisa Campus, Politecnico di Milano, Milan, June 19-21, 2023, and published in the 2023 IEEE 10th International Workshop on Metrology for AeroSpace (MetroAeroSpace), 247.

Image: ESA/ATG medialab

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Earth Observation; Satellite Data; Data Management; Privacy Law.

Summary: 1. Introduction. – 2. The international framework on space activities. – 3. National and EU laws on remote sensing activities. – 3.1. Lobbying in the field of EO operations. – 3.2. Some example of national frameworks. – 3.3. EU framework for remote sensing activities: the Copernicus Programme. – 4. A combination of licensing procedures with privacy assessment? – 4.1. When can EO data become personal data? – 4.2. A first hypothesis: combining evaluation for ITU licences with privacy protection. – 5. Conclusions.

1. Introduction.

The Space Age, which in fact began as a result of Wernher von Braun's rocket research, saw as its protagonists the States. However, it is also true that the private sector immediately experienced intensive growth, which began in the United States of America with telecommunications satellites (Communications Satellite Act of 1962) and later extended to almost every type of space activity (Commercial Space Launch Act of 1984). Subsequently, the various national regulations have evolved steadily to encompass all areas of space operations and to bolster the competitiveness of companies operating in the overall sector.

This has allowed private players to attract new investments, further advancing technologies and reducing the cost of the assets needed to operate in the space[1]. This is true not only in the field of telecommunications or geolocation but also in the field of Earth Observation.

First of all, the progressive process of miniaturisation of the electronic and sensor components in general of satellites must be considered. For example, SAR sensors - in the civil sector - were initially used on a platform whose mass was 1800 kg (NASA SeaSat 1, launched in 1978[2]) while we are now witnessing a miniaturisation such that they can be used on platforms in the 'smallsat' class[3] and on specific microsatellites[4], in contrast to the large platforms still used by States[5].

The same tendency is also present for optical sensors, already available for CUBESat satellites[6]. Another element to be taken into account is the wide availability of medium or light launchers for launching satellites, whose

[1] D. Chow, "To cheaply go: How falling launch costs fueled a thriving economy in orbit", https://www.nbcnews.com/, April 2022.
[2] NASA webpage for the SeaSat 1 satellite, https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=1978-064A
[3] FAA, The Annual Compendium of Commercial Space Transportation: 2018, 2018, p. 94.
[4] A. Golkar, G. Cataldo, K. Osipova, "Small satellite synthetic aperture radar (SAR) design: A trade space exploration model", Acta Astronautica, Vol. 187, 2021, 458-474. See also W. Johannes *et al.*, "Miniaturized high resolution Synthetic Aperture Radar at 94 GHz for microlite aircraft or UAV," SENSORS, 2011 IEEE, Limerick, Ireland, 2011, 2022-2025.
[5] S.W. Paek, S. Balasubramanian, S. Kim, O. de Weck, "Small-Satellite Synthetic Aperture Radar for Continuous Global Biospheric Monitoring: A Review.", Remote Sens. 2020, 12, 2546.
[6] T. Rotovnik, D. Gacnik, I. Kramberger, "Miniaturized Multispectral VNIR/SWIR Imager for Small Satellites - System Design", IFAC-PapersOnLine, Vol. 48, Issue 10, 2015, 12-15.

operating costs are much lower than those for 'heavy' launchers[7]. But, now, the launchers are being challenged by an even cheaper system, at least for the smallest satellites, a ground-based 'slingshot' designed by SpinLaunch[8], with a single launch cost of less than half a million dollars[9].

Finally, consider the advances in the field of image resolution. With reference only to SAR sensors, if we compare images produced in the 1990s with those currently available, we can see that in the 1990s the EO satellites were using a C-Band sensor with a resolution of 20m, while the satellites launched in the first decade of 2000s were using X-band sensors with a resolution of 1m[10]. Thus, in less than two decades, an outstanding achievement in the field of SAR sensors has been achieved, increasing the attractiveness of their data.

As a result of the above, new issues arise from a legal point of view. In the long run, it would be possible to perpetrate violations of the privacy of individuals through the processing of images from EO satellites. Of course, this might seem like a forced and hasty statement. Yet, as has happened in the fields of telecommunications, geo-localisation and information technology, nothing prevents technological advances and economic policy choices by major private players from leading to privacy risks.

Just with regard to information technology and personal computers, the initial spread of PCs and the Internet could not lead to systematic and widespread privacy concerns, which only spread later, with innovations in operating systems and economic policy choices[11], forcing legislators to address the issue and introduce new legal instruments. Thus, action was taken, but only after the problem had manifested itself, instead of adopting an overall approach aimed at preventing it, as far as possible.

2. The international framework on space activities.

First, it is worth taking a brief look at the international law framework on space.

As is well known, the *Corpus Iuris Spatialis* saw the light of day in a context of high conflict and its core consists of five Treaties: the Outer Space Treaty, the Rescue Agreement, the Liability Convention, the Registration Convention and the Moon Agreement[12], all drafted by the Committee on the Peaceful Uses of

[7] See FAA, The Annual Compendium, Launch Vehicle Fact Sheets "Falcon 9" and "Vega". See also J. Joly, "Move over, SpaceX: ArianeGroup to make Europe's first reusable and 'eco-friendly' rockets", www.euronews.com, July 2022.
[8] SpinLaunch homepage, https://www.spinlaunch.com/
[9] P. V. Siddhart, "Why Launch Rockets When You Can Just Fling Them Into Space?", https://www.bloomberg.com/, May 2023.
[10] A. Moreira, P. Prats-Iraola, M. Younis, G. Krieger, I. Hajnsek, and K. Papathanassiou, A Tutorial on Synthetic Aperture Radar. IEEE Geoscience and Remote Sensing Magazine, vol. 1, issue 1, April 2013, 6-43.
[11] See L. Gatt, R. Montanari and I.A. Caggiano (eds.), Privacy and Consent. A Legal and UX&HMI Approach University Suor Orsola Press, 2021. L. Gatt (ed.), Social Networks and Multimedia Habitats. Jean Monnet Chair PROTECH. "European Protection Law of Individuals in Relation to New Technologies". 1st International Workshop A.Y. 2019-2020 University Suor Orsola Press, 2020.
[12] For more information about the Five Treaties see F. G. von der Dunk, Advanced Introduction to Space Law, Elgar, 2020, 14-39.

Outer Space (COPUOS) of the United Nations[13]. The 1967 Outer Space Treaty, actually considered *customary law*, contains the structural principles that regulate activities in outer space. This means that any space activity by any Nation is subject to the provisions of this Treaty.

However, it is focused on peaceful cooperation, on the impossibility of placing state jurisdictions in orbit (as is the case, instead, with the so-called 'territorial waters' and 'national airspace'). This is the reason why the first four articles (Articles I, II, III, IV) focus on conceptually denying the possibility of expanding national jurisdictions beyond their current boundaries. It follows, therefore, that the Treaty just referred to does not focus at all on the activities of private entities, even though, due to the provisions of Articles VI, VII and VIII and, above all, thanks to the existence of a convention on the registration of 'vehicles' sent into orbit, it constitutes the fundamental basis for any further development of space legislation. This is also due to the presence of provisions that are deliberately broad in meaning, so that they can be applied by interpretation in the most diverse cases, as well as serving as a legal basis for various future provisions. Indeed, it would not be wrong to think that the Outer Space Treaty is, in the sphere of space and international law, a kind of Constitutional Charter, from which all other provisions relevant to the sphere under consideration are derived.

This makes it possible to introduce UN General Assembly Resolution 41/65[14], which, as far as the subject of this contribution is concerned, still focuses on legal entities called 'States' but provides an initial legal basis for remote sensing activities. In fact, the resolution is headed 'Principles Relating to Remote Sensing of the Earth from Outer Space'. This resolution recalls the concept of peaceful exploitation of space based precisely on the provisions of the Outer Space Treaty (see Principle III).

The problem addressed by the Resolution was very simple: as F. G. von der Dunk summarises, it "*concerned the increasing possibilities of using satellite remote sensing for sounding out terrestrial opportunities for mineral resource mining […] giving rise to worries in particular with developing States being sensed that the developed State sensing them would use the knowledge gained for their own economic purposes, in addition to worries that data which could alleviate suffering and destruction in humanitarian crises would not be made readily and/or freely available*"[15]. For this reason, the sensed States sought to promote the principle of "prior consent" in the field of remote sensing while the States operating the satellites were obviously against such a regulatory development.

In an attempt to reconcile the two, Principle XII was outlined, which provides that the sensed State shall have access to these data on a non-discriminatory basis and on reasonable cost terms, taking particularly into account the needs and interests of the developing countries.

The problem is this: does the data that can be accessed also include data produced by private companies specialising in remote sensing (e.g. Maxar) or

[13] COPUOS webpage: https://www.unoosa.org/oosa/en/ourwork/copuos/index.html
[14] UN General Assembly Resolution 41/65 - https://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/remote-sensing-principles.html
[15] F. G. von der Dunk, Advanced Introduction to Space Law, 59.

only those produced by state-owned satellites[16]? If one considers that the principle requires that the data must be in the possession of the State carrying out the remote sensing activities, then it could be understood to mean that data in the possession of companies specialising in Earth Observation in that same State are not covered by this principle. Therefore, those companies would be free to sell them on the market at the conditions they consider most appropriate. If one thinks, however, that Principle XIV invokes the responsibility of States under Article VI of the Outer Space Treaty, then one might think that States with such responsibility are also, in a sense, 'in possession' of the data generated by private operators authorised by them. Thus, data generated by private EO satellites would also be subject to the provisions of Principle XII. In both cases, since this was a UN Resolution passed in 1986, no consideration was given to the possibility that such data might later lead to hypothetical violations of privacy.

3. National and EU laws on remote sensing activities.

3.1. Lobbying in the field of EO operations.

First of all, when talking about EO activities and the respective national regulations, it is necessary to start from a fundamental element: these are legal provisions aimed at private legal entities and designed to reconcile the needs of the market with national security requirements. For this very reason, it is impossible to deny the existence of lobbying activity at the national level, in the various states with a flourishing aerospace industry, especially those in the West, aimed at reducing the limits on the resolution and dissemination of data produced by EO satellites[17].

This activity has become even more intense in recent years in view of the progress made by various states (India, China, etc.) in developing their aerospace industries [18]. Hence, a serious issue arose concerning the competitiveness of Western companies, influencing the evolution of national regulations.

3.2. Some examples of national frameworks.

First consider the US framework, placed in the Code of Federal Regulations, in the Title devoted to Foreign Trade (Title 15, Subtitle B, Chapter IX, Subchapter D, Part 960)[19], recently reformed involving the NOAA and the major players in the industry[20].

---

[16] F. G. von der Dunk, Advanced Introduction to Space Law, pp. 61 and following.

[17] P. B. de Selding, "Satellite Imagery Firms in U.S. and Europe Pushing for Permission To Sell Sharper Imagery", https://spacenews.co/, September 2013. T. Hicthens, "Commerce Slashes Restrictions On Remote Sensing Sats", https://breakingdefense.com/, May 2020.

[18] S. Singh, "New space policy allows pvt cos to set up, operate own network of remote sensing satellites", https://timesofindia.indiatimes.com/, April 2023.

[19] US Code of Federal Regulations, Title 15, Subtitle B, Chapter IX, Subchapter D, Part 960, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-IX/subchapter-D/part-960

[20] Comments to the Final Rule, https://www.regulations.gov/document/NOAA-NESDIS-2018-0058-0040/comment.

This has led to a licensing system based on three tiers, each characterised by a common set of operating conditions plus a set of peculiar predictions for each Tier. When analysing the characteristics of the various Tiers, it becomes clear that the first two concern licences for remote sensing systems operating in an internationally competitive environment. Conversely, Tier 3 is aimed at those companies that intend to provide products that do not currently exist on the market, as in the case of the 10cm resolution imagery promised by Albedo Space Corp[21].

The US system, therefore, is aimed above all at ensuring national security, protecting the competitiveness of domestic remote sensing companies only to the extent strictly necessary for this purpose, so much so that the various operators in the sector have not concealed a certain disappointment with the reformed regulations that have come into force[22]. Yet, as the case of Albedo shows, NOAA does not prevent such companies from obtaining licences to operate remote sensing systems with resolutions so high that they are not available from other competitors. However, if there are no national security reasons to note, there does not seem to be a mechanism to limit dissemination. So, the various companies could - one day - produce imagery with a resolution of 5cm relating to an urban area totally devoid of military targets (or national security agency facilities) and be able to sell it to anyone, without limits, precisely because there are no elements such as those mentioned above to limit its dissemination.

With regard to regulations in countries other than the US, examples include the Title VII Space Operations Act and its implementing legislation in France[23], the Satellite Data Security Act (SatDSiG) of 2007 and the Satellite Data Security Ordinance (SatDSiV) of 2008 in Germany[24].

First of all, the French framework has been implemented with additional regulatory outline provisions, specifically Decree 2009-640 of June 2009, the Order of 4 September 2013, and Decree 2013-654 of July 2013. A key feature is that, once resolution limits are outlined for satellite images, operators only have to notify the Secretariat General of Defence of the start of operations two months in advance if the payload installed on the satellites is such that it exceeds these limits. So, there are no *ex-ante* limitations. The Secretariat can only provide for *ex-post* limitations where necessary and only if the resolution limits provided for by the regulations are exceeded. Hence, if the sensors do not exceed these limits, they are not subject to the *ex-ante* reporting requirement, nor can they be subject to data dissemination limitations[25].

---

[21] D. Werner, "Albedo wins license to sell 10-centimeter imagery", December 2021, https://spacenews.com/

[22] For instance, see the comments of Maxar Technologies Inc., Capella Space Corp. and Planet Labs Inc. about alleged ambiguities in the regulatory dictate regarding the requirements for each specific Tier. They also rail against transparency obligations.

[23] Loi no 2008-518 du 3 juin 2008 relative aux operations spatiales, Republique Francaise, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000018931380.

[24] Satellitendatensicherheitsgesetz, vom 23. November 2007 (BGBl. I S. 2590), das zuletzt durch Artikel 92 des Gesetzes vom 29. M€ arz 2017 (BGBl. I S. 626), Bundesministerium der Justiz und Fur Verbraucherschut https://www.gesetze-im-internet.de/satdsig/index.html - Satellitendatensicherheitsverordnung, vom 26. Marz 2008 (BGBl. I S. 508), die durch Artikel 1 der Verordnung vom 30. Juli 2014 (BGBl. I S. 1314), Bundesministerium der Justiz und Fur Verbraucherschutz https://www.gesetze-im-internet.de/satdsiv/.

[25] R. Harris, I. Baumann, "Satellite Earth Observation and National Data Regulation", Space Policy, 56, 2021, 3.

In Germany, however, an approach based entirely on primary legislation seems to predominate. The SatDSiG is the basic law, while the SatDSiV contains the technical characteristics used to classify Earth observation data as sensitive or non-sensitive. This regulation focuses, unlike the French one, not only on the resolution limits, but also on certain aspects of data dissemination, mainly related to assessing the reliability of the data requester and whether these data concern sensitive areas for national security[26]. The sensitivity check procedure is already outlined in the SatDSiG.

However, as in the case of the US framework, the French and German frameworks do not adopt privacy risk assessment procedures, limiting themselves solely to protecting national security.

3.3. EU framework for remote sensing activities: the Copernicus Programme.

Given the above, it is possible to analyse European legislation on Earth observation operations. However, in order to better understand the current European regulatory framework, it is necessary to reconstruct its evolution.

It all started in 1998 with the establishment of the GMES Programme (subsequently named Copernicus Programme), an Earth monitoring initiative led by the Union and implemented in cooperation with the Member States and the European Space Agency (ESA). Its objective, since the time of the Baveno Manifesto[27], has been to provide, under the control of the Union, information services that allow access to accurate data and information in the field of environment and security, adapted to the needs of users. Subsequently, the GMES programme was formally established by Regulation (EU) No 911/2010[28], which immediately paid attention (albeit with brief references) to the protection of personal data. In Recital 27, in fact, the European legislator expresses itself in these words: "*GMES initial operations should be implemented consistently with other relevant Union policies, instruments and action, in particular with […] the protection of personal data.*". Article 4(2) also states that "*The Commission shall manage the funds allocated to the activities under this Regulation in accordance with the Financial Regulation and with the management procedure referred to in Article 16(4). It shall ensure the complementarity and consistency of the GMES programme with other relevant Union policies, instruments and actions, relating in particular to the […], the protection of personal data […]*".

This led to the issuing of the Commission Delegated Regulation (EU) No 1159/2013[29], drafted in order to establish registration and licensing conditions for GMES users and define criteria for restricting access to GMES dedicated data and GMES service information. Recital 12 of this Delegated Regulation follows what was already described in recital 27 of the 2010 Regulation. Even

[26] R. Harris, I. Baumann, "Satellite Earth Observation and National Data Regulation" 4.
[27] Editorial, "A short history of the Copernicus In Situ Component since the Baveno Manifesto", June 2018, https://insitu.copernicus.eu/news/the-copernicus-in-situ-component-since-the-baveno-manifesto.
[28] Regulation (EU) No 911/2010 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32010R0911.
[29] Commission Delegated Regulation (EU) No 1159/2013 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R1159.

more important is the content of the Regulation itself, since it makes a very clear separation between the protection of the national security of European countries and the protection of the privacy of individuals. While national security is the subject of Art. 12, privacy is included among the conflicting rights listed (non-exhaustively) in Art. 11, always leaving it to the Commission to act, on a case-by-case basis and if necessary, to limit the dissemination of EO data.

As can be seen on the official EUR-Lex website, this Delegated Regulation is still in force, despite the fact that the 2010 Regulation was repealed by Regulation (EU) No 377/2014[30], which only mentions the protection of personal data in Recital 9, along the lines of what was written in Recital 27 of the repealed Regulation. Subsequently, the 2014 Regulation was in turn repealed by Regulation (EU) 2021/696[31], which created a European Union Space Agency (EUSPA, not to be confused with its partner ESA, the European Space Agency, founded several decades earlier) and provided the legal basis for a fully-fledged European space programme, including the Copernicus programme.

This Regulation fully takes up the legacy of the previous regulatory texts. In fact, in Recital 81 it expressly recalls the 2013 Delegated Regulation, requiring its application and compliance, and there is a dedicated article, Article 104(1), aimed precisely at the protection of personal data which states as follows: *'1. All personal data handled in the context of the tasks and activities provided for in this Regulation, including by the Agency, shall be processed in accordance with the applicable law on personal data protection, in particular Regulations (EU) 2016/679 and (EU) 2018/1725 of the European Parliament and of the Council.*'.

As can be seen, the expression is particularly broad (which makes its application by interpretation possible even in future and particularly problematic cases) and such as to allow for the assumption that it may include – in the future – not only the personal data of persons directly interacting with EUSPA, ESA and the service providers related to the Copernicus programme, but also satellite, EO, geolocation (GALILEO) and telecommunication data which, as a result of appropriate processing or by reason of their specific characteristics, are such as to take on the typical characteristics of personal data as set out in Art. 4 of Regulation (EU) 2016/679 (also known as GDPR).

The European Union has therefore shown that it is well aware that any kind of satellite data, is capable of damaging people's privacy by adopting an approach to monitor and limit the dissemination of EO data. However, as interesting as the EU framework is, it should not be forgotten that it applies to European space policies, so it does not apply to private companies.

4. A combination of licensing procedures with privacy assessment?

Given what has been said in the preceding paragraphs, it is clear that there is a need to innovate the regulatory framework and the approach in general.

Therefore, the following questions will be addressed below: when can EO data become personal data? When is the highest level of privacy risk reached?

[30] Regulation (EU) No 377/2014 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0377.
[31] Regulation (EU) 2021/696 - https://eur-lex.europa.eu/eli/reg/2021/696/oj.

How could privacy verification be reconciled with preparatory activities for obtaining authorisations to operate in space?

4.1. When can EO data become personal data?

Regarding the first two questions, in order to verify whether EO data are capable of becoming personal data, it will be necessary to analyse the following elements on a case-by-case basis: (1) the type of sensor; (2) the spatial resolution of the sensor; (3) the revisiting time of the satellite or satellite constellation; 4) the possibility of combining them with other data, including data from other satellite sensors and other types of data (e.g. cadastral data); and (5) the level of dissemination and the procedures adopted to allow access to EO data.

Indeed, while it is true that there is a plurality of sensors currently used for Earth observation, it is equally true that only a few of these are capable of producing images perceived as such by us. If one looks at the images produced by IR sensors[32], it is difficult to perceive anything other than differences in temperature or in the absorption of infrared radiation. It follows that only certain types of sensors, such as optical sensors (which immediately produce true images) or SAR sensors (whose data lead to the creation of 'images'), are currently capable of producing data that can be used "immediately". Indeed, it is with these sensors that it is possible to distinguish buildings, moving vehicles and, in the near future perhaps, people.

The second element, the spatial resolution of a sensor, is in turn influenced by three different factors: 1) the technological development - already mentioned - on the ability to acquire increasingly better-defined images; 2) the positioning of an EO satellite at a lower orbit than usual (in which case it is the greater proximity to the subject to be imaged that allows for better-defined images); 3) the possibility of combining several images of equal resolution of the same area into a single image of better quality. On point 1), I will not add anything, but as far as factor 2) is concerned, it is necessary to point out that the recent licence (Tier 3) assigned to Albedo envisages precisely the use of EO satellites placed in VLEO orbit[33], i.e. at an altitude between 250 and 450 km, and this is enough to make one imagine how it is possible to obtain even better images. As for the possibility of fusing several images together to improve their quality, this is already a reality in consumer products (think of Olympus cameras, now OM System, equipped with a Hi Res Shot mode based on sensor displacement), so it was only a matter of time before the same concept was applied to much 'heavier' data, such as that produced by satellites[34].

[32] Earthdata-NASA, "Seeing Earth in a New Light", https://www.earthdata.nasa.gov/learn/articles/earth-ir-sensing.
[33] T. Hitchens, "Albedo catches Space Force eyes with ultra-high fidelity imagery from very low satellites", www.breakingdefense.com, April 2023.
[34] EUSI, "15cm HD imagery", https://www.euspaceimaging.com/15-cm-hd/. You can get the data sheet about Maxar imageri at https://www.euspaceimaging.com/15-cm-hd-imagery-by-maxar/. See also F. D. Javan, F. Samadzadegan, S. Mehravar, A. Toosi, R. Khatami, A. Stein, "A review of image fusion techniques for pan-sharpening of high-resolution satellite imagery", in ISPRS Journal of Photogrammetry and Remote Sensing, Vol. 171, 2021, 101-117.

The third element, then, is as important as any of the others. This is because, in order to have the most accurate data possible, it is (usually) not sufficient to have very high-resolution images of a given area. It is also necessary to have several images, staggered in time, of that same area in order to perceive the changes in it. It is in this sense that, for example, Maxar has planned to form a constellation of satellites capable of providing 15 daily revisits of a given area[35].

The fourth element, then, is particularly critical. We are currently in the era of big-data, i.e. in a historical period in which the fusion of data of different origins and types is now an established practice[36]. Therefore, making an assessment of the possibility of obtaining the complete picture of a data area through these practices is an essential element for a correct assessment of privacy risk.

The last element, i.e. the level and procedures of EO data dissemination, is only relevant if taken into account in conjunction with the previous elements. If there is a (potentially privacy-impairing) combination of the elements considered above, then the lesser or greater dissemination of EO data may be the decisive criterion for deciding whether or not there is a privacy risk in the concrete case under consideration. Below is an example to better render the concept (Fig. 1).

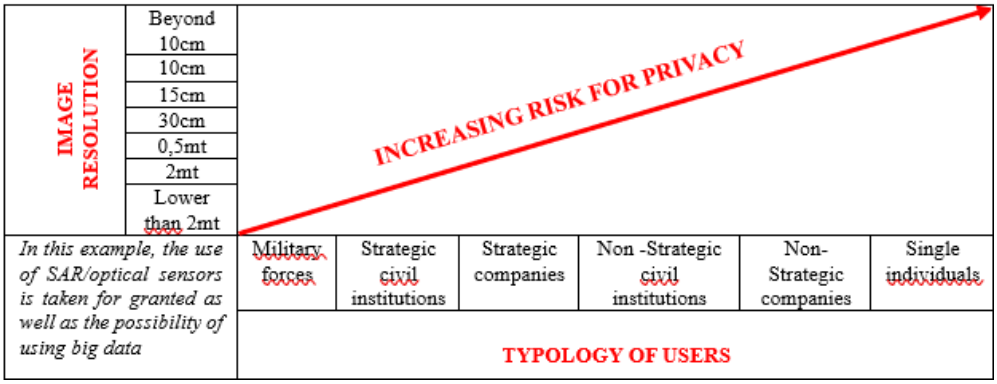


Fig. 1 - the relationship between dissemination and all other criteria

As can be seen, the risk arising from EO data, taking for granted the use of precise sensors and the possibility of exploiting big data, increases not only as the resolution of the images increases, but above all as the level of dissemination of possible users increases, dividing these into military forces, strategic civil institutions (such as civil defence, health, police forces, disaster relief), strategic companies (transport, energy, primary resources, telecommunications) and then non-strategic civil institutions and companies, and finally individuals. In fact, one could even divide that empty space within the table into four 'risk zones'. Well, any combination involving the dissemination to non-strategic civilian institutions, non-strategic companies

[35] Satellite Imaging Corporation, "WorldView Legion Satellite Constellation (30cm)", https://www.satimagingcorp.com/satellite-sensors/worldview-legion-satellite-constellation/.

[36] L. Zhao, X. Zhou and G. Kuang, "Building detection from urban SAR image using building characteristics and contextual information", in EURASIP Journal on Advances in Signal Processing, 2013 (56). J. D. Wegner, U. Soergel, R. Haensch and A. Thiele, "Fusion of high-resolution InSAR data and optical imagery for building detection using Conditional Random Fields", 8th European Conference on Synthetic Aperture Radar, Aachen, Germany, 2010, 1-4.

and individuals of EO data with a resolution of 15cm/pixel or better would fall within the maximum risk zone indicated by the red area (Fig. 2).

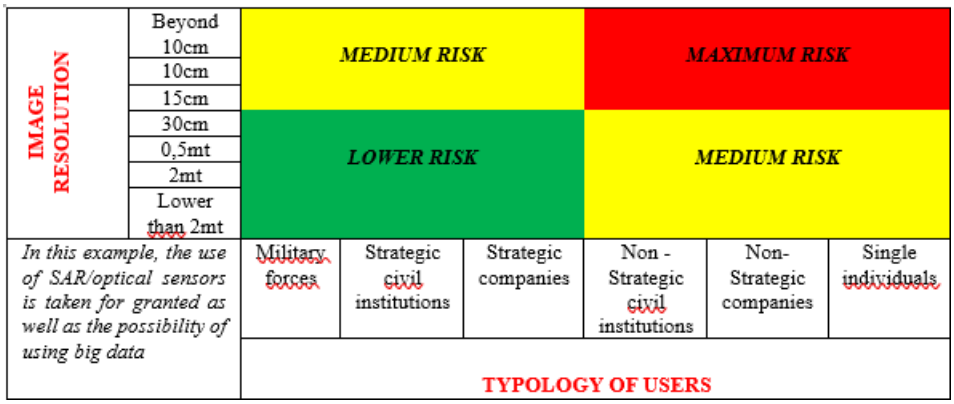


Fig. 2 - a variant of the previous table

It follows, therefore, that one of the most relevant criteria is the extent of EO data dissemination.

4.2. A first hypothesis: combining evaluation for ITU licences with privacy protection.

The evaluation outlined above is particularly complex, so it must be 'triggered' upon the occurrence of some precise precondition. This could be done by creating a link between the activities aimed at obtaining authorisations for space operations and those aimed at verifying data protection compliance.

For example, consider that operating a satellite requires a radio frequency link between the satellite itself and the control centre, which can be operated using a precise radio frequency.

To do this, however, it is necessary to obtain a special licence from the International Telecommunication Union (ITU), which deals with the allocation of radio frequencies. In fact, the radio spectrum is to be regarded as a finite good, not as an asset to which anyone who applies for it has unlimited access. Normally, relations with the ITU are taken care of by the same body that issues, at national level, the licences to operate a satellite (in the United States, in fact, it is NOAA that deals with this[37]).

So, let us assume that a company applies for licences (including ITU licences) to operate an EO satellite with particularly high resolutions. In such a case, the licensing body would have to immediately liaise with the privacy protection body. While the former would verify compliance with the national security and technical design requirements of the satellite, the latter would carry out a privacy compliance check with regard to the dissemination and processing of EO data.

At the same time, it should be borne in mind that the use of SAR sensors itself requires a precise licence due to the physical principle that characterises

[37] NOAA, "Radio Frequency Management", https://www.noaa.gov/information-technology/ocio-programs/radio-frequency-management. See also ITU Radio Regulations Articles, Edition of 2020.

the operation of a 'radar', so much so that the ITU classifies it as 'active sensing', in contrast to the 'passive sensing' implemented with normal optical sensors. In fact, on p. 137 of the ITU-RRs (Edition of 2020) there is a table with the allocations of frequencies between 8,500 and 10,000 MHz, i.e. that part of the radio spectrum known as the 'X Band', which is particularly prized for the resolution of the images that are generated. Well, the fact that a company applies for an X-Band licence could itself be a prerequisite for initiating a privacy check on single companies. Similarly, should the opportunity arise to use other different radio frequencies (although physical limits, such as those due to atmospheric absorption, must be considered), should they provide even sharper images than those obtainable in the X-band, then a joint check by the national security (and space) authority and the privacy authority would again be 'triggered'.

5. Conclusions.

It is well known that EO data are essential in the current context[38], so much so that an open access policy is being pursued[39]. Yet, the democratisation of space and data has shown how EO data can become (in the future) personal data, although this has only recently emerged in academic research[40]. It is therefore necessary to adopt 'shutter control' type systems[41], but adapted from the military to the civil sphere, so as to limit the dissemination of certain types of EO data only within specific institutional or corporate environments, following a casuistic analysis as outlined above. Such limitations in dissemination could also be added to the use of EO data processing systems that precede dissemination and are in line with privacy protection[42].

[38] M. Obersteiner, J. Balkovič, H. Böttcher et al., "The Value of Global Earth Observations", in Satellite Earth Observations and Their Impact on Society and Policy (Masami Onoda • Oran R. Young, 2018), pp. 137-141.
[39] J. Aschbacher, "ESA's Earth Observation Strategy and Copernicus" in Satellite Earth Observations and Their Impact on Society and Policy (Masami Onoda and Oran R. Young, Editors), 2018, 81-85.
[40] C. Santos and L. Rapp, "Satellite Imagery, Very High-Resolution and Processing-Intensive Image Analysis: Potential Risks Under the GDPR", in Air and Space Law. 2019/44, pp. 275-295. ESPI, "Current Legal Issues for Satellite Earth Observation: Treaty Verification and Law Enforcement Through Satellite Observation, Privacy Conflicts from High Resolution Imaging", Report 25, August 2010.
[41] D.F. Dumaris Sitanggang, "International Law Analysis of The Restrictions Imposed on Remote Sensing Satellite Through Shutter Control", MIMBAR HUKUM Vol. 30, no. 2, (Halaman, June 2018), pp. 389-406.
[42] M. Alkhelaiwi, W. Boulila, J. Ahmad, A. Koubaa, M. Driss, "An Efficient Approach Based on Privacy-Preserving Deep Learning for Satellite Image Classification", Remote Sens. vol. 13, no. 11, 2221, Jun. 2021.

Ferretti F, 'Human enhancement ed identità genetica dell'embrione' (2024) 1 EJPLT, 231-251.
DOI: https://doi.org/10.57230/EJPLT241FF

EJPLT
ISSN 2704-8012



Human enhancement ed identità genetica dell'embrione

Human enhancement and genetic identity of the embryo

FRANCESCA FERRETTI
Ph.D. (c) in Civil Law and Constitutional Legality
Università degli Studi di Camerino

Abstract

Gli interventi di editing genetico eseguiti con la tecnica CRISPR-Cas9 aprono a scenari migliorativi per la salute umana, ma presentano criticità non trascurabili, a partire dalle definizioni giuridiche di salute e malattia, fino alla configurabilità di un diritto alla «non (arbitraria) manipolazione genetica» e all'eventuale risarcimento di una sua lesione. Sotto il profilo regolatorio, si suggerisce l'impiego di un multi-level risk-based approach che individui puntuali limiti per interventi di genome editing vietati o ad alto rischio.

The genetic editing operations carried out with the CRISPR-Cas9 technique open up improvement scenarios for human health, but present not negligible criticalities, starting from the legal definitions of health and disease, up to the configurability of a right to «not (arbitrary) genetic manipulation» and any compensation for his injury. From the regulatory point of view, it is suggested the use of a multi-level risk-based approach that identifies specific limits for genome editing interventions that are prohibited or at high risk.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: editing genetico; human enhancement; linea germinale; identità genetica; salute *vs* malattia.

Sommario. 1. Introduzione. Editing genetico e tecnica CRISPR/Cas9. – 2. Il quadro normativo di riferimento. – 3. *Somatic* vs *Germline* editing e l'incerto confine distintivo. – 4. Il potenziamento umano tra salute e malattia. – 5. *Editing* genetico e diagnosi genetica pre-impianto. – 6. Identità genetica: diritto al "futuro aperto" o diritto "a non nascere se non (arbitrariamente) modificato"? – 7. Riflessioni conclusive: tentativi di strategie definitorie e *risk-based approach*.

1. Introduzione. Editing genetico e tecnica CRISPR/Cas9.

Lo scorso 20 ottobre 2022 si è svolta – in modalità virtuale e grazie all'organizzazione della società statunitense Synthego[1] – la terza edizione del "*World Crispr Day*", la giornata internazionale dedicata allo studio dell'editing genetico attraverso l'uso dell'omonima tecnica. Sempre nell'anno 2022 si è festeggiato il decorso del primo decennio di ricerche intorno a questa metodica, avviate nel 2012 grazie all'ormai noto studio pubblicato sulla rivista "*Science*", che è valso alle due scienziate Emmanuelle Charpentier e Jennifer Doudna il Premio Nobel per la Chimica nel 2020, per lo sviluppo di un metodo di editing genomico basato su CRISPR[2].

Gli interventi di editing genetico, volti ad introdurre, modificare o sostituire una sequenza di DNA all'interno di un sito specifico, sono effettuati attraverso endonucleasi ingegnerizzate, cioè enzimi di restrizione progettati per recidere la struttura a doppia elica del DNA umano (cd. *double-stranded breaks*, DSBs). A seguito della rottura del filamento, all'interno della cellula possono attivarsi due meccanismi diversi di riparazione: l'unione non omologa (*non-homologous and joining*, NHEJ) e la ricombinazione omologa (*homologous directed repair*, HDR). Il primo procedimento, in cui le due estremità sono tenute in stretta prossimità a poi riunite attraverso la ligasi, è tanto più rapido quanto più impreciso, ed è spesso causa di aberrazioni cromosomiche e mutazioni del gene coinvolto, determinanti la perdita di funzionalità dello stesso (cd. *knock-out*); nel secondo caso, dopo la nucleasi del filamento, viene inserito, all'interno della sequenza danneggiata, un frammento di DNA esogeno che lega gli estremi separati (cd. *knock-in*).

Sotto il profilo tecnico, a seconda del tipo di nucleasi utilizzata (cioè, in base agli enzimi impiegati per scindere gli acidi nucleici, quali DNA o RNA), è possibile distinguere tra: nucleasi *zincfinger* (ZFN), *nucleasi Transcritpion activator-like effector* (TALEN) e nucleasi guidate da RNA, caratterizzate da brevi ripetizioni palindrome raggruppate e separate ad intervalli regolari (*clustered regularly*

[1] Per informazioni sull'iniziativa, sia consentito il rinvio al sito ufficiale dell'evento e a quello della società, rispettivamente: https://www.worldcrisprday.com e https://www.synthego.com/blog/world-crispr-day-2022-recap.

[2] M. JINEK, K. CHYLINSKI, *et al.*, *A Programmable Dual-RNA–Guided DNA Endonuclease in Adaptive Bacterial Immunity*, in *Science*, 2012, Vol. 337, 816-821.

interspaced short palindromic repeats, CRISPR)[3]. Mentre i primi due metodi (ZFN e TALEN) richiedono un'attività di programmazione personalizzata in base alla sequenza di DNA che si intende correggere, nelle procedure del terzo tipo, tra le quali è compresa tecnica CRISPR-Cas9, questo procedimento non è necessario. La tecnica da ultimo citata, definita "*the Breakthrough to Genome Editing*[4]" si avvale dell'enzima Cas9, che viene condotto verso il punto preciso da recidere dall'RNA, senza alcuna personalizzazione dell'operazione. In questo modo, la forbice molecolare (*molecular scissors*) della CRISPR-Cas9 riesce, più agevolmente e con un livello di rendimento maggiore, ad individuare, eliminare o sostituire porzioni di genoma in cui è presente un'alterazione genetica[5]. Queste operazioni possono essere eseguite sia *in vivo*, cioè direttamente sul corpo del paziente, senza estrarre le cellule dalla loro collocazione, sia *ex vivo*, cioè prelevando prima le cellule dal corpo, intervenendo su di esse e reintroducendole successivamente.

Agli indubitabili vantaggi offerti da questa tecnica corrispondono tuttavia altrettanti rischi non trascurabili, rappresentati dalle modifiche non intenzionali (*off-target*) e dal mosaicismo, che, ad oggi, ne impediscono il trattamento generalizzato in ambito medico e nei confronti degli esseri umani[6]. Anche laddove questi impedimenti tecnici fossero risolti, rimarrebbero comunque aperte alcune rilevanti questioni di carattere etico-giuridico[7], di cui si dirà nel prosieguo della trattazione (v. *infra* para 4 e 6).

Tra le sperimentazioni più recenti dell'editing genetico sugli esseri umani, merita di essere ricordato lo studio clinico di EBT-101, una potenziale terapia contro l'HIV: la *Food and Drug Administration* (Fda), l'ente regolatorio statunitense, ha autorizzato nel 2021 la sperimentazione di fase 1/2 di questa ricerca, sviluppata da Kamel Khalili e il suo gruppo di ricercatori della *Lewis Katz School of Medicine* della *Temple University di Philadelphia* (Usa)[8].

Gli interrogativi tecnici, etici e giuridici aumentano laddove le operazioni di editing genetico abbiano ad oggetto non individui già viventi e formati, ma gameti ed embrioni, come è accaduto durante la prima applicazione di tale tecnica sul DNA umano: il 18 aprile 2015 un gruppo di scienziati della Sun Yat-sen University di Guangzhou ha annunciato di averla utilizzata su 86 embrioni umani per correggere la mutazione genetica causa della beta-talassemia[9]. Ed

---

[3] La classificazione è ripresa da C. IAGNEMMA, *L'editing genetico: una sfida (anche) normativa*, in *Riv. It. Med. Leg.*, 2019, IV, 1309-1318. Per approfondimenti, v. anche T. GAJ, C.A. GERSBACH, C.F. BARBAS, *ZFN, TALEN, and CRISPR/Cas-based methods for genome engineering*, in *Trends Biotechnol*, 2013, VII, 397-405.

[4] M. MC NUTT, *Breakthrough to Genome Editing*, in *Science*, 2015, Vol. 350, 1445-1448.

[5] Sul tema, si vedano, *ex multis*, S.P.B VAN BELJOUW, J. SANDERS, A. RODRÍGUEZ-MOLINA, *et al.*, *RNA-targeting CRISPR–Cas systems,* in *Nat Rev Microbiol*, 2023, XXI, 21–34; I. GOSTIMSKAYA, *CRISPR-Cas9: A History of Its Discovery and Ethical Considerations of Its Use*, in *Genome Editing. Biochemistry (Mosc)*, 2022, VIII, 777-788; S.S. WU, Q.C. LI, C.Q YIN, W. XUE, C.Q. SONG, *Advances in CRISPR/Cas-based Gene Therapy*, in *Human Genetic Diseases. Theranostics.* 2020, X, 4374-4382.

[6] Sui rischi dell'editing genetico, v. M. SCHACKER, D. SEIMETZ, *From fiction to science: clinical potentials and regulatory considerations of gene editing*, in *Clinical Trans. Med.*, 2019, 27-41; Y. YANG, Y. HUANG, *The CRIPSR/Cas gene- editing system: an immature but useful toolkit for experimental and clinical medicine*, in *Animal Models and Exp. Med.*, 2019, 5-8.

[7] P. REFOLO, V. L. PASCALI, A. G. SPAGNOLO, *Editing Genetico: Nuova Questione Bioetica?,* in *Medicina E Morale*, Vol. 66, III, 291-304.

[8] Per alcuni sia pure provvisori, ma incoraggianti risultati, si rinvia a *Study of EBT-101 in Aviremic HIV-1 Infected Adults on Stable ART*, disponibile su: https://clinicaltrials.gov/ct2/show/NCT05144386.

[9] P. LIANG, Y. ZU, X. ZHANG et al., *CRISPR/Cas9 mediated gene editing in human tripronuclear zygotes*, in *Protein & Cell*, 2015, 363 ss.

ancora, è noto il caso, avvenuto sempre in Cina, della nascita, a fine 2018, delle gemelle Lulu e Nana, geneticamente immuni all'HIV grazie alla disattivazione della proteina CCR5 per effetto di un intervento di *editing* genetico ad opera dello scienziato He Jankui[10]. Nel 2019, in Russia, sull'esempio del collega cinese, il biologo molecolare Denis Rebrikov ha concentrato i suoi studi su ovuli donati da una donna udente, per offrire i suoi risultati a cinque coppie russe affette da sordità e disposte a sottoporsi a procedure Crispr; in particolare, intervenendo sul gene GJB2, correlato alla sordità, sarebbe possibile eliminare il difetto ed ottenere così embrioni modificati e sani[11].

Prima di delineare con più precisione le differenze tra l'applicazione dell'*editing* all'individuo già formato (*somatic editing*) ovvero all'embrione (*germline/hereditable editing*) cui si è fatto cenno, sembra opportuno fornire una breve ma esaustiva disamina del quadro regolatorio vigente, al fine di esaminare le problematiche secondo una prospettiva tecnica non solo medico-scientifica, ma anche giuridica.

2. Il quadro normativo di riferimento.

In ambito sovranazionale, la "Dichiarazione Universale sul Genoma Umano", adottata dall'Unesco nel 1997, definisce, all'art. 1, il genoma umano come la *fundamental unity* della specie umana, espressione al contempo della *inherent dignity* e *diversity* di ciascun essere umano, e dunque, the *heritage of humanity*. Il successivo art. 11 tuttavia, nel vietare in generale le pratiche considerate contrarie alla dignità umana, indica, a titolo esemplificativo, solo la clonazione umana, senza menzionare le modifiche genetiche[12]; esse sono però richiamate espressamente dall'art. 24, che attribuisce all'*International Bioethics Commettee* (IBC) il compito di individuare le pratiche contrarie alla dignità umana, tra cui annovera anche gli interventi sulla linea germinale[13]. Lo stesso IBC ha confermato questa posizione nel 2003, e ha valutato, nel 2015,

[10] S. Bonomelli, *Gene Editing embrionale: il vaso di Pandora è stato scoperchiato? Riflessioni a margine del caso di Jiankui He*, in *Riv. Biodiritto*, 2019, III, 67 ss.

[11] Sempre in rapporto alla sordità, si ricorda il noto caso della coppia di genitori sordi che aveva manifestato il desiderio di un figlio dotato della loro stessa caratteristica, considerata non come una patologia o un difetto, ma come un dato peculiare, identitario, ed unico. Sul punto, v. G. Baldini, *Eugenetica alla rovescia: selezione embrionaria per avere un figlio non udente*, in F. Giunta, P. Funghi (a cura di), *Medicina, bioetica e diritto. I problemi e la loro dimensione normativa*, Milano, 2012, 32-38.

[12] *Universal Declaration on the Human Genome and Human Rights*, 11 novembre 1997, adottata in seno alla General Conference of the United Nations Educational, Scientific and Cultural Organization at its twenty-ninth session. In particolare, l'Art. 1 così dispone: "The human genome underlies the fundamental unity of all members of the human family, as well as the recognition of their inherent dignity and diversity. In a symbolic sense, it is the heritage of humanity". Ai sensi dell'art. 11, invece, "Practices which are contrary to human dignity, such as reproductive cloning of human beings, shall not be permitted. States and competent international organizations are invited to co-operate in identifying such practices and in taking, at national or international level, the measures necessary to ensure that the principles set out in this Declaration are respected".

[13] *Universal Declaration on the Human Genome and Human Rights*, cit., Art. 24: "The International Bioethics Committee of UNESCO should contribute to the dissemination of the principles set out in this Declaration and to the further examination of issues raised by their applications and by the evolution of the technologies in question. (…) It should make recommendations, (…) in particular regarding the identification of practices that could be contrary to human dignity, such as germ-line interventions.

l'opportunità di intervenire con una moratoria volta a precludere l'impiego di tecniche di intervento sulla linea germinale[14].

Nel continente europeo, già negli anni Ottanta l'Assemblea Parlamentare del Consiglio d'Europa aveva adottato tre raccomandazioni, rispettivamente nel 1982, 1986 e 1989, nel tentativo di fornire una prima regolamentazione all'editing genetico. L'iniziale atteggiamento prudente, ma ispirato all'apertura verso le possibilità dischiuse dalle nuove tecnologie genetiche presente nei primi due atti [15] ha conosciuto un brusco cambio di rotta con la terza raccomandazione, che ha vietato radicalmente, qualsiasi forma di terapia genica germinale, senza fornire, al riguardo, alcuna motivazione esaustiva[16].

Questo atteggiamento di diffidenza si è cristallizzato nella "Convenzione sui diritti dell'uomo e la biomedicina", approvata ad Oviedo nel 1997, attualmente l'unico strumento internazionale giuridicamente rilevante in materia di bioetica per gli Stati Membri del Consiglio d'Europa che l'hanno ratificata[17]. Tra di essi non figurano né la Germania né, tecnicamente, l'Italia, a causa del mancato perfezionamento del processo di ratifica regolato dall'art. 80 Cost., come chiarito anche dalla Corte costituzionale, secondo la quale poiché "lo Stato italiano finora non ha depositato lo strumento di ratifica nei suoi confronti la Convenzione non è entrata in vigore[18]"; l'Italia, infatti, si è limitata ad adottare la legge n. 145/2001 di autorizzazione alla ratifica, omettendo di compiere l'adempimento successivo [19] . Nonostante la non vincolatività della Convenzione, essa non è del tutto priva di valore giuridico, secondo la giurisprudenza, poiché, anche se "essa dovrà cedere di fronte a norme interne contrarie, ma può e deve essere utilizzata nell'interpretazione di norme interne al fine di dare a queste una lettura il più possibile ad essa conforme[20]".

---

[14] International Biotethics Committee (IBC), *Report of the IBC on pre-implantation genetic diagnosis and germ-line intervention*, 2003, 12: "(…) The Universal Declaration on the Human Genome and Human Rights states in Article 24 that "germ-line interventions could be contrary to human dignity" and there is no reason to date to modify this position"; ID., *Report of the IBC on Updating Its Reflection on the Human Genome and Human Rights*, 2015, 14: "Due to uncertainties on the effect of germline modification on the future generations, such interventions have been strongly discouraged or legally banned in many countries"; 28: "the IBC (…) recommends a moratorium on genome editing of the human germline. There is no medical or ethical argument to support the former".

[15] Council of Europe Parliamentary Assembly, Recommendation n. 934 (1982), *Genetic Engineering*, 6 gennaio 1982; Council of Europe Parliamentary Assembly, Recommendation n. 1046 (1986), *Use of human embryos and foetuses for diagnostic, therapeutic, scientific, industrial and commercial purposes*, 24 settembre 1986.

[16] Council of Europe Parliamentary Assembly, Recommendation n. 1110/1989, *Use of human embryos and foetuses in scientific research*, 2 febbraio 1989; La parte finale della lettera G, punto 18 dell'appendice della raccomandazione in discorso chiarisce che "*Any form of therapy on the human germinal line shall be forbidden*".

[17] *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*, approvata dal Consiglio d'Europa, Oviedo, 4 aprile 1997.

[18] Corte Cost., Ord. n. 282/1983 disponibile su: www.giurcost.org: "Neppure l'eventuale declaratoria di illegittimità costituzionale della menzionata legge, per mancata fissazione del termine per la ratifica, potrebbe rendere vincolante per lo Stato italiano la Convenzione internazionale - con le conseguenti operatività della suddetta legge e applicabilità del menzionato art. 53 della Convenzione da parte del giudice a quo - perché tali effetti derivano esclusivamente dal deposito dello strumento di ratifica".

[19] In argomento, v. F. G. PIZZETTI, *La delega per l'adattamento dell'ordinamento italiano alla Convenzione di Oviedo tra problemi di fonti ed equilibri istituzionali: un nuovo "cubo di Rubik"?,* in *Rass. parl.*, 2007, III, 585-608; C. CASONATO, T. E. FROSINI, T. GROPPI, *Introduzione. L'atipicità del panorama italiano in tema di biodiritto*, in *Diritto pubblico comparato ed europeo*, 2007, IV, 1650-1652.

[20] Cass., 16 ottobre 2007, n. 21748, in *Foro It.*, Vol. 130, XI, 2007, 3025-3026.

L'art. 13 della già menzionata Convenzione stabilisce che sono consentiti interventi sul genoma solo per scopi preventivi, diagnostici o terapeutici, e solo se non abbiano come scopo principale l'introduzione di modifiche nel genoma dei discendenti[21]". Il tenore letterale della disposizione ha dato adito a qualche dubbio interpretativo: dal momento che il divieto ha ad oggetto solo le modifiche attutate "allo scopo" (specifico) di mutare il genoma delle generazioni future, potrebbe sostenersi che sarebbero invece consentite quelle operazioni eseguite a fini di cura, nelle quali l'ereditarietà della modifica genetica rappresenta solo un effetto collaterale ineliminabile, secondario e non voluto[22]. Questa ricostruzione interpretativa, pur ipotizzabile in astratto, contrasta, secondo l'opinione maggioritaria[23] – ma non unanime[24] – con lo scopo della norma, volta ad introdurre un divieto di terapia genica germinale in termini assoluti e non meramente contingenti.

Più di recente, il Consiglio d'Europa, pur ricordando che l'impiego dell'editing genomico oltrepasserebbe i confini dell'"eticamente inviolabile[25] ", ha innovativamente considerato la possibilità di emendare l'art. 13 mediante il procedimento descritto dall'art. 32 della Convenzione e previo coinvolgimento della popolazione attraverso apposite consultazioni pubbliche[26].

La Carta dei diritti fondamentali dell'Unione Europea non contiene invece previsioni specifiche in tema di editing genetico germinale: la disposizione più

---

[21] Art. 13, *Convention on Human Rights and Biomedicine*, cit.: "An intervention seeking to modify the human genome may only be undertaken for preventive, diagnostic or therapeutic purposes and only if its aim is not to introduce any modification in the genome of any descendants".

[22] Nuffield Council on Bioethics, *Genome editing and human reproduction: social and ethical issues*, 2018, 117: "On its face, Article 13 of the Oviedo Convention appears to prohibit heritable genome editing interventions (although not without some ambiguity)" ed ivi, nota 423: "It might be argued that Article 13 of the Oviedo Convention will not apply to all heritable genome editing, at least not to some genome editing carried out for the avoidance of certain genetic conditions. This is because, in such a case, the editing of embryos would be carried out for a preventative reason and, although it would introduce a modification into the genome of potential descendants (i.e. any children of the people those embryos may become), this would not be the aim of the procedure (any more than the use of radiotherapy to treat a cancer has the aim of disrupting the DNA of a patient's gametes or of making them infertile. The Article refers to the aims of the procedure precisely in order not to exclude such treatments, as the explanatory report makes clear)".

[23] In questo senso, D'Andrea, *Ricerca scientifica, principio di precauzione, eugenetica e tutela della salute: la regolamentazione della terapia genica germinale nell'art. 13 della Convenzione di Oviedo*, Relazione svolta al convegno L'impatto delle innovazioni biotecnologiche sui diritti della persona, Trento, 17-18 maggio 2012, secondo il quale "Il divieto contenuto nell'art. 13 della Convenzione è nato proprio per essere irreversibile: la Convenzione di Oviedo è una moderna carta dei diritti e, pur non essendo stata solennemente dichiarata nel corso di un particolare momento di transizione storico-politica di un ordinamento giuridico, per sua natura ha l'ambizione di fissare principi e disposizioni validi da qui in avanti". v. Per la circostanza che le carte dei diritti sono sempre "*sub specie eternitatis*", C. Mortati, *Costituzione (Dottrine generali)*, in *Enc. Dir.*, XI, Milano, 1962, 146, 185.

[24] Per un'opinione possibilista, v. I. De Miguel Beriain, E. Armaza Armaza, A. Duardo Sánchez, *Human germline editing is not prohibited by the Oviedo Convention: An argument,* in *med. L. Intern.,* 2019, XX, 1-7, che rispetto agli interventi sulla linea germinale, chiariscono che "it was the Committee's intention to exclusively impede its clinical application due to the risks involved. Moreover, the Committee even advocated that this prohibition should be periodically revised according to the state of the art (...). Even if it was never put into practice, this statement reinforces the idea that no general ban on germ line editing was ever intended. (…) The parties to the Convention never intended to instigate a ban".

[25] Council of Europe Parliamentary Assembly, Recommendation n. 2115/2017, *Deliberate germ-line editing in human beings would cross a line viewed as ethically inviolable*, 12 ottobre 2017.

[26] Il fatto che la Convenzione di Oviedo preveda espressamente un procedimento per la propria modifica "is implicitly to accept that the line related to genome-editing that can be inherited may not in fact be 'inviolable' at all": Cfr. J. Montgomery, *Modification of the human genome: Human rights challenges raised by scientific and technological developments*, in *Council of Europe, 20th Anniversary of the Oviedo Convention: Relevance and Challenges. Proceedings*, 2017, 60-72.

rilevante è rappresentata dall'art. 3, rubricato "Diritto all'integrità della persona", che, al secondo comma, si limita a vietare le pratiche eugenetiche, il cui scopo sia la selezione delle persone[27]. Il primo problema sollevato dall'art. 3 deriva dall'esegesi del termine "persona", che, se interpretato estensivamente, potrebbe ricomprendere anche la vita umana prenatale e le generazioni future, nei cui confronti si produrrebbero gli effetti degli interventi genetici a livello germinale; in questo contesto è preferibile, tuttavia, far decorre la tutela della vita e dei diritti ad essa correlati dal momento della nascita, e conferire al termine un'accezione più ristretta[28].

Inoltre, la finalità specifica della norma è quella di precludere l'organizzazione e l'attuazione di programmi di selezione che comportino, per esempio, campagne di sterilizzazione, gravidanze forzate, matrimoni etnici obbligatori, atti considerati crimini internazionali dallo statuto della Corte penale internazionale adottato a Roma il 17 luglio 1998[29], senza che il divieto in esame si estenda anche agli interventi di editing genetico posti in essere su base volontaria, allo scopo di curare gravi malattie genetiche in un soggetto già esistente, o prevenirne l'insorgenza in individui non ancora nati, a seconda che l'intervento sia realizzato a livello somatico o germinale.

Per quanto riguarda la normativa nazionale, l'unico riferimento rilevante è rappresentato dall'art. 13 della legge 40/2004 sulla procreazione medicalmente assistita, il cui terzo comma vieta "ogni forma di selezione a scopo eugenetico degli embrioni e dei gameti, ovvero interventi che, attraverso tecniche di selezione, di manipolazione o comunque tramite procedimenti artificiali, siano diretti ad alterare il patrimonio genetico dell'embrione o del gamete ovvero a predeterminarne caratteristiche genetiche, ad eccezione degli interventi aventi finalità diagnostiche e terapeutiche, di cui al comma 2 del presente articolo". La norma, attraverso il richiamo alla diagnosi e alla terapia, introduce a livello legislativo la distinzione tra *treatment* ed *enhancement* (v. *infra*, para. 4), senza chiarirne esattamente la linea di confine.

Questa ambiguità genera dubbi di conformità anche rispetto al principio di determinatezza della norma penale, corollario del principio di legalità: questo aspetto viene in rilievo poiché il primo comma configura un delitto di sperimentazione sugli embrioni umani[30], la cui integrazione è tuttavia esclusa

---

[27] Articolo 3. Diritto all'integrità della persona. "2. Nell'ambito della medicina e della biologia devono essere in particolare rispettati: (…) il divieto delle pratiche eugenetiche, in particolare di quelle aventi come scopo la selezione delle persone".

[28] R. YOTOVA, *Report on Regulation. The Regulation on Genome Editing and Human Reproduction Under International Law*, in *EU Law and Comparative Law*, 2017, 1-61. Contra, A. FALCONE, *Biotecnologie e diritti fondamentali nel "trattato costituzionale europeo"*, in S. GAMBINO (a cura di), *Trattato che adotta una costituzione per l'Europa, costituzioni nazionali, diritti fondamentali*,, Milano, 2006, 396-397: "la previsione di un discrimine soggettivo e temporale che limiti ai soli nati la garanzia di tutela dell'integrità genetica non sarebbe coerente con la natura dei beni tutelati le cui violazioni espressamente punite nello stesso articolo – clonazione, manipolazioni eugenetiche, selezione eugenetica, commercializzazione di materiale genetico – sono suscettibili di essere realizzate prima ed a prescindere dalla nascita".

[29] *Spiegazioni relative alla Carta dei diritti fondamentali* (2007/C 303/02), 14 dicembre 2007.

[30] I commi 4 e 5 dello stesso articolo sanzionano severamente il delitto in esame. In particolare, il comma 4 stabilisce che "La violazione dei divieti di cui al comma 1 è punita con la reclusione da due a sei anni e con la multa da 50.000 a 150.000 euro. In caso di violazione di uno dei divieti di cui al comma 3 la pena è aumentata. Le circostanze attenuanti concorrenti con le circostanze aggravanti previste dal comma 3 non possono essere ritenute equivalenti o prevalenti rispetto a queste". Il comma 5, poi, aggiunge che "È disposta la sospensione da uno a tre anni dall'esercizio professionale nei confronti dell'esercente una professione sanitaria condannato per uno degli illeciti di cui al presente articolo".

quando ricorre la causa di giustificazione contenuta nel secondo comma e richiamata dal comma 3 lett. b), cioè quando l'agente ha eseguito la condotta perseguendo "finalità esclusivamente terapeutiche e diagnostiche", e "qualora non siano disponibili metodologie alternative". In dottrina è stato osservato che, "sebbene semanticamente e linguisticamente la causa di giustificazione risulti abbastanza chiara, il riferimento a finalità terapeutiche e diagnostiche come elementi descrittivi rende indeterminabile la norma da un punto di vista empirico. E ciò tanto più se si prende in considerazione che la formulazione della norma prevede anche l'uso del termine *finalità*, che potrebbe indurre l'interprete a far spazio, nel proprio processo ermeneutico, a riferimenti alla sfera delle intenzioni[31]".

A parere di chi scrive, la circostanza che l'unico dato normativo italiano in tema di *editing* genetico sia inserito in una legge in materia di procreazione implicitamente conferma che i profili di maggiore incertezza sotto il versante etico, giuridico e tecnico, che inevitabilmente coinvolgono ogni intervento sul genoma umano, si acuiscono e si moltiplicano in caso di interventi sulla linea germinale, dove vengono in rilievo gli ulteriori aspetti della tutela dell'embrione e delle generazioni future [32] cui le modifiche genetiche sarebbero trasmesse, con esiti imprevedibili a priori; questo secondo aspetto è stato spesso utilizzato come *catch-call argument* contro ogni possibile ipotesi di editing genetico germinale[33].

3. *Somatic* vs *Germline* editing e l'incerto confine distintivo.

Come già accennato alla fine del precedente paragrafo, le tecniche di editing, a seconda della cellula umana sulla quale intervengono, possono determinare modifiche alternativamente a livello somatico e a livello germinale[34]. Queste ultime coinvolgono non solo i gameti umani, quali ovuli e spermatozoi, le uniche cellule umane dotate di un corredo cromosomico aploide, ma riguardano anche le modifiche genetiche da effettuare in vitro su gameti ed embrioni.

Le terapie geniche somatiche consentono una modifica del DNA del paziente, senza incidere sulle cellule coinvolte nella procreazione: in questo modo, l'individuo trattato, pur liberato dalla patologia dalla quale risultava affetto, rischia comunque di trasmetterla alle generazioni successive. La terapia somatica è tradizionalmente più accettata rispetto a quella germinale,

---

[31] F. INSANGUINE, *Manipolazione genetica germinale e diritto. Una ricostruzione critica a partire dalla vicenda di He Jiankui*, in *Riv. Crit. Dir. Priv.,* IV, 2019, 595-618.

[32] Per alcune considerazioni sulla responsabilità (morale) nei confronti delle generazioni future, v. S. ZULLO, *Il ruolo dell'epigenetica tra il paradigma dell'identità e quello della responsabilità*, in *Ragion pratica*, 2015, ILV, 529-554.

[33] M. BAUMANN, *CRISPR/Cas9 genome editing – new and old ethical issues arising from a revolutionary technology*, in *Nanoethics*, X, 2016, 139-159.

[34] Un'ulteriore alternativa è rappresentata dal cd. editing epigenetico, in cui il DNA rimane intatto, ma si interviene sui meccanismi di accensione e di spegnimento dei geni che lo compongono, e dunque il gene responsabile della patologia può essere lasciato intatto, e le mancanze sono colmate in via indiretta, attraverso l'espressione di altri geni. J.C. IZPISUA BELMONTE et al*, In Vivo Target Gene Activation via CRISPR/Cas9-Mediated Trans-epigenetic Modulation*, in *Cell*, 2017, Vol. 14, 1495-1507; R.A.F. GJALTEMA, M. G. ROTS., *Advances of epigenetic editing,* in *Current Op. Chem. Biol.,* 2020, Vol. 57, 75–81.

poiché è ritenuta meno problematica della prima dal punto di vista etico, ed è assimilata, da taluni, ad un qualsiasi altro trattamento di cura sperimentale, sia pure non privo di rischi[35].

La distinzione tra modifiche somatiche e germinali, già nota in letteratura[36], è stata di recente richiamata all'interno di un documento dello STOA – *Panel for the Future of Science and Technology*, recante il titolo "*Genome editing in humans*" e pubblicato nel giugno 2022. Lo STOA ha avuto tuttavia cura di puntualizzare che, dal punto di vista regolatorio, l'uso di espressioni come "somatico vs germinale", "intervento di modifica genetica ereditabile" o "modifica dell'identità genetica" è considerato scientificamente superato, vago e suscettibile di interpretazioni contrastanti[37].

Anche in una prospettiva tecnico-scientifica, la distinzione non è così netta poiché, si legge ancora nel documento, "*somatic as well as germline applications may carry associated dangers*". Anzi, c'è anche chi sostiene che gli interventi genetici sulla linea somatica sarebbero addirittura più rischiosi di quelli effettuati sulla linea germinale[38]: eventuali fallimenti dell'intervento genetico germinale potrebbero essere più efficacemente controllati e risolti, attraverso lo scarto dell'embrione a seguito di DGP o l'interruzione volontaria di gravidanza[39].

L'esigenza di provvedere ad una delimitazione chiara e precisa tra le due operazioni è rafforzata anche dal tenore letterale della legislazione tedesca, che sul punto ha dato adito a qualche dubbio interpretativo. In generale, nell'ordinamento tedesco[40], la "legge sulla protezione degli embrioni" (*Embryonenschutzgesetz – ESchG*[41]) vieta qualsiasi forma di manipolazione genetica embrionale e l'utilizzo di cellule umane della linea germinale il cui patrimonio genetico sia stato modificato artificialmente (§ 5(1) e (2[42])). Per

---

[35] P. BORSELLINO, *Bioetica tra "morali" e diritto. Nuova edizione aggiornata*, Milano, 2018, 378-380; A. SANTOSUOSSO, *Diritto, scienza, nuove tecnologie,* Padova, 2016 129-133, secondo il quale la terapia genica somatica "è assimilabile a quella di un trapianto di organo o di tessuto"; M.H, PORTEUS, C.T. DANN, *Genome Editing of the Germline: Broadening the Discussion*, in *Molecular Therapy*, Vol. 23, VI, 2015, 981-982: "There is no controversy over the potential of curing patients by editing of somatic cells, and it is critical that the scientific community speak with a clear voice on this application".

[36] J.A. DOUDNA, S.H. STERNBERG, *A crack in creation. Gene editing and the unthinkable power to control evolution*, Boston, 2018,158: "Deciding what types of cells to target is one of the many dilemmas confronting researchers – should they edit somatic cells (…) or germ cells (…)? The distinction between these two classes of cells cuts to the hearth of one of the most heated and vital debates in the world of medicine today".

[37] European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA) *Genome editing in humans. A survey of law, regulation and governance principles*, PE 729.506, 2022, 5: "From a regulatory perspective, the use of qualifiers such as 'somatic versus germline', 'hereditable' genome editing, or 'modifying genetic identity', is considered scientifically outdated, vague and prone to differing legal interpretations".

[38] G. CHURCH, *Compelling Reasons for Repairing Human Germlines*, in NEJM, 377, XX, 2017, 1909-1911.

[39] R. RANISCH, *Germline genome editing versus preimplantation genetic diagnosis: Is there a case in favour of germline interventions?,* in *Bioethics*, Vol. 34, 2020, 60-69.

[40] Per un'analisi in prospettiva comparative, v. T. FALTUS *The Regulation of Human Germline Genome Modification in Germany*, in A. BOGGIO, C.P.R. ROMANO e J. ALMQVIST (a cura di), *Human Germline Genome Modification and the Right to Science: A Comparative Study of National Laws and Policies*, Cambridge, 2020.

[41] Gesetz zum Schutz von Embryonen (Embryonenschutzgesetz – EschG), Legge sulla protezione degli embrioni, 13 dicembre 1990.

[42] Traduzione in inglese fornita dal Robert Koch Institut, disponibile su: https://www.rki.de/SharedDocs/Gesetzestexte/Embryonenschutzgesetz_englisch.pdf, Section 5, Artificial alteration of human germ line cells. (1) Anyone who artificially alters the genetic information of a human germ line cell will be punished with imprisonment up to five years or a fine. (2) Likewise anyone will be punished who uses a human germ cell with artificially altered genetic information for fertilisation.

comprendere l'esatta portata del divieto in esame, è necessario fare riferimento alla § 8(3) dell'ESchG, che definisce cellule della linea germinale sia tutte le cellule che, a partire dall'ovulo e dagli spermatozoi, costituiranno il nuovo essere umano, sia, inoltre, la cellula uovo a partire dal prelievo o dalla penetrazione ad opera dello spermatozoo, fino al termine della fecondazione per fusione dei nuclei[43]. Nella fase iniziale dello sviluppo del feto, non è ancora chiaro quali cellule somatiche andranno a costituire la linea germinale dell'embrione, differenziandosi funzionalmente dalle altre; ne consegue che una modifica in questa fase così precoce e dai contorni non definiti potrebbe non ricadere nel divieto di cui al § 5[44].

Dalle precedenti considerazioni si evince come anche sotto l'aspetto scientifico, siano presenti dubbi e incertezze definitorie, che inevitabilmente riducono la chiarezza del quadro regolatorio del fenomeno. Il già citato Report dello STOA si mostra consapevole del valore delle definizioni, in termini di chiarezza, assenza di ambiguità, aderenza alle risultanze scientifiche. Non a caso, infatti, lo studio sottolinea l'importanza di "*harmonised*" e "*uniform*" definition, che facilitano la comparazione e l'adattamento tra normative nazionali, e aiutano la crescita e lo sviluppo del mercato interno dei prodotti e dei servizi della salute e del benessere. È altresì opportuno che la redazione delle definizioni avvenga in maniera tale da assicurare "*sustained correspondence with scientific knowledge*[45]".

4. Il potenziamento umano tra salute e malattia.

Altra distinzione non chiara a livello scientifico (prima che giuridico) è quella tra "*treatment*" e "*human enhancement*": questo secondo sintagma viene definito dallo STOA come "*not useful, vague, value-charged and difficult to enforce*". Da questa distinzione dipende la liceità o meni degli interventi di editing genetico, dal momento che l'art. 13 comma 3 lett. b) della L. 40/2004 sulla fecondazione assistita, vieta tutti le forme di alterazione del patrimonio genetico, "ad eccezione degli interventi aventi finalità diagnostiche e terapeutiche".

Per questa ragione, diventa essenziale l'individuazione di una linea di confine tra i concetti di trattamento e potenziamento, e – a monte – tra quelli di salute e malattia, solo apparentemente antitetici e facilmente distinguibili [46] .

[43] Section 8 Definition. "(1) Germ line cells, for the purpose of this Act, are all cells that lead of the egg and sperm cells to the resultant human being and, further, the egg cell from capture or penetration of the sperm cell until the ending of fertilisation by fusion of the nuclei".

[44] Il professor Jochen Taupitz evidenzia come, in questa fase e nei cd. "early embryos (…), it is difficult to say which cells will become germ line and which will become somatic cells, are legally controversial. In terms of definitions, germ line is not the same as embryo protection, and alterations to the germ line may be authorised or banned without protecting or harming an existing embryo"; cfr. *Call for a moratorium on germ line experiments in humans,* Healthcare industry BW, 2015, disponibile su: https://www.gesundheitsindustrie-bw.de/en/article/news/call-for-a-moratorium-on-germ-line-experiments-in-humans.

[45] European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA) *Genome editing in humans. A survey of law, regulation and governance principles*, cit., 5.

[46] Diversi autori rifiutano la distinzione tra terapia e potenziamento a causa della sua inutilità e della dubbia possibilità di distinguere i due profili secondo criteri oggettivi. Cfr. A.M. GOUW, *Challenging the Therapy/Enhancement Distinction in CRISPR Gene Editing*', in D. BOONIN (a cura di) *The Palgrave Handbook of*

L'incertezza definitoria è evidenziata anche dallo stesso Nuffield Council of Bioethics, secondo il quale, "*given the substantial 'grey area' between these two classes, this distinction is neither clear nor well understood, and it might also be unstable*[47]*"*.

Alla fine degli anni Settanta, il sociologo Andrew C. Twaddle ha esaminato in maniera sistematica la nozione di "malattia", ricostruendola, a seconda dei distinti approcci teorici, alternativamente come "*disease*", "*illness*", "*sickness*[48]". La prima dimensione (*disease*) corrisponde all'elemento oggettivo, cioè medico-biologico della malattia, che si indentifica in uno stato fisiologico alterato; la seconda dimensione della malattia (*illness*) coincide con l'elemento soggettivo, e descrive l'esperienza sensoriale di sofferenza percepita dal paziente; la terza prospettiva (*sickness*) invece è espressione della dimensione sociologica della malattia, ricca di implicazioni culturali e storiche, come rappresentazione sociale di un fenomeno che si svolge secondo le aspettative sociali e le istituzioni proprie di una determinata comunità. La ricostruzione individuata da Twaddle è stata condivisibilmente definita una triade, e non una tricotomia, poiché i tre termini non si escludono a vicenda, potendo bensì coesistere ed essere variamente combinati tra di loro[49].

A livello giuridico, la distinzione tra le condizioni di salute e malattia è stata resa problematica dal progressivo disancoramento della salute dalla sua tradizionale concezione, esclusivamente biologico-fisica ed oggettivamente valutabile. La salute era stata inizialmente letta in un'accezione "normativa", legata al rispetto di tradizionali standard predefiniti, in termini di corrispondenza dell'organismo a parametri biologici indicativi di un corretto e normale funzionamento. Tale impostazione si poneva tuttavia in evidente antitesi con quanto espresso dall'OMS, che, al contrario, aveva definito la salute quale "stato di completo benessere fisico, mentale e sociale e non semplice assenza di malattia o d'infermità [50]".

La distinzione in discorso ha delle ricadute pratiche anche in termini di allocazione delle spese sanitarie: solo gli interventi terapeutici sono erogabili attraverso il servizio sanitario nazionale (SSN), nel rispetto dei livelli essenziali di assistenza (LEA), mentre gli interventi di potenziamento sarebbero a carico del soggetto che sceglie di sottoporvisi[51].

Philosophy and Public Policy, Springer, 2018; D. GREENBAUM, L.Y. CABRERA (a cura di) *ELSI in Human Enhancement: What Distinguishes it from Therapy?*, in *Frontiers Media*, 2020.

[47] Nuffield Council on Bioethics, *Genome editing and human reproduction: social and ethical issues*, cit., 71. Già prima, nello stesso senso, v. International Biotethics Committee (IBC), *Report of the IBC on pre-implantation genetic diagnosis and germ-line intervention*, cit., 12: "in many considerations it also plays a role that a distinction between "therapeutic" purposes and "enhancement of normal characteristics" is far from being clear".

[48] A. Twaddle, *Disease, Illness and Sickness Revisited*", in Id., L. Nordenfelt, (a cura di) *Disease, illness and sickness: Three central concepts in the theory of health*, Linköping, 1993; 1-18. Vedi anche il commento di M.C. Amoretti, *Filosofia e medicina. Pensare la salute e la malattia*, Roma, 2015, 17-43.

[49] B. HOFMANN, *On the Triad Disease, Illness and Sickness*, in *Journal of Medicine and Philosophy*, Vol. 27, VI, 651-673.

[50] La citazione è tratta dal preambolo dell'atto costitutivo dell'Organizzazione Mondiale della Sanità stipulato a New York il 22 luglio 1946 e oggi presente all'interno del sito ufficiale del World Health Organization, disponibile online: https://www.who.int/about/governance/constitution.

[51] Con riguardo alla chirurgia sono inclusi in Italia nei Lea solo gli interventi che sono conseguenza di incidenti, esiti di procedure medico-chirurgiche o malformazioni congenite o acquisite, cioè solo i casi in cui rispondono a finalità terapeutiche, nel senso che, in loro mancanza, possono determinarsi con evidenza scientifica seri danni per la salute. Cfr. DPCM, 29 novembre 2011, *Definizione dei livelli essenziali di assistenza,*

Anche a livello nazionale, la qualificazione della salute ha risentito in maniera crescente dell'inscindibilità della dimensione del corpo dalla persona unitariamente considerata, e si manifesta oggi come un aspetto ricollegabile al suo libero e sano sviluppo[52]. In seguito alla soggettivizzazione del concetto, è oggi possibile definire, la salute quale stato di complessivo benessere psicofisico, che si estende alla tutela dell'integrità psico-fisica e al diritto all'autorealizzazione dell'individuo e della sua personalità. La giurisprudenza è costante nell'affermare che "l'idea tradizionale di patologia risulta sempre più distante da quella di salute, ormai carica di una forte componente soggettiva" e che "gli atti terapeutici, secondo una visione allargata di salute (...) non fanno più riferimento ad una concezione organica della malattia, ma tengono conto degli aspetti fisici e psichici della persona, e delle sue personali ed insindacabili aspettative di vita [53] ". L'aspetto fisico e quello psichico divengono così componenti indivisibili della salute della persona, che assume una sua unità ed unicità nell'esperienza individuale del singolo, comprensiva degli aspetti psicologici legati anche all'identità sessuale [54] . Con specifico riguardo a quest'ultimo aspetto, la Corte di Cassazione, in una recente sentenza in tema di rettificazione dei caratteri anagrafici di un soggetto transessuale, ha ribadito che, in caso di disforia di genere, la coincidenza tra *soma* e *psiche* è, anche in mancanza dell'intervento di demolizione chirurgica volto a modificare i caratteri sessuali, il risultato di un'elaborazione sofferta, intima e personale della propria identità di genere, i cui momento conclusivo è inevitabilmente influenzato dalle caratteristiche individuali[55].

Sul fronte opposto, l'espressione "potenziamento umano" assume carattere residuale rispetto alla definizione di "trattamento" e di "cura", attività rivolte alla rimozione di una patologia, e al passaggio da uno stadio di malattia ad uno di salute, attraverso un processo di guarigione. Lo *human enhancement* richiama l'uso volontario delle diverse conoscenze e tecnologie biomediche di intervento sul corpo finalizzato ad ottenere un'alterazione migliorativa del normale funzionamento fisico-psichico-emotivo dell'individuo, per superare alcune limitazioni funzioni organiche o mentali già esistenti o introdurne di nuove. Si assiste, anche in questo caso, ad una transizione da uno stadio antecedente ad uno futuro: il primo si richiama ad una condizione di "normalità" o condizione "standard", in assenza di patologie; lo stato futuro è rappresentato da un percorso di cambiamento orientato "verso il meglio"[56].

Allegato 2°, Prestazioni totalmente escluse dai LEA. Sui profili fiscali del potenziamento umano, si veda A. URICCHIO, *Robot tax: modelli di prelievo e prospettive di riforma*, in *Giust. civ.*, 2019, 7, 1749-1761.

[52] V. P. PERLINGIERI, "Il diritto alla salute quale diritto della personalità", *Rassegna diritto civile.*, 1982, vol. 2, pgs. 1020 ss; ID., *La persona e i suoi diritti. Problemi del diritto civile*, Esi, Napoli, 2005, pgs. 81-87; ID., *La personalità umana nell'ordinamento giuridico*, Esi, Camerino-Napoli, 1972, pg. 104.

[53] Per un commento, v. P. Zatti, *Il diritto a scegliere la propria salute (in margine al caso S. Raffaele)*, in *Nuova giur. civ. comm.*, 2, 92 ss. In generale, v. Cfr. A NICOLUSSI. *Enhancement e salute nel rapporto medico-paziente*, in L. PALAZZANI (a cura di), *Verso la salute perfetta. Enhancement tra bioetica e biodiritto*, Edizioni Studium, Roma, 2014, pgs. 181-191.

[54] S. Viciani, "Il riconoscimento del danno non patrimoniale alla salute sessuale della persona, libero dagli stereotipi di genere", *Nuova giur. civ. comm.*, 2017, 12, 1646-1651.

[55] Cass. civ., 20 luglio 2015, n. 15138, *Diritto di famiglia e delle persone*, 2015, num. 4, pgs. 1279-1286, con nota di Cavana, P., "*Mutamento di sesso o di genere? Gli equivoci di una sentenza*, in Il Diritto di famiglia e delle persone".

[56] L. PALAZZANI, *Il potenziamento umano. Tecnoscienza, etica e diritto*, Torino, 2015, 71-72.

Un rilevante elemento di incertezza che ostacola l'individuazione del limite tra cura e potenziamento è rappresentato dalla categoria degli interventi in prevenzione, richiamati dall'art. 13 della Convenzione di Oviedo, accanto a quelli di carattere diagnostico e terapeutico. La collocazione di interventi volti ad evitare dei risultati negativi (come l'insorgenza di una malattia) che potrebbero o meno verificarsi, è controversa, soprattutto all'interno di un "modello binario", scisso tra operazioni curative e non[57].

Questo problema era stato segnalato già nel 2016 in uno studio, il quale ha evidenziato, con specifico riguardo all'editing per scopi riproduttivi, come esso non possa definirsi "esattamente terapeutico", poiché non mira al trattamento di un paziente esistente affetto da una condizione indesiderata; né similmente può dirsi "preventivo" nel modo in cui lo sono alcune politiche di salute pubblica in relazione ad un rischio imminente e non altrimenti evitabile, potendosi all'opposto evitare di concepire prole. Dal lato opposto, l'editing genetico è in un certo senso sia "terapeutico", poiché mira a superare potenzialmente l'infertilità (anche se l'infertilità è volontaria, una scelta difficile tra un insieme indesiderabile di opzioni) che "preventivo" in quanto, consente ai genitori di decidere in anticipo di impedire la nascita di soggetti con una disabilità grave o limitante la vita[58].

La qualificazione degli interventi di editing in termini curativi dipende anche dal tipo di terapia da somministrare. Nel caso di interventi contro quelle monogeniche (anche note come mendeliane, perché il loro *pattern* di trasmissione rispetta le leggi di Mendel – n cui "il difetto del gene è il principale responsabile della patologia [59]) la tecnica di editing mira ad eliminare l'alterazione genetica, attraverso un intervento correttivo sul gene "malato", che viene curato, impedendo lo sviluppo della patologia. Interventi di questo tipo possono essere qualificati come trattamenti: si pensi agli interventi volti alla cura di malattie come la Corea di Huntington, la fibrosi cistica, la betatalassemia, l'anemia falciforme.

Più complesso è il caso delle malattie multifattoriali, che risultano dalla combinazione di predisposizioni genetiche e fattori ambientali, come per diabete, cancro, morbo di Alzheimer, obesità, malattie cardiache. In questi casi, l'embrione non eredita precisamente una malattia, ma solo la predisposizione genetica alla stessa, che sfocerà nella vera e propria patologia solo in presenza di ulteriori condizioni, determinate dai fattori ambientali. In questo caso, l'intervento correttivo avrebbe ad oggetto geni non malati, ma solo predisposti ad una futura ed eventuale situazione patologica che però da soli non sarebbero in grado di cagionare, senza il concorso con i fattori ambientali. L'editing genetico non assicura la permanenza dello stato di salute, ma si limiterebbe a ridurre il rischio di contrarre tali patologie, eliminando uno dei due gruppi di co-fattori che ne concorrono alla causazione, In relazione a questo

[57] Nuffield Council on Bioethics, *Genome editing and human reproduction: social and ethical issues*, cit., 71. V. anche I. De Miguel Beriain, *Gene editing and the slippery slope argument: should we fix the enhancement/therapy distinction as the definitive boundary?*, in *Science and Eng. Ethics*, 2018, 1257-1258.

[58] Nuffield Council on Bioethics, *Genome editing: an ethical review*, Londra, 2016, 49.

[59] A. Santosuosso, I.A. Colussi, *Diritto e genetica delle popolazioni*, in S. Canestrari, G. Ferrando, C.M. Mazzoni, S. Rodotà., P. Zatti (a cura di), *Il governo del corpo*, in *Trattato di Biodiritto* I, Milano, 2011, 358.

tipo di malattie, fattori genetici e fattori ambientali devono essere valutati non in termini di alternatività, bensì di cumulabilità[60].

Dubbi simili sono posti dalle malattie di origine non genetica, ma prevenibili attraverso un intervento sul genoma, come nel caso delle infezioni virali. Di recente, diversi studi hanno approfondito la possibile disattivazione del gene CCR5 per conferire all'individuo una particolare resistenza al virus dell'HIV; scenari simili potrebbero verificarsi anche per la prevenzione di malattie connessi con altri virus, come l'Ebola o il Coronavirus. Tuttavia, se l'intervento su un soggetto sano (sia già in vita, sia un embrione) che elimina il rischio di contagio rispetto ad una malattia virale, sembra assimilabile più ad un intervento migliorativo (in termini di resistenza "sovraumana" rispetto a malattie non genetiche) che non ad una terapia, anche intendendola nel senso esteso di "cura preventiva".

Infine, non sono trascurabili neppure i rischi connessi agli effetti non voluti ed imprevisti, cui si aggiungono quelli derivanti dalla commistione tra scopi di cura e potenziamento, che colora alcuni interventi di una certa ambiguità teleologica: ad esempio, proprio il noto caso delle gemelle cinesi nate editate nasconderebbe fini potenziativi, poiché sembra che la disattivazione della proteina CCR5, oltre a favorire l'immunità all'HIV, sortisca l'ulteriore effetto di potenziare le capacità cognitive[61].

La presenza delle difficoltà definitorie sino ad ora descritte (v. supra, anche para 3) non rappresenta tuttavia un argomento sufficiente per rinunciare a regolamentare il fenomeno dell'editing genetico; pertanto, si concorda con chi ha formulato la seguente riflessione: "*some have argued that the fact that it is difficult to draw bright lines regarding the therapy/enhancement distinction means that no lines can be drawn. But this is a specious argument. Public policy is in large part a matter of drawing lines; we do it all the time*[62]".

5. *Editing* genetico e diagnosi genetica pre-impianto.

La correzione del corredo genetico degli embrioni non è l'unico procedimento per evitare la nascita di prole non sana, anche da parte di coppie fertili portatrici di difetti genetici trasmissibili. Oltre alla possibilità di tentare la procreazione naturale, seguita da aborto terapeutico, in caso di esito sfavorevole degli esami diagnostici prenatali, gli aspiranti genitori possono optare anche per la PMA, accessibile, dopo il noto intervento della Corte

[60] La coesistenza di questi due fattori di rischio non consente di concludere nel senso dell'inutilità di un intervento volto a rimuovere il rischio genetico, come sostenuto da C. GYNGELL, T. DOUGLAS, J. SAVULESCU, 2017, *The Ethics of Germline Gene Editing*, in *Journal of Applied Philosophy*, 34, IV, 2017, 498-513, spec. 502: "it does not follow from the fact that a disease is partly or even primarily caused by environmental factors that environmental interventions are effective in preventing it".

[61] M.T. JOY et al., *CCR5 Is a Therapeutic Target for Recovery after Stroke and Traumatic Brain Injury*, in *Cell*, 2019, Vol. 76, V, 1143-1157.

[62] R. HAYES, *Is There an Emerging International Consensus On the Proper Uses Of the New Human Genetic Technologies*?, Center for Genetics and Society House Foreign Affairs Committee, Subcommittee on Terrorism, Nonproliferation and Trade, USA, 2008, disponibile su: https://www.geneticsandsociety.org/sites/default/files/20080619_hayes_testimony.pdf, citato da I. DE MIGUEL BERLAIN, L. MASTRANGELO, *Cosa c'è di sbagliato nel modificare la linea germinale*? In *BioLaw J.-Riv. Biodiritto*, 2020, I, 231-249.

Costituzionale, non solo nei casi di infertilità o sterilità, ma anche da parte dei fertili portatori di gravi malattie genetiche trasmissibili[63]. In questa seconda ipotesi, è possibile campionare gli embrioni ottenuti attraverso la procreazione assistita, allo stadio di blastomeri, per controllarne la struttura genetica e l'avvenuta trasmissione o meno delle malattie genetiche, attraverso la tecnica della diagnosi genetica preimpianto (DGP[64]). Gli embrioni sono sottoposti ad un processo di crioconservazione, in attesa del risultato, all'esito del quale, quelli sani saranno considerati idonei all'impianto; al contrario, quelli portatori di difetti genetici, saranno scartati.

L'impiego coordinato delle tecniche di PMA e DGP si rivela utile a prevenire molte malattie genetiche negli embrioni, con relativa facilità di impiego e con molti meno rischi rispetto all'editing genetico; anche questa tecnica presuppone il ricorso alla PMA e alla fecondazione degli embrioni in vitro, cui deve aggiungersi la successiva fase di "correzione delle bozze". Ci si interroga allora sull'effettiva utilità dell'editing come strumento alternativo alla DGP e selezione di embrioni, quale mezzo di soddisfacimento del desiderio di una coppia portatrice di malattie genetiche, di avere un figlio sano[65].

Pur essendo uno strumento più rischioso, i sostenitori dell'editing genetico germinale ne evidenziano i vantaggi, sia dal punto di vista clinico, che sotto il profilo etico.

In relazione al primo aspetto, l'editing genetico è l'unica opzione scientifica che residua quando la DGP rileva l'assenza di embrioni sani. Ciò può accadere nelle patologie autosomiche dominanti, come la sindrome di Huntington: in questo caso, affinché la malattia si manifesti nell'individuo, è sufficiente che questi possieda una sola copia del gene malato, ereditato da uno dei genitori. In presenza di un genitore malato eterozigote (cioè portatore nel genoma anche della copia sana del gene, cioè con genotipo per metà sano ma fenotipo malato) la probabilità di trasmissione della malattia è pari al 50% (figura 1); un genitore malato omozigote (con entrambi i geni difettosi), genererà inevitabilmente solo prole malata (figura 2).

---

[63] C. Cost., 5 giugno 2015, n. 96, *in Riv. it. dir. proc. pen.*, 2015, III, 1453 ss., con nota di A. VALLINI, *Il curioso (e doloroso) caso delle coppie fertili portatrici di malattie ereditarie, che potevano ricorrere all'aborto, ma non alla diagnosi e selezione preimpianto, ha caducato il divieto di accesso alla procreazione assistita per tali coppie;* C. TRIPODINA, *Le parole non dette. In lode alla sentenza 96/2015 in materia di fecondazione assistita e diagnosi preimpianto per coppie fertili portatrici di malattia genetica*, in *Costituzionalismo.it*, 2015, II, 5 e segg.; M. GIACOMINI, *Il sì alla diagnosi preimpianto: un punto di arrivo o un punto di partenza*?, in *Forum Quad. cost.*, 2015; S. PENASA, *L'insostenibile debolezza della legge 40: la sentenza n. 96 del 2015 della Corte costituzionale tra inevitabili illegittimità e moniti "rafforzati"*, in *Forum Quad. cost.*, 2015; A. IANNUZZI, *La Corte Costituzionale dichiara l'illegittimità del divieto di accesso alla diagnosi preimpianto e alla procreazione medicalmente assistita per le coppie fertili e sgretola l'impianto della legge n. 40 del 2004*, in *Giur. cost.*, 2015, 805 e segg.; C. NARDOCCI, *Dalla Convenzione alla Costituzione: la tacita sintonia tra le Corti. A margine di Corte cost. sent. n. 96 del 2015,* in Riv. Biodiritto, 2016, 1, 271-281; C. IAGNEMMA, *Diagnosi genetica preimpianto: problemi aperti in rapporto alla sentenza della corte costituzionale n. 229/2015*, in *Riv. it. med. leg.*, 2016, 322 e segg.; R. POMIATO, *Diagnosi preimpianto e tutela dell'embrione: un equilibrio ancora precario*, in *Europa dir. priv.*, 2016, I, 219-247; A. CARRATO, *Diagnosi preimpianto: l'applicazione giurisprudenziale della sentenza n. 96/2015 della Consulta*, in *Famiglia e diritto*, 2017, VI, 541-558.

[64] Con riguardo alle fattispecie cliniche nelle quali le coppie possono agevolarsi di tale tecnica si veda, S. LA ROSA, *La diagnosi preimpianto: un problema aperto*, in *Fam. e dir.*, 2011, 839.

[65] M. BRAUN, H. SCHICKL H., P. DABROCK, *Between Moral Hazard and Legal* Uncertainty, in ID., (a cura di), *Ethical, Legal and Societal Challenges of Human Genome Editing*, Wiesbaden, 2018, 8-9: "It can be argued that in the cases where PGD is an actual alternative its application is ethically always preferable to the application of genome editing techniques, as long as there remains even a little health risk (because this little health risk would still be bigger than the minimal to zero risk of PGD".

A → gene dominante (malato); a → gene recessivo (sano)

	A	a
a	Aa MALATO	aa SANO
a	Aa MALATO	aa SANO

Figura 1

	A	A
a	Aa MALATO	Aa MALATO
a	Aa MALATO	Aa MALATO

Figura 2

Invece, le patologie autosomiche recessive, come la fibrosi cistica, si manifestano solo nella prole che eredita una doppia copia del gene mutato. Ne consegue che se entrambi i genitori sono portatori sani della patologia, il 25% dei figli sarà malato, il 50% portatore sano, il 25% sano (figura 3); se uno dei due genitori è malato (omozigote recessivo) e l'altro portatore sano, il 50% dei figli sarà portatore sano ed il restante 50% malato (figura 4); se entrambi i genitori sono malati, la prole nascerà sicuramente affetta dalla patologia (figura 5).

A → gene dominante (sano); a → gene recessivo (malato)

	A	a
A	AA SANO	Aa PORTATORE SANO
a	Aa PORTATORE SANO	aa MALATO

Figura 3

	a	a
A	Aa PORTATORE SANO	Aa PORTATORE SANO
a	aa MALATO	aa MALATO

Figura 4

	a	a
a	aa MALATO	aa MALATO
a	aa MALATO	aa MALATO

Figura 5

Nei casi descritti dalle figure 2 e 5, l'impiego della DGP sarebbe infruttuoso, poiché qualsiasi embrione prodotto sarebbe malato, con una impossibilità assoluta di impiantarne uno privo della malattia genetica di cui i genitori sono portatori. L'unico rimedio possibile è quello della correzione del corredo genetico dell'embrione selezionato: infatti, l'editing genetico offrirebbe una gamma molto più vasta di scelte alternative, attraverso la correzione, la modifica o la sostituzione di singoli geni; al contrario, "*selection is unable to introduce anything new* ", poiché attraverso la DGP ci si limita a scegliere

l'embrione sano tra quelli esistenti e predeterminati, senza incidere sul contenuto del corredo genetico[66].

Sotto il versante etico, si è evidenziato che, mentre la selezione operata con la DGP determina l'eliminazione degli embrioni in eccesso o malati, l'editing genetico consentirebbe di curare future persone malate, intervenendo in via preventiva. La contrapposizione tra DGP selettiva e genome editing correttivo appare tuttavia troppo semplicistica: optare per la seconda soluzione non esclude che gli embrioni, anche se editati, non siano successivamente scartati, qualora, a seguito di DGP emergesse la non riuscita dell'operazione genetica, o venissero riscontrati casi di mosaicismo o mutazioni *off-target*, impreviste e non volute. Nonostante il tenore letterale del'art. 6 comma 3 della L. 40/2004, che limita la revoca del consenso dei genitori alla PMA fino al momento della fecondazione dell'ovulo, nel rispetto del divieto costituzionale di imposizione di trattamenti sanitari, la donna può rifiutarsi in ogni momento, anche successivo al limite cronologico di legge, di accettare l'innesto. La revoca, anche tardiva della donna, quale che sia la motivazione sottesa – e dunque anche a seguito di editing degli embrioni – del consenso all'impianto conferma l'incertezza dello stesso anche nel caso di esito positivo della correzione del corredo genetico embrionale[67].

La letteratura in argomento concorda dunque correttamente nel ritenere, quanto ai rapporti tra le due tecniche, che "*it is unlikely that GGE will have a significant effect on rescuing embryos. It is even less likely that GGE will soon become a 'replacement for PGD*'[68]".

6. Identità genetica: diritto al "futuro aperto" o diritto "a non nascere se non arbitrariamente modificato"?

Ulteriori dubbi in tema di interventi genetici sulla linea germinale scaturiscono dalla loro incidenza sull'identità del soggetto colpito, con conseguente lesione del diritto soggettivo all'identità genetica. Il riconoscimento di una tale situazione giuridica soggettiva trae origine dalla normativa europea [69] : già la Raccomandazione 1046/1978, nel vietare la clonazione umana, aveva evidenziato come "ogni individuo ha diritto alla sua specifica identità genetica". Anche il diritto dell'Unione Europea ha fatto riferimento espresso all'identità genetica in due documenti: la Direttiva UE sulle invenzioni biotecnologiche (Direttiva 98/44/CE), il cui articolo 6 lett. b) prevede che "i processi di modificazione dell'identità genetica germinale degli

[66] D. BIRNBACHER, *Prospects of Human Germline Modification by CRISPR-Cas9: an Ethicist's View*, in M. BRAUN, H. SCHICKL H., P. DABROCK, (a cura di), *Between Moral Hazard and Legal Uncertainty. Ethical, Legal and Societal Challenges of Human Genome Editing*, cit., 65.

[67] In arg. R. S. BONINI, *Procreazione medicalmente assistita: vittime del consenso?* in *Politica del diritto,* 2021, III, 475-488; A. BOSSO, *Irrevocabilità del consenso alla procreazione medicalmente assistita e tutela dell'embrione. Nota a ordinanza: Trib. Santa Maria Capua Vetere, sez. I civ., 27 gennaio 2021,* in *giustiziacivile.com,* 2021, IV, 1-9; M. FACCIOLI, *Procreazione assistita omologa, separazione dei coniugi e revoca del consenso da parte dell'uomo*, in *Persona e Mercato*, 2021, II, 361-369.

[68] R. RANISCH, *Germline genome editing versus preimplantation genetic diagnosis: Is there a case in favour of germline interventions*?, in *Bioethics*, Vol. 34, 2020, 60-69.

[69] I. DE MIGUEL BERIAIN, *Legal issues regarding gene editing at the beginning of life: An EU perspective*, in *Regenerative Medicine*, Vol. 12, VI, 2017, 669-679.

esseri umani sono considerati non brevettabili", e il regolamento (UE) n. 536/2014, del 16 aprile 2014, concernente la sperimentazione clinica di medicinali per uso umano, che "non possono essere effettuate sperimentazioni cliniche di terapia genica che comportano modifiche dell'identità genetica della linea germinale del soggetto[70]". Tuttavia, come è stato evidenziato anche dalla Dichiarazione Internazionale sui Dati Genetici Umani[71], l'identità personale non è sovrapponibile a quella genetica, che ne rappresenta solo una componente, in concorso con altri fattori, ambientali, culturali ed emotivi, che ne costituiscono la dimensione esteriore-relazionale[72].

Per quanto l'essere umano non possa essere ridotto alla somma delle sue informazioni genetiche, queste contribuiscono in misura significativa alla formazione della sua individualità, inevitabilmente intaccata dagli interventi sul genoma. La programmazione genetica crea delle relazioni interpersonali caratterizzate da una peculiare – e inedita – asimmetria, definita da Habermas "una sorta di paternalismo *sui generis*", in virtù del quale "il programmatore dispone in modo unilaterale (…) delle caratteristiche genetiche di un altro, nella paternalistica intenzione di condizionare significativamente la storia di vita di questo dipendente[73]".

È opportuno dunque valutare l'ammissibilità, sotto il profilo tecnico-giuridico, di un "diritto all'integrità del patrimonio genetico", espressione dell'identità genetica dell'embrione, a garanzia del suo "diritto ad un futuro aperto". Se ricostruito in questi termini, tale diritto sarebbe automaticamente violato da ogni intervento di editing, poiché la nascita dell'individuo titolare del diritto asseritamente leso, avverrebbe necessariamente a manipolazione genetica già avvenuta.

Se l'intervento di editing avviene per scopi terapeutici, l'esistenza di un "diritto a nascere con un patrimonio genetico non modificato" presenta alcune somiglianze con il "diritto a non nascere" o "a non nascere se non sano". Si pensi al caso di un embrione portatore di una patologia, riscontrata a seguito della diagnosi genetica preimpianto: grazie alla decisione dei genitori di editare l'embrione e di impiantarlo successivamente, nasce un individuo sano, ma con un patrimonio genetico modificato. In assenza dell'intervento di editing, l'embrione non sarebbe mai venuto ad esistenza, poiché sarebbe stato

---

[70] Rispettivamente, Direttiva 98/44/CE del Parlamento europeo e del Consiglio del 6 luglio 1998 sulla protezione giuridica delle invenzioni biotecnologiche; Regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio del 16 aprile 2014 sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE.

[71] Unesco, *International Declaration on Human Genetic Data*, Parigi, 16 ottobre 2003 (disponibile su: https://www.unesco.org/en/legal-affairs/international-declaration-human-genetic-data), Article 3 – Person's identity: "Each individual has a characteristic genetic make-up. Nevertheless, a person's identity should not be reduced to genetic characteristics, since it involves complex educational, environmental and personal factors and emotional, social, spiritual and cultural bonds with others and implies a dimension of freedom".

[72] Sulla dimensione dinamico-relazionale dell'identità, v. Corte Cost. 24 gennaio 1994, n. 13: "Si tratta - come efficacemente è stato osservato - del diritto a essere se stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo. L'identità personale costituisce quindi un bene per sé medesima, indipendentemente dalla condizione personale e sociale, dai pregi e dai difetti del soggetto, di guisa che a ciascuno è riconosciuto il diritto a che la sua individualità sia preservata".

[73] J. HABERMAS, *Il futuro della natura umana. I rischi di una genetica liberale*, Torino, 2010, 55-57.

scartato, in quanto malato: l'alternativa è dunque tra la nascita come soggetto sano ma editato, e la non-nascita.

In Italia, l'irrisarcibilità del danno da *wrongful life*, derivante dall'asserita violazione del "diritto a non nascere", è stata definitivamente confermata dalle Sezioni Unite della Corte di Cassazione, a composizione del precedente contrasto giurisprudenziale[74]. Sia per il soggetto nato malato che per quello nato (sano perché) editato, l'unica alternativa possibile sarebbe stata la non-nascita; tuttavia, la non-vita, quale condizione ontologicamente peggiore, in quanto necessariamente "negativa", non può essere preferita ad alcuna forma di esistenza in positivo, anche malata o geneticamente modificata[75]. Inoltre, il diritto al risarcimento del danno sarebbe un "diritto adespota", di cui il soggetto diviene titolare solo a seguito della sua violazione per nascita malformata o alterazione genetica, senza la quale non avrebbe mai avuto possibilità alcuna di venire ad esistenza e, per l'effetto, di esercitare tale diritto.

Si tratta di conclusioni oggi condivise, ma non immodificabili, anche alla luce del futuro raggiungimento di adeguati livelli di sicurezza nell'applicazione della tecnica di editing. Ad esempio, il soggetto nato (naturalmente) malato potrebbe agire in giudizio nei confronti dei propri genitori per il risarcimento del danno da *wrongful life* ed invocare, quale alternativa alla propria esistenza attuale da malato, non la "non-vita", bensì "l'esistenza sana" ottenibile attraverso un intervento di editing, per cui i genitori non hanno optato, ma che gli avrebbe consentito di vivere una vita libera dalla malattia. In una simile ipotesi, potrebbe configurarsi in capo ai genitori una responsabilità da "omesso intervento" di editing [76] ; condotto tale ragionamento alle estreme conseguenze, anche un soggetto sano potrebbe ritenersi leso dal mancato editing potenziativo da parte dei genitori, preclusivo di un'esistenza potenziata e di innumerevoli chance ulteriori rispetto ad una "vita ordinaria".

All'opposto, anche la scelta in positivo di effettuare un intervento di editing potrebbe generare conseguenze risarcibili, senza dover necessariamente sostenere l'ardito scenario della lesione del "diritto alla disabilità", causata da un intervento genetico curativo[77]. Se il "diritto al futuro aperto" si traduce giuridicamente nel "diritto a nascere con un patrimonio genetico non arbitrariamente modificato[78], e se le di tecniche di editing sono impiegate per un fine diverso da quello terapeutico, per alterare una caratteristica genetica qualsiasi del soggetto, a discrezione dei genitori, l'ipotesi di un danno risarcibile

---

[74] Cass. Civ. SS.UU., 22 dicembre 2015, n. 25767, con nota di G. Bilò, *Nascita e vita indesiderate: i contrasti giurisprudenziali all'esame delle Sezioni Unite*, *Corriere giuridico*, 2016, I, 47-55; Cass. civ., 29 luglio 2004, n.14488, *Giust. civ.*, 2005, III, 136-148, con nota di E. Giacobbe, *Wrongful life e problematiche connesse*; Cass. civ., 2 ottobre 2012, n. 16754, *Il Diritto di famiglia e delle persone*, 2013, II, 474-501, con nota di P. Stanzione, G. Salito, *La tutela del nascituro: una ricorrente vicenda giudiziaria*.

[75] Per citare il pensiero di F. Carnelutti, "senza l'inadempimento il preteso danneggiato anziché più avrebbe meno di quello che ha, perché questo non avrebbe, anzi non sarebbe, nulla", *Postilla a Trib. Piacenza 31.7.1950*, *Foro it.*, 1952, I, 990-992.

[76] M. Rizzuti, *Editing genetico e diritto di famiglia*, in B. Agostinelli, V. Cuffaro, *Relazioni, Famiglie, Società*, 2020, 221-244, 238: "Se l'alternativa al nascere malato non si configurasse più come il "non nascere" (…) bensì il "nascere editato" allora il discorso andrebbe quantomeno riaperto su basi nuove".

[77] I. de Miguel Beriain, *Gene editing and disabled people: a response to Felicity Boardman*, in *J. Community Genet.* 2020, Vol. 11, III, 241-243; S. Benston, *CRISPR, a Crossroads in Genetic Intervention: Pitting the Right to Health against the Right to Disability*, in *Laws*, 2016, Vol. 5, I, 1-5.

[78] A. Alcone: *La tutela del patrimonio genetico umano fra Costituzione e diritti. Verso la formazione di un corpus iuris sul genoma umano*, Soveria Mannelli, 2012, 19-20.

in capo al neonato editato non sarebbe così peregrina. Sebbene anche in questa seconda ipotesi la nascita del titolare del diritto e la violazione dello stesso siano contestuali, l'alternativa, per il nato editato non sarebbe stata una condizione di non-nascita, bensì di nascita senza intervenuta manipolazione genetica, non necessaria per lo svolgimento di un'esistenza sana. Oltre alle ipotesi di danno da editing più immediate e facilmente individuabili, che abbiano inciso sulla salute del soggetto (effetti collaterali dannosi, errata esecuzione dell'operazione) possono prospettarsi scenari molto più incerti, con il rischio di scivolare verso relativismi soggettivistici di privi di stabili punti di riferimento: si pensi, ad esempio, ai casi in cui il presunto danneggiato sostenga "con l'argomento del futuro aperto o altri consimili, che sarebbe stata preferibile una vita non condizionata dal positivo esito dell'editing genetico o di altre metodiche di *enhancement*" ovvero se "prospetti come migliore, nel confronto con quella "potenziata, un'esistenza normale, cui non ha avuto accesso[79]".

7. Riflessioni conclusive: tentativi di strategie definitorie e *risk-based approach*.

Pur nelle difficoltà di inquadramento del fenomeno dell'editing genetico già a livello tecnico-scientifico, oltre che etico, stante la delicatezza del tema *in primis* dipendente dalla vulnerabilità intrinseca dell'embrione, il giurista, sia italiano sia europeo, non può esimersi dal fornire delle proposte di regolazione giuridica. Le soluzioni, sul punto, possono essere diverse.

In primo luogo, potrebbero essere considerati legittimi solo gli interventi manipolativi che provvedono a correggere una manipolazione genetica volta ad eliminare una malformazione genetica responsabile di una patologia inserita all'interno di un documento apposito. Già la raccomandazione 1047/1986 del Consiglio d'Europa[80] suggeriva che "*it would be desirable to create a list of those illnesses where therapy can be based on reliable means of diagnosis and reasonable guarantees of success. This list would be periodically updated to take account of new discoveries and scientific progress*". In maniera non dissimile, più di recente, anche la Corte Costituzionale, con la citata sentenza 96/2015, nel dichiarare l'illegittimità costituzionale del divieto del ricorso alle tecniche di procreazione medicalmente assistita per le coppie fertili portatrici di patologie genetiche trasmissibili", aveva invitato il legislatore italiano a predisporre un elenco delle gravi patologie che avrebbero giustificato l'accesso alla PMA, tuttavia mai emanato. Il silenzio del legislatore risulta opportuno, poiché il sistema normativo, come corretto dal giudice delle leggi, è in grado di funzionare pur in assenza di un elenco rigido e formalizzato di tutte le malattie rilevanti, essendo necessaria e sufficiente una certificazione in concreto della gravità della patologia.

[79] M. Rizzuti, *Editing genetico e diritto di famiglia*, cit., 243.

[80] Recommendation n. 1046 (1986), *Use of human embryos and foetuses for diagnostic, therapeutic, scientific, industrial and commercial purposes*, 24 Settembre 1986; condivide questa soluzione N. Conditi, Il diritto a nascere con un patrimonio genetico non arbitrariamente modificato come limite alla legittimità delle manipolazioni genetiche embrionali, I, 2020, 251-271, spec. 269-270.

Anche per le procedure di editing genetico, l'elencazione puntuale delle patologie che ammetterebbero un intervento di questo tipo non sembra l'opzione migliore, sia per il rischio di incompletezza e il costante bisogno di aggiornamento, sia per l'effetto di "ostracismo sociale" di una tale lista, nei confronti dei soggetti affetti dalle malattie ivi contenute[81].

L'approccio suggerito di recente dall'Unione Europea si basa invece su un criterio più elastico: dal Report dello STOA emerge che sarebbe opportuno indicare gli interventi di editing concessi o vietati, le qualifiche dei professionisti coinvolti, i requisiti tecnici e di sicurezza, attraverso l'impiego di un "*multi-level, risk-based approach*" anche al fine di individuare le regole specifiche per gli interventi di *genome editing* vietati e ad alto rischio. I possibili criteri di individuazione del rischio includono lo scopo dell'intervento, i risultati attesi, il livello di rischio per l'individuo e la società. Ai legislatori nazionali potrebbe essere affidato il compito di curare la procedimentalizzazione dell'iter, per valutare, caso per caso, il livello di rischio in concreto presente nell'intervento di *editing*[82].

[81] Si concorda con le riflessioni di M. Rizzuti, *Editing genetico e diritto di famiglia*, cit. 237; Id., *Il problema della diagnosi pre-impianto*, in *Diritto e salute*, 2017, III, 65-76.

[82]Sulla falsariga di quanto affermato nel testo, la Germania, all'interno della legge sulla diagnosi genetica preimpianto (*Gesetz zum Schutz von Embryonen*, Legge sulla protezione degli embrioni, cit.), ha indicato un procedimento autorizzatorio imperniato sull'intervento di una *Ethikkommission* (§ 3a Präimplantationsdiagnostik; Verordnungsermächtigung, comma 3: "La diagnosi genetica preimpianto di cui al paragrafo 2 può essere effettuata soltanto: 1. dopo aver ricevuto informazioni e consulenza sulle conseguenze mediche, psicologiche e sociali dell'esame genetico delle cellule degli embrioni richiesto dalla donna, che deve essere effettuato prima di ottenere il consenso, 2. dopo che un comitato etico composto su base interdisciplinare ha verificato il rispetto delle condizioni di cui al paragrafo 2 presso i centri riconosciuti per la diagnosi genetica preimpianto e ha fornito una valutazione favorevole; e 3. da un medico qualificato in centri riconosciuti per la diagnosi preimpianto che dispongano delle capacità diagnostiche, mediche e tecniche necessarie per l'attuazione delle misure di diagnosi preimpianto. Le azioni intraprese nell'ambito della diagnostica preimpianto, compresi i casi respinti dai comitati etici, sono notificate e documentate in forma anonima dai centri autorizzati a un ente centrale").

LIST OF AUTHORS OF THIS EJPLT ISSUE

GIOIA ARNONE – Ph.D., Researcher of the Digitalisation and Access to justice Research Group (DIKE), Private and Economic Law Department (PREC), Vrije Universiteit Brussel, Belgium.

NIKOLA DACEV – Associate Professor of Civil Law, Faculty of Law, International Balkan University, Skopje, North Macedonie.

LORENZO DEL FEDERICO – Full Professor of Tax Law, Università G. D'Annunzio Chieti – Pescara, Italy.

FRANCESCA FERRETTI – Ph.D.(c) in Civil Law and Constitutional Legality, Università degli Studi di Camerino, Italy.

PAOLO GAGGERO – Full Professor of Economic Law, Università degli Studi di Roma La Sapienza, Italy.

STEFANO GATTI – Lecturer (RTD-B) in Private Law, Università di Verona, Italy.

MARCO GIACALONE – Research Professor and Co-Director of the Digitalisation and Access to justice Research Group (DIKE), Private and Economic Law Department (PREC), Vrije Universiteit Brussel, Belgium.

MEVLUDIN IBISH – Associate Professor, Faculty of Law, International Balkan University, Skopje, North Macedonie.

CLAUDIA IRTI – Full Professor of Private Law, Università Ca' Foscari di Venezia, Italy.

LUIGI IZZO – Ph.D.(s) in Humanities and Technologies: an Integrated research path, Università degli Studi Suor Orsola Benincasa, Napoli, Italy.

KONSTANTINOS KOUROUPIS – Assistant Professor of European and Data Rights Law, Frederick University, Cyprus.

RAMZI MADI – Full Professor of Commercial Law and Intellectual Property Law, Al Ain University, United Arab Emirates. Deputy Dean of College of Law, Al Ain University, United Arab Emirates.

ROBERTA MONTINARO – Full Professor of Private Law, Università degli Studi di Napoli L'Orientale, Italy.

JUAN SEBASTIÁN ALEJANDRO PERILLA GRANADOS – Associate Professor, Universidad Tecnológica de Bolívar, Colombia.

CRISTINA ELENA POPA TACHE – Associate Professor of Public International Law and Communications and New Technologies Law, Bucharest University of Economic Studies, Romania. Researcher at CIRET - Center International de Recherches et Études Transdisciplinaires, Paris, France.

GEMMA RUBIO GIMENO – Associate Professor of Private Law, Universitat de Barcelona, Spain.

GIULIO SANTONI – Ph. D., Università degli Studi Roma Tor Vergata, Italy.

CĂTĂLIN SILVIU SĂRARU – Associate Professor of Administrative Law, Bucharest University of Economic Studies, Romania.

CALOGERO ALBERTO VALENZA – Research Fellow, Università degli Studi di Roma La Sapienza, Italy.

GERARDO VILLANACCI – Full Professor of Private Law, Università Politecnica delle Marche, Ancona, Italy.