LAW IN THE AGE OF DIGITALIZATION

FEDERICO PEDRINI
Editor

Law in the age of Digitalization

Fernando H. Llano Alonso
Thomas Casadei
Rosaria Pirosa
Lucia Bosoer
Marta Cantero
Ruth Rubio
Matteo Caldironi
Valentina Cavani
Carmine Andrea Trovato
Marina Caporale
Mario Santisteban Galarza
Elsa Marina Álvarez González
Manuel Moreno Linde
Chiara Francioso
Francesco Diamanti
Fernando Miró-Llinares
Alessandro V. Guccione
Federica Nizzoli
Giacomo Pailli
Cinzia Valente

ARANZADI

Editorial Aranzadi, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@aranzadilaley.es
https://www.aranzadilaley.es

First edition: June 2024

Legal Deposit: M-13846-2024
ISBN print version: 978-84-1163-964-4
ISBN electronic version: 978-84-1163-965-1

This book was financed with funds 'FAR 2022' from the Unimore Department of Law

Design, Prepress and Printing: Editorial Aranzadi, S.A.U.
Printed in Spain

Table of contents

Page

CRIMINAL LAW

Page

PROCEDURAL LAW

PRIVATE COMPARATIVE LAW

Science and law in the age of digitalization

This book is part of a series of initiatives aimed at consolidating the internationalization of the Department of Law of the University of Modena and Reggio Emilia. In particular, it was strongly desired by its Director, Prof. Elio Tavilla, who is its real creator. I figure as editor only thanks to his kindness, since, as the Department's research delegate, I materially followed the stages of the book.

In this stimulating process I have had the privilege of meeting distinguished foreign scholars and the pleasure of deepening relationships with many Italian colleagues, both from the University of Modena and from other prestigious universities. None of this would have been possible without the connections that for years our Department has been patiently cultivating with a now "global" scientific community.

The topic of digitalization immediately seemed to be the most suitable common ground for establishing a dialogue that went beyond the national boundaries of positive law. Indeed, it is one of those "cross-cutting" issues that are structurally interdisciplinary, and by their nature pose questions whose answers often lie beyond the regulatory capacities of the single State.

The digital innovations and their legal consequences with which this study deals are the most recent and significant page of an ancient problem. The problem is that of the relationship between law and science.

From this point of view the most interesting profiles are two, connected to each other in numerous ways. In the first profile science and/or certain technological applications are directly the subject of normative discipline. In the second profile, science is the "de facto" premise, which indirectly influences the production of new law and the interpretation and application of existing law.

The first aspect, relating to science as an object of legal discipline, is well summarized at the general level in the opening formula of Article 33 of the

Italian Constitution: "art and science are free and free is their teaching". Similar provisions can be found in many constitutional texts, such as Article 4 of the **Grundgesetz** or Articles 20 and 44 of the Spanish Constitution. It thus concerns the constitutional value of the autonomy of science over normative constraints that impose from outside on the scientist what to do or how to do it.

To work properly, science must be free. And this applies both to its pure dimension of theoretical research (and teaching) and to its practical dimension of technological applications. Of course, this does not mean that law cannot place limits on scientific research and/or its technological applications. However, such limits in contemporary constitutional States cannot be merely ethical in nature or freely selected by the legislature. Instead, these limits will have to find their justification in other constitutional goods. In other words, science is constitutionally free. Even if it remains possible to balance that freedom with other constitutional rights or goods that in practice are likely to be affected by the concrete exercise of that freedom.

In the second of the aforementioned relationships between law and science, the latter is no longer directly relevant as the object of legal discipline, but as a particular factual premise that, indirectly, can influence the application of other (not only constitutional) norms.

Indeed, the rise of new scientific discoveries and new technologies, while opening up new practical possibilities, can pose (and often concretely poses) new problems of legal qualification and regulation. It imposes the subsumption of new cases into already existing norms and sometimes, if this is not enough to achieve a desirable social arrangement, suggests the adoption of new norms.

Examples of such situations abound in every field, and not surprisingly are the beating heart of this volume. It sufficient to recall, among many others, the issues of big data and algorithms, new digital media, fake news and artificial intelligence. These are technologies that evidently make it possible to achieve desirable goals. At the same time, they raise dilemmas regarding both their greater or lesser appropriateness (**de jure condendo**) and the actual lawfulness (**de jure condito**) of certain conduct that has now become materially possible.

What kind of transformations affect the subjective rights of classical constitutionalism in the face of modern neurotechnology and computerized processing of personal data? Can the phenomena of information disorder that

now characterize the so-called digital information ecosystem be effectively countered? What are the systemic perspectives and implications with respect to the introduction of electronic voting in the national and supranational context?

What are the rights and duties that would result from a "European digital citizenship"? What contribution can modern digital technologies make to processes of participatory democracy and the reduction of social inequalities? What will be the impact of AI on the paradigms of tax and criminal law? What problems does the modern concept of "digital identity" pose for law? What are the prospects at the European level in terms of financial supervision and the dematerialization of public services linked to digital innovations?

These are just some of the questions to which this book tries to offer a framework and a first attempt at an answer, ranging over numerous fields of legal knowledge: from the philosophy of law to constitutional law and **ius publicum europaeum**, from administrative law to tax law, from criminal and commercial law to procedural and labor law, passing through comparative law. At the same time, there is an awareness that these are extremely fluid matters, susceptible to rapid and often unpredictable developments. In the background, of course, the fundamental question remains: will the technology of the present and the near future – whether it is the protection of privacy or the fight against climate change – be able to assert its positives or will it remain predominantly victim of its risks?

Needless to say, such a dilemma should not be approached fatalistically. Digitalization, at least for now, is a human product. Responsibility for its use, good or bad, should not be imagined abstractly, but remains with concrete people. It is on their intelligence, individual and collective, that depend – now more than ever – not only the type and quality, but the very existence of life on the planet. In such a venture it is inevitable that jurists are also called upon to make their contribution, and in our own small way this is what we have tried to do in this publication.

Federico Pedrini
Modena, Januar 2024

Philosophy of law

Technological singularity and personal identity. Reflections for an ethical-legal debate

[1]Fernando H. Llano Alonso*

SUMMARY: I. NEURO-IMPLANTS AND THE THERAPEUTIC USE OF ARTIFICIAL INTELLIGENCE - II. THE NEW GENERATION OF DIGITAL RIGHTS AND THE RECOGNITION OF NEURORIGHTS - III. WHEN A PERSON BECOMES AN AVATAR: THE NOVO HOMO LUDENS IN THE INTERNET METAVERSE - IV. CONCLUSION

ABSTRACT: Man's absorption by the virtual universe of digital technologies, his abandonment of the real world and tangible reality, produces in the individual a form of profound identity crisis, a kind of acute disorientation with regard to the place in which he finds himself.

As the lines that demarcate the horizon of the technological singularity gradually take shape, a hypothesis in which the creation of strong AI by machines will supposedly surpass the control and capacity of human intelligence, the identity of individuals is becoming increasingly blurred in the face of this transhuman future in which both their position and their role are completely uncertain. The crisis of personal and human identity in the face of the progressive self-determination of machines developed with AI, as well as the expansion of the virtual world and the immersion of the individual in a meta-universe (or metaverse) in a multi-sensory and three-dimensional experience enjoyed through the applied use of devices and technological developments of the internet, raise innumerable anthropological, ethical, political and sociological questions.

With regard to the ethical-legal implications arising from the interaction between the novo homo ludens with the meta-universe of the internet and AI technology, it would be appropriate to determine to what extent not only the denaturalisation of contemporary

* Full Professor in Philosophy of Law, University of Seville.

man is taking place, but also, to a certain extent, the dehumanisation of technology for the sake of an evolutionary leap that, as transhumanists predict, will bring us as a species closer to the horizon of the singularity of homo excelsior (hybrid between homo excelsior and homo ludens), the dehumanisation of technology for the sake of an evolutionary leap that, as the transhumanists predict, will bring us as a species closer to the horizon of the singularity of homo excelsior (hybrid between man and intelligent machine), without this serving as an excuse to avoid the benefits and wellbeing that the technological revolution 4. 0 technological revolution, and in particular AI and advanced robotics, represent for the improvement of the quality of life of future generations.

KEYWORDS: Neurorights; Digital Revolution; Technological Singularity; Human Identity; Metaverse.

I. NEURO-IMPLANTS AND THE THERAPEUTIC USE OF ARTIFICIAL INTELLIGENCE

The digital transformation is progressing at such a dizzying pace that, just as we have barely begun to familiarize ourselves with the Internet of Things, an evolutionary leap in technology is already being heralded in its quest to explore and expand the sensory frontiers of the network. The Internet of Senses is intended to merge the real and digital worlds to the point of making them indistinguishable. The goal of connecting a human to the network makes it possible to imagine a future in which the *homo excelsior* (a cyborg resulting from the symbiosis between machine and human) can develop neurologically and experience the five senses through digital technologies. Human beings can be neurologically connected to New Digital Technologies using subdermal implants, neurotransmitters, interfaces and brain microchips. Well-known examples are the neural engineering projects of Elon Musk (through the company Neuralink) or Mark Zuckerberg (through the virtual reality Metaverse VR)[1].

1. Martha J. Farah was one of the first researchers to analyze the ethical implications of neurosurgical technology, with special emphasis on the use of neuropharmacology through neurotransmitters for the treatment of diseases such as Alzheimer's, Attention Deficit Hyperactivity Disorder. She is also one of the first authors to consider the potential ethical-legal effects of judicial imposition of behavior-modifying treatments for people with asocial behaviors, cfr. M.J. FARAH, *Emerging Ethical Issues in Neuroscience*, in *Nature Neuroscience*, n. 5/2022, 1123-1129.

When determining the capacity and limits of human intelligence from a scientific point of view, we must first consider that a large part of our brain activity is dedicated to receiving and processing the sensory information that influences our actions and decision making. In this regard, Kevin Warwick, one of the world's leading experts in AI and cybernetics (considered by many to be the first cyborg in history since he connected the nerves in his arm to a bionic hand in 2002), warns of the limited ability of human thought to potentially perceive signals that are not perceptible to humans but are perceptible to intelligent robots developed with AI. Given the limited capacity of the human mind, most current applications of non-human sensors are precisely to convert such extra-sensory signals for humans into energy that humans can perceive, such as a virtual X-ray image. According to Warwick's forecast, the use of the potentially wide range of sensory inputs by AI systems will clearly increase their range of capabilities as time goes on[2].

Proof that the line between man and machine is becoming ever narrower can be found in the brain implant system *BrainGate*. So far, brain-computer interfaces have been used for therapeutic purposes to overcome medical/neurological problems. However, there is also the possibility of employing this technology to endow individuals with abilities that, in general, humans do not possess[3].

Apart from the multiple therapeutic advantages offered by neuroimplants, and the potential beneficial effects of the technological-sensory input for the advancement of mental communication research, an individual with neural implants connected to AI could also enjoy fast and high accuracy in terms of "number crunching", access a high-speed, almost infinite knowledge base on the internet, develop an accurate long-term memory and increase his or her sensing ability.

2. K. WARWICK, *Artificial Intelligence: the Basics*, London-New York, Routledge, 2012, 146 and 173-174.
3. According to Kevin Warwick's explanation of how the brain implant *Braingate works*, the electrical activity of a few neurons monitored by an electrode array is decoded into a signal to direct cursor movement. This allowed a patient who voluntarily underwent this neurological monitoring test to position a cursor on a computer screen, using neural signals for control, combined with visual information. The same technique was later used to perform several operations with a robotic arm on a patient suffering from paralysis in one of his arms: K. Warwick, *The Disappearing Human-Machine Divide*, in J. Romportl, E. Zackova, J. Kelemen (eds.), *Beyond Artificial Intelligence. The Disappearing Human-Machine Divide*, Cham-Heidelberg-New York-Dordrecht-London, Springer, 2015, 1-10.

However, despite these promising effects of applying computer engineering and cybernetics in the health sector, we must also consider the reality and the limits of human physiology in relation to the introduction of New Technologies in medicine, in general, and neurology in particular. In this regard, notes Warwick, from a technical point of view, humans can only visualize and understand the world around them in terms of a limited three-dimensional perception, whereas computers are quite capable of handling hundreds of dimensions[4].

It is also useful to know what ethical-legal implications the advance of AI and robotics may have in the field of human freedoms, rights, and obligations (to the point that a recent philosophical debate has been opened on the recognition of a new type of human rights: "neurorights")[5]. There are two research projects aimed at creating a cutting-edge infrastructure in the field of neuroscience[6], computing and brain-related medicine. The first one is the *BRAIN Project* (acronym for Brain Research through Advancing Innovative Neurotechnologies), led by Spanish scientist Rafael Yuste and funded by the US government in 2013. The second one is the European project *Human Brain Project*. The two projects share an aim to "map" neural activity by means of neuroimaging techniques to decipher the neural interconnection of the human brain[7].

In an article recently published in the magazine *Horizons,* under the title: "It's time for neurorights", its authors, including Rafael Yuste, are convinced that the technological advances that will mark the transition of the individual towards the universe of the singularity are not only redefining human life but are even transforming the role of human beings in their social life. In the

4. *Ivi*, 5.
5. The first allusion to neurolawyers was made by J. Sherrod Taylor, J. Anderson Harp and Tyron Elliot in an article on the growing collaboration between neuropsychologists and neurolawyers entitled precisely thus: "Neuropsychologists and neurolawyers", *Neuropsychology* 5 (4), October 1991, 293-305. However, it has been Marcello Ienca and Roberto Andorno who, strictly speaking, have expressly referred to the term "neurorights" in an article entitled *A New Category of Human Rights: Neurorights*, 2017, available at *http://blogs.biomedcentral.com/bmcblog/2017/04/26/new-category-human-rights-neurorights/*
6. Neuroscience acquired a charter at the San Francisco Congress entitled "Neuroethics: Mapping the Field", held May 13-14; cf., S.J. Marcus, *Neuroethics. Mapping the Field*, New York, The Dana Press, 2002.
7. V. Morente Parra, *La inteligencia híbrida: ¿hacia el reconocimiento y garantía de los neuroderechos?*, in F.H. Llano Alonso, J. Garrido Martín (eds.), *Inteligencia Artificial y Derecho. El jurista ante los retos de la era digital*, Cizur Menor (Navarra), Thomson Reuters Aranzadi, 2021, 265.

field of biomedical engineering, neurotechnology (a set of tools or methods to enhance and stimulate brain activity) is the field in which the alteration of the meaning of what we have hitherto considered essentially human is being most profoundly verified. It is no coincidence that the brain is the organ responsible for generating all our mental and cognitive activity[8].

Undoubtedly, the transformational potential of neurotechnology implies an improvement in living conditions in the short- to medium-term and makes it possible to conceive of a longer-term leap in the evolution of the human species. On the other hand, neurotechnology's transformation of human nature has raised a debate on the need to create a specific legal framework that serves to recognize and protect a new catalog of human "neurorights"[9].

It is easy to imagine the multiple advantages offered by neurotechnologies applied to health sciences. Let us think, for example, of the brain-computer interface (BCI: *brain-computer interface*), a communication system that monitors brain activity and enables people with disabilities or degenerative diseases that reduce or prevent their mobility to interact through a device[10]. It cannot be overlooked that neurotechnology also has a reverse side. It can also be used for purposes that are completely spurious and harmful to human rights, as in the case of mind control of the enemy in the military sphere, such as the torture of prisoners of war to extract information. Generally, this also includes any of the other cases in which, according to scholars who

8. R. Yuste, J. Genser, S. Herrmann, *It's Time for Neurorights. Horizons*, in *Journal on International Relations and Sustainable Development. The (Not So) Roaring Twenties?*, n. 18/2021, 154-165.

9. Section XXVI of the Charter of Digital Rights (which is not legally binding, but which does have a prospective objective with respect to the application and interpretation of rights in the digital environment in the immediate future) sets out the purposes to which digital rights are oriented in the use of neurotechnologies (purposes that some consider directly as the five fundamental neurorights): (a) guaranteeing each person's control over his or her own identity; (b) guaranteeing individual self-determination, sovereignty and freedom in decision-making; (c) ensuring the confidentiality and security of data obtained or relating to his or her brain processes and the full mastery and disposal thereof; (d) regulating the use of person-machine interfaces liable to affect physical or psychological integrity; (e) ensuring that decisions and processes based on neurotechnologies are not conditioned by the provision of incomplete, unwanted, unknown or biased data, programs or information. Official information on this document can be found at *https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf*.

10. R. De Asís Roig, *Una mirada a la robótica desde los derechos humanos*, Instituto de Derechos Humanos "Bartolomé de Las Casas" de la Universidad Carlos III de Madrid-Dykinson, Madrid, 2014, 35-36.

advocate the "criminal law of the enemy" (*Feindstrafrecht*), would justify the legalization of the use of neurotechnology to interfere in the will of those who do not deserve to be treated as persons, but as enemies of society[11].

But without going as far as to consider such extreme scenarios in the use of neuroscience as those just mentioned, access to the information stored in the human brain could also pose ethical-legal dilemmas in the field of labor relations. In this sense, one might wonder what would happen if a hiring algorithm discriminated against a potential employee of a company because it misinterpreted his or her brain data because algorithms are capable of developing biases that mimic those humans have, such as race or gender[12].

In the above cases, it is demonstrated that neurotechnology whether for therapeutic or malicious purposes can be subject to intentional or accidental abuse by those who employ it. In this era of technological revolution, marked by the omnipotence and omnipresence of AI, neither the right to personal identity (understood as the set of attributes and characteristics that make it possible to individualize a person in society), nor free will, nor mental privacy, nor equitable access to neuro-potentiation, nor protection against bias and discrimination caused by the erroneous or self-interested use of neuroscience can be taken for granted. For this reason, in view of the need to protect the rights and freedoms of citizens in the face of the possible invasive and perverse use of neurotechnologies, a debate has begun on the advisability of creating a legal framework to safeguard neurorights. In this sense, this neuroscientific initiative of Rafael Yuste and the *Neurorights Foundation* has especially resonated in Chile, where it has inspired a constitutional amendment (Law 21.383, D.O. 25-10-2021) to reform Article 19.1 of the Political Constitution of Chile and the implementation of laws to define and delimit the conditions under which the processing of brain data could be carried out. This initiative has also inspired a draft bill for the neuroprotection of mental identity, recognizing a new human right which characterizes the brain and its functionality as the nucleus of free will, thoughts and emotions that characterize and differentiate the human species[13].

11. G. Jakobs, M. Polaino Orts, *Derecho penal del enemigo: fundamentos, potencial de sentido y límites de vigencia*, Barcelona, Bosch, 2009.
12. R. Yuste, J. Genser, S. Herrmann, *It's Time for Neurorights. Hori*zons, cit., 159.
13. H. López Hernández, *Neuroderecho, neuroabogado, neurojusticia: una realidad innegable*, in S. Barona Vilar (ed.), *Justicia algorítmica y neuroderecho. Una mirada interdisciplinar*, Valencia, Tirant lo Blanch, 2021, 95.

In any case, as has become clear in this new constituent process in Chile, the discussions held in connection with the approval of this bill on neurorights have served to make visible the arguments of two distinct sides. On the one hand, we find those who consider the recognition of a new generation of rights a priority, that is, a fourth generation of human rights, framed in the category of digital rights. And on the other hand, we find those who understand that legislating in a technological-scientific context is still so premature, speculative, and hypothetical that it would be counterproductive in legal-political terms. This latter position defends that the eventual recognition of such a reduced and specific catalog of neurorights would contribute to the inflation and relativization of the human rights that are already consolidated. Instead, they advocate a reformulation of the existing rights that would update and adapt them to the *momentum* of digital transformation that technological society and, particularly, the world of law, is undergoing.

In the face of the antagonistic positions held by the apocalyptic and the integrative perspectives on the New Digital Technologies, there are those who appeal to "technological responsibility", a reflective and critical attitude towards the new problems raised by science and technology, before which neither democracy, nor science, nor law, nor the humanities can remain impassive, especially because of their repercussions on the scope and exercise of human rights[14].

II. THE NEW GENERATION OF DIGITAL RIGHTS AND THE RECOGNITION OF NEURORIGHTS

Since its origin and development in the nineties, the internet has become the world's leading communication network. Although it offers many advantages and benefits in terms of access to a huge amount of data and information, we should not overlook the transformation that the digital space model is undergoing. Such a transformation, for reasons of cybersecurity and global market interests, is not only modifying the open, free, and neutral nature with which the internet was created, it is also affecting the privacy and identity of its millions of users (social media derived *Big Data* establishes patterns of behavior and profiles its millions of users by collecting not only their personal data, but also their beliefs and emotions). In this regard,

14. A.E. Pérez Luño, *Los derechos humanos en la sociedad tecnológica*, Madrid, Editorial Universitaria, 2012, 42-43.

Moisés Andrés Barrio comments that much of our daily life has migrated to the internet to such an extent[15].

We usually refer to the Internet of all things to refer to the access to such an immeasurable amount of data and information that it makes available to users unlimited sources of knowledge without precedent in history. However, digital transformation should also guarantee the improvement of democracy and the exercise of citizens' rights. In other words, it is not enough to conceive of the internet as an artificial universe through which millions of data circulate, but also as a space in which we are guaranteed protection and the free exercise of our rights in the digital sphere.

As a result of the impact of this revolution in the world of law, a new generation of rights has emerged whose main objective is to correct the problems and damage caused to citizens due to the lack of appropriate regulation capable of establishing a specific legal framework for the use, deployment and development of the internet, AI, robotics, and related digital technologies. It is about digital rights, rights conceptually based on a virtual support, not analogical, where the body is volatilized to give way to a different structure of rights that must seek the security of the person on the processing of data and the mathematical architecture of algorithms[16].

Article 18.4 of the Spanish Constitution, inspired by Article 35 of the Portuguese Constitution of 1976, was a novelty in establishing the legal limit to the use of information technology to guarantee the honor and privacy of citizens. This constitutional precept would lead to the development of a body of norms and an important line of case law on data protection. However, data protection is neither sufficient nor does it exhaust all the options to satisfy the necessary establishment of a framework for guaranteeing and effectively protecting the rights and freedoms of citizens in the digital era. Two pieces of legislation were passed to address such issues, Organic Law 3/2018, of December 5, on Personal Data Protection and Guarantee of Digital Rights; and more recently, the Charter of Digital Rights (CDD) which, despite lacking legal enforceability, has the value of serving as a reference for a future law regulating digital rights. The rights recognized by the CDD include rights protecting people from AI and neuroscience (which could open the way for the future recognition of neurorights).

15. M. Barrio Andrés, *Génesis y desarrollo de los derechos digitales*, in *Revista de las Cortes Generales* 110, 2021, 197-233.
16. *Ivi*, 209.

Rafael Yuste and Sara Goering have expressed their concern regarding the recognition of neuro-rights, especially since the convergence of the development of neurotechnologies which directly link human brains with AI. They have pointed out that the development of devices marketed by neurotechnology companies in the general consumer market should be done in accordance with ethical principles and following minimum standards of quality and good practice, meaning that, when implanted, they are non-invasive and present the least possible risk to people. In relation to connecting the human brain and machines equipped with AI, either through neuroimplants[17]have identified *four concerns* related to the need for the development and application of new neurotechnologies. They propose, for example, that deep brain stimulation and brain-computer interface, need to be carried out in accordance with the ethical principles of neurotechnology and AI, so that respect and preservation of the ethical principles of neurotechnology and AI can be guaranteed, ensuring[18].

These authors' first concern is the effects that the interaction between neuroscience and AI may have on safeguarding privacy and respecting the consent of patients who do not wish to share their neural data. In this regard, they propose to regulate the sale, commercial transfer and use of neural data (a regulation similar to the *US National Organ Transplant Act* of 1984). Another measure to protect the privacy of the user of neurotechnologies could be the application of techniques based on *blockchain* and *smart contracts* that provide, without the intermediation of a centralized authority, transparent information on how the neural activity data of individuals are being managed.

Rafael Yuste and Sara Goering's second concern is the hypothesis that neurotechnologies and AI may alter people's sense of identity and rational agency and may even subvert the very nature of the self and the moral and legal responsibility of the individual. Indeed, if the loss of our sense of agency and identity eventually occurs (e.g., through neural control devices that remotely monitor thought or through the interconnection of several brains working together), individuals could end up behaving in a way that is alien to their true personality, to the point that they would not be able to recognize themselves in their actions. As a possible solution to this second concern, Yuste and Goering propose the inclusion of neuro-rights

17. The Morningside Group is comprised of neuroscientists, neurotechnologists, physicians, ethicists and artificial intelligence engineers.
18. R. Yuste, S. Goering et al., *Four ethical priorities for neurotechnologies and AI*, in *Nature*, 551, 2017, 159-163.

protective clauses in international treaties and the creation of an international convention to define prohibited actions related to neurotechnology and AI, similar to the prohibitions enumerated in the International Convention for the Protection of All Persons from Enforced Disappearance (which entered into force on December 23, 2010).

The third reason for concern of the authors linked to the Morningside Group has to do with the increased cognitive capacity and neuro-potentiation that is currently one of the spearheads of technological transhumanism. In this regard, Laurent Alexandre, a prestigious French physician and transhumanist neurobiologist, has warned that the only way out for humanity in the face of the inevitable advent of the technological singularity is to "co-evolve" with machines and technologically enhance the human brain to adapt it to the strong AI that, according to his prognosis, will determine the posthuman future[19]. Against this backdrop, Yuste and Goering consider it likely that the pressure to adopt enabling neurotechnologies will reach such a level that it will end up changing social uses and rules from an ethical-political point of view, and even create problems of equitable access and new forms of discrimination (technological divide). For this reason, both authors propose establishing ethical and legal limits to the development of neurotechnologies and defining the contexts in which they can be applied (as is the case, for example, with gene editing in humans), but without imposing absolute prohibitions on certain technologies (such as those that stimulate and enhance the human brain), which would only serve to push them into clandestinity.

The fourth concern shared by Rafael Yuste and Sara Goering is that of biases or prejudices that are so influential, for example, in the selection or decision-making processes in which an infinite amount of workers' personal data is collected through data mining and algorithmic discrimination techniques that are put at the service of those responsible for optimizing a company's human resources (*workforce analytics*). In this regard, it should be noted that, as Serena Vantin points out, the use of algorithmic tools in the labor and business sphere is not only limited to workforce analytics techniques, but also extends to the digitization of production processes, gig economy services (an online contracting formula that is absolutely flexible for both employer and employee and is presented as an alternative to the

19. L. Alexandre, *La guerra delle intelligenze. Intelligenza artificiale contro intelligenza umana*, transl. it., N. Nappi, Turin, EDT, 2018, 291 ff.

traditional fixed-term contract model), new techniques for monitoring employees by employers during working hours, etc.[20].

As we can see, the enormous potential offered by the use of algorithms to facilitate citizens' access to a more transparent and efficient public administration, to guarantee our security and the exercise of our rights, or to boost the modernization of companies, also has a dark side, implying risks of digital discrimination both in the network and in AI systems, robotics and related technologies[21]. On the other hand, discriminatory biases, prejudices contrary to dignity and the right to equality, and algorithmic errors do not harm the entire population uniformly but tend to particularly affect the most vulnerable groups and the most disadvantaged individuals within society[22].

Regarding discriminatory biases, Yuste and Goering recommend the participation of likely users – especially those who are marginalized – in the design of algorithms and devices from the very first stage of technological development precisely to avoid situations of discriminatory biases in algorithmic decision-making systems. In recent years, some scholars specializing in algorithmic decision-making processes are investigating how to reverse the use of selective algorithms in a fair sense and in accordance with the guarantee of transparency contemplated in the European digital strategy[23]: I am referring here to the *Critical Data Studies*[24].

A good synthesis of the current theoretical debate on the need to build a theory of neurorights as human rights is provided by Rafael de Asís in his book *Derechos y tecnologías*[25]. As highlighted in this monographic study, there

20. S. Vantin, *Il diritto antidiscriminatorio nell'era digitale. Potenzialità e rischi per le persone, la pubblica Amministrazione, le imprese*, Milano, Wolster Kluwer, 2021.
21. S. Pietropaoli, *Cyberspazio. Ultima frontera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in *Rivista di Filosofia del diritto*, n. 2/2019, 379-400.
22. *Ivi*, 96.
23. Within the framework of the European institutions there are some studies on the algorithmic decision-making procedure; see, for example, in this regard: "Understanding Algorithmic Decision-making. Opportunities and Challenges", 2019, available at: *https:// www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf*; "A Governance Framework for Algorithmic Accountability and Transparency", 2019, available at: *https:// www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf*; on the digital strategy "Shaping Europe's Digital Future", 2020, available at:, *https:// ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf*.
24. N. Lettieri, *Antigone e gli algoritmi. Appunti per un approccio giusfilosofico*, Modena, Mucchi, 2020, 54-55.
25. R. De Asís Roig, *Derechos y tecnologías*, Madrid, Dykinson-Departamento de Derecho Internacional Público, Eclesiástico y Filosofía del Derecho de la Universidad Carlos

is an incipient Ibero-American doctrinal line that advocates the recognition of a new generation of human rights, based on the proclamation of the five neurorights proposed by Rafael Yuste, Jared Genser and Stephanie Herrmann[26][27].

Enrique Cáceres Nieto, Javier Díaz García and Emilio García García are representative of the position in favor of the recognition of the ethical-legal aspect of neurorights and their formal incorporation into the legal system, as well as their recognition as belonging to a fourth generation of human rights[28]. This theoretical line in favor of the recognition of neurorights also has an institutional framework of regional *soft law* the Declaration of the Inter-American Committee on "Neuroscience, Neurotechnologies and Human Rights: New Legal Challenges for the Americas"[29] and follows the same path previously traced by a doctrine in favor of the adoption of a Universal Declaration of Human Neurorights[30].

Other scholars are more reluctant to propose expanding the catalog of human rights, arguing that the profusion of human rights generates problems of indeterminacy and incoherence in their substantiation, and may weaken their effectiveness by overlapping with human rights of previous generations. In this sense, Francisco Laporta's position against lowering the rigor in the process of recognition of new human rights (such as those related, precisely, to New Technologies) is eloquent. In this regard, Laporta points out:

III de Madrid, 2022.

26. The five neurorights proposed by Yuste, Genser and Hermann are: 1.- the right to identity, or the ability to control our physical and mental integrity; 2.- the right to freedom of thought and free will to decide how to act; 3.- the right to mental privacy, or the protection of our thought from disclosure; 4.- the right to fair access for the enhancement of the mind's potential, i.e., the ability to guarantee that the benefits of sensory and mental capacity enhancements through neurotechnology are distributed fairly across the population; and 5. the right to protection against algorithmic bias, or the guarantee that technologies do not introduce bias.
27. R. Yuste, J. Genser, S. Herrmann, *It's Time for Neurorights. Horizons*, cit., 160-161.
28. E. Cáceres Nieto, J. Díaz García, E. García García, *Neuroética y neuroderechos*, in *Revista del Posgrado en Derecho de la UNAM* 15, 2021, 37-86.
29. This Declaration was adopted following the meeting held by the Inter-American Juridical Committee on August 2-11, 2021, during its 99th regular session, and was published on August 4 of the same year. The text is available at the following address: *https://kamanau.org/wp-content/uploads/2021/08/Neuro-derechos-doc-641-rev-1-esp-DN-ROA.pdf*.
30. P. Sommaggio, M. Mazzocca, A. Gerola, F. Ferro, *Cognitive liberty. A first step towards a human neuro-rights declaration*, in *BioLaw Journal-Rivista di BioDiritto*, n. 3/2017, 27-45.

It seems reasonable to assume that the longer the list of human rights is, the less force they will have as claims, while the stronger moral or legal force they are attributed, the more limited the list of rights that adequately justify them must be[31].

Regarding the overlapping of neurorights in relation to the rights and freedoms enshrined in the Universal Declaration of Human Rights (UDHR), there are scholars who argue that their recognition is not justified if the legal goods that neurorights seek to guarantee (privacy, intimacy, liberty, human dignity and equitable access to scientific resources) have already been recognized and guaranteed in the UDHR, as well as in subsequent international covenants and conventions[32].

In an intermediate position within this debate on the opportunity for the recognition of neurorights, Rafael de Asís is perplexed by the fact that in the process of incorporating the New Technologies in the educational sphere, human rights education is being left aside or even rejected (the necessary technological training of our students is not only not incompatible, but complementary to training in the humanities and the transmission of the culture of human rights)[33]. In any case, concludes de Asís, the application to social issues of New Technologies, in general, and of neurotechnologies, in particular, «is a reality that should be faced»[34].

---

31. F. Laporta San Miguel, *Sobre el concepto de derechos humanos*, in *Doxa*, 1987, 23-46.
32. V. Morente Parra, *La inteligencia híbrida*, cit., 273; in analogous sense, cfr., D. Borbón Rodríguez, L.F. Borbón Rodríguez, J. Laverde Pinzón, *Critical analysis of the NeuroHuman Rights to free will and equal access to enhancement technologies*, in *Ius et Scientia* , n. 2/2020, 135-161.
33. Regarding the importance of human rights education, Manuel Atienza points out that although knowledge and education alone are not enough to put an end to evil in the world, they are nevertheless essential: «the reading of the texts containing the declarations of human rights, the reflection on the various problems they raise and, in general, the incorporation of this subject (theoretical and practical) into the curricula of schools and universities and its presence in public discussion forums will probably not achieve a significant effect of persuasion on the great powers (partly public but, above all, private) of this world, which are mainly responsible for the fact that these rights are not guaranteed for a vast majority of the inhabitants of the planet. But all of this can contribute to making many people aware of the rights they can legitimately claim (and the duties they must assume) and of the causes that prevent them from being fulfilled. And if this enlightened moral conscience were sufficiently generalized, it would most likely become a socially irresistible force as well» (Atienza 2020: 152).
34. R. De Asís Roig, *Derechos y tecnologías*, cit., 148-152; see also, by the same author, *Sobre la propuesta de los neuroderechos*, in *Derechos y libertades. Revista de Filosofía del Derecho y derechos humanos*, 47, 2022, 51-70.

Therefore, rather than a repetition of rights under different labels, it would be a matter of further concretization within the so-called specialization phase of human rights. This implies a historical approach to rights, that is, their placement in a diachronic or evolutionary dimension over time. In accordance with the thesis of the historical mutation of human rights (*Wandel der Grundrechte*), rights should not become fossilized concepts within a timeless catalog incorporated into a list with *numerus clausus*. As Antonio E. Pérez Luño warned in the 1980s, in line with the generational conception of human rights, the new generation of rights and freedoms is presented as a response to the process of erosion and degradation that afflicts fundamental rights in the face of certain uses of the New Technologies (a problem to which the Anglo-Saxon doctrine refers with the term *liberties' pollution*). The considerations made by Pérez Luño, regarding the "information society" and the priority interest in the legal regulation of the use of information technology, could well be extended today to the technological society and the need to establish a legal framework around the use of new NBIC technologies and the development of AI and advanced robotics[35].

In the following section I will focus on personal identity (the set of specific traits that make a person unique) in the face of the challenges posed by the digital metaverse. The concept of identity acquires its full meaning when complemented by new rights and freedoms, such as the right to free development of personality, mental integrity and cognitive freedom (the freedom to control one's own conscience). The latter, by the way, is closely linked to the classic freedom of thought[36], although adapted to the circumstances of the 21st century, and it has been defined by Richard G. Boire as "the quintessence of freedom"[37].

III. WHEN A PERSON BECOMES AN AVATAR: THE NOVO HOMO LUDENS IN THE INTERNET METAVERSE

Reference has been made above to the hopes opened up by new neurotechnologies, such as deep brain stimulation (DBS) and brain-computer interface (BCI), in the prevention, treatment and cure of diseases such as Parkinson's, epilepsy, ALS or obsessive-compulsive disorder (OCD).

35. A.-E. Pérez Luño, *Concepto y concepción de los derechos humanos: (Acotaciones a la ponencia de Francisco Laporta)*, in *Doxa* 4, 1987, 47-66.
36. W. Sententia, *Neuroethical Considerations: Cognitive Liberty and Converging Technologies for Improving Human Cognition*, in *Annals of the New York Academy of Science* 1013, 2004, 221-228.
37. R.G. Boire, *On cognitive liberty III*, in *Journal of Cognitive Liberties*, 2001, 7-22.

However, the detrimental effects that these devices can have on a person's identity, authenticity and autonomy should not be overlooked. For better or worse, the fact is that these devices are capable of interfering with the self-awareness and altering the agency of the individuals in whom they are implanted[38].

By invoking the sovereignty of our mind as an innate and non-acquired right, we are also appealing to the inalienability of our personal identity, the inviolability of our physical and mental integrity, the preservation of our authenticity, the ability to freely decide our actions (a faculty also known as "agential control"), and the autonomy of our will[39].

The problem appears when the individual unconsciously loses control of his autonomy due to external factors or agents that interfere with his mental faculties, cloud his judgment and direct his behavior[40]. This inadvertent manipulation of the individual agent would break the psychological continuity by introducing a hiatus between the agent's current preferences and those he had ingrained in his personality when he was a psychologically autonomous subject until such interference from the outside occurred[41].

The line between habit and dependence of the *phono sapiens* (the *novo homo ludens*) on the electronic and digital devices he uses in his daily life is so thin at times that it is not easy to differentiate, and the apparent freedom of choice to use his fingertips on the surface of the screen of his laptop, cell phone or tablet is nothing more than "a consumerist selection"[42].

In these daily intervals of man's absence from his reality, in this detachment from his circumstances and from the things of the real world, and in his power to withdraw virtually and temporarily from the world and to withdraw into himself, there occurs a phenomenon characteristic of the human being that

38. S. Goering, T. Brown, E. Klein, *Neurotechnology Ethics and Rational Agency*, in *Philos Compass,* 2021.
39. J.C. Bublitz, *My Mind is Mine!?*, in E. Hildt, A. Francke (eds.), *Cognitive Liberty as a Legal Concept. Cognitive Enhancement*, Berlin, Springer, 2013, 233-264.
40. J.C. Bublitz, R. Merkel, *Autonomy and Authenticity of Enhanced Personality Traits*, in *Bioethics*, 2009, 360-374.
41. A.R. Mele, *Autonomous Agents. From Self-Control to Autonomy,* Oxford/New York, Oxford University Press, 1995, 187; I. Hagi, *Moral Appraisability. Puzzles, Proposals and Perplexities*, Oxford/New York, Oxford University Press, 1998, 108 ff; T. Kapitan, *Autonomy and Manipulated Freedom, Philosophical Perspectives*, in *Action and Freedom* 14, 2000, 81-103.
42. B.-C. Han, *No-cosas. Quiebras del mundo de hoy*, Spanish trans J. Chamorro Mielke, Barcelona, Taurus, 2021, 24.

other animals lack: "self-absorption"[43]. For Ortega y Gasset this act of self-absorption ("ensimismamiento"), a strategic withdrawal into oneself, is a privilege with which man manages to free himself temporarily from things precisely through the mastery of technology. Ortega understands that the initial mission of technology consists precisely in «giving man the freedom to commit to being himself», that is, to create an extra-natural space of leisure (*otium*) that enables him to entertain activities beyond the satisfaction of elementary needs, such as imagining, inventing and creating, both in the sciences and the arts[44].

Just as Sartori denounced in *Homo videns,* the influence that the media, and especially television, exerted on the masses, a quarter of a century later we find ourselves in a similar situation of alienation on the part of the *novo homo ludens*, with the only exception that now it is the NBIC neotechnologies under the domination of *Big Tech.* Such technologies surround the individual and direct and control his daily habits and even his will, as if he were a puppet moved by the metadata and algorithms that make up the inscrutable universe of the internet. This situation brings man closer to what Ortega calls "alteration", which is typical of the animal life and distances him from human self-consciousness and self-absorption. Ortega explains it beautifully in *Ensimismamiento y alteración*:

To say, then, that the animal does not live from *itself* but from *the other*, brought and carried and tyrannized by *the other*, is equivalent to saying that the animal lives always altered, alienated, that its life is a constitutive *alteration*[45].

Regarding the alienation and alteration of the contemporary man, Sartori warns that ours is an extraordinary era in which those who still have that critical capacity of thinking beings have the duty to denounce the irresponsibility and unconsciousness of the growing legions of snake oil salesmen who forget that what we live and will live is not "nature" (a given thing that is there forever) but is from end to end an artificial product constructed by *homo sapiens*. Can it be sustained without your support? No, surely not. And if we heed the false prophets who are bombarding us with

43. J. Ortega y Gasset, *Ensimismamiento y alteración* (1939), in *Obras completas. Volume V (1932/1940)*, Madrid, Fundación José Ortega y Gasset/Taurus, 2006, 529-550.
44. J. Ortega y Gasset, *Meditación de la técnica* (1939), in *Obras completas. Volume V (1932/1940)*, Madrid, Fundación José Ortega y Gasset/Taurus, 2006, 551-605.
45. *Ivi*, 535.

their multi-messages, we will quickly arrive at a virtual world that turns upside down in a "real catastrophe"[46].

The expansion of digital space beyond the limits imagined by Giovanni Sartori more than twenty years ago has not only blurred the tenuous line of separation between nature and virtual reality that the Florentine philosopher and political scientist already discerned with difficulty, but in some areas, it is even absorbing human identity. I am referring to the virtual world of the metaverse, 3D augmented reality with 5G capability, Artificial Intelligence, and the imminent development of the Internet of the senses, which aims to use the brain as an interface, modulate the world of sound around us with micro-implants, personalize the taste of food or even recreate (or create *ex novo*) aromas and other digital senses such as touch.

Human reality seems to have been surpassed by the mechanical fiction of the digital world when it is already possible to conceive friendship and even virtual love with a machine developed by AI, or with a fantasy character or avatar designed virtually. This is, by the way, a trend in Japan, as evidenced by the curious or rather bizarre case of Mr. Akihito Kondo, married to a manga singer named Hatsune Miku with millions of fans. This would not be peculiar except for the fact that she is a hologram that has virtual "existence" as *Vocaloid* (or virtual singer) in a device called Gatebox. Not only does the device provide Miku with "life" as some sort of sentimental *tamagotchi*, but it has even enabled the formalization of a marriage between a man and a hologram in a document without legal validity. Regarding this confusion between human reality and digital fiction, a recent study on the ethical-legal effects of human dissociation has warned that when human identity tries to connect with a cybernetic fetish, it is a sign that there is an inexorable propensity to descend into the realm of the virtual and to forget the consciousness of human identity on the digital continent (something akin to entering a trance that plunges us into a technologically induced digital dream)[47].

Apart from the mirage produced in the human psyche by virtual reality, and the interaction between the human figure outlined and reproduced in the digital continent recreated by the metaverse, interfaces and 3D video games, the truth is that humans and machines are not ontologically equal, nor do they belong to the same category: holograms are three-dimensional

46. G. Sartori, *Homo videns. La sociedad teledirigida*, Barcelona, De Bolsillo, 2018, 197.
47. R. Curcio, *Identità cibernetiche. Dissociazioni indotte, contesti obbliganti e comandi furtivi*, Roma, Edizioni Sensibili alle foglie, 2020.

images configured with numbers and algorithms, while human beings are made of flesh and blood, *ratio et emotio*[48].

The increasingly thin line of separation between the natural-real world and the digital-artificial universe is a warning to us about the need to preserve human identity. Therefore, returning to the diatribe on whether or not to recognize neurorights, it seems reasonable to at least ask whether, perhaps, given the loss of awareness of reality by the *novo homo ludens*, it would not make sense to protect at least the first of these neurorights, i.e., the right to identity, or the ability to control our physical and mental integrity.

According to the criterion of the generational perspective of human rights, whose catalog does not consist of a closed list of rights and freedoms, but of a list open to the most pressing changes and problems affecting contemporary man in the era of new technologies[49], a fourth generation could be added, which would include precisely the right to human identity. In the same way that the first generation would correspond to individual rights and freedoms; the second to economic, social and cultural rights; and the third to the fundamental legal-subjective guarantees of the technological era; and just as each of these generations would correspond to the guiding values of freedom, equality and solidarity, respectively[50], we could conclude that the fourth generation would refer to those rights and freedoms that protect the human condition in the face of the onslaught of technological transhumanism, and whose guiding principle would be precisely human dignity.

The fourth generation of human rights is justified in a virtual scenario, determined by AI, and integrated by virtual recreations that provoke in the internet user the hallucination of interacting with non-things that neither *exist* as physical reality nor *are placed* in it, but that increasingly influence his daily routine and even his behavior. The actions of the individual in the digital environment, however artificial, have legal consequences that bind him. For example, the *blockchain* technology has made it possible to create

48. I.D. Illich, *L'alfabetizzazione informática e il sogno cibernético*, in *Nello specchio del passato*, Milano, RED Edizioni, 1992; R. Curcio, *Identità cibernetiche,* cit., 56.

49. K. Vašák, *Pour les droits de l'homme de la troisième génération*, Strasbourg, Institut International des Droits de l'Homme, 1979; see also, by the same author, *Les différents catégories des droits de l'homme*, in *Les dimensions universelles des Droits de l'Homme*, in A. Lapeyre, F. De Tinguy, K. Vašák (eds.), Brussels, Unesco-Bruylant, 1990, 297.

50. A.E. Pérez Luño, *La tercera generación de derechos humanos*, Cizur Menor (Navarra), Thomson/Aranzadi, 2006, 232; see also, by the same author, *Derechos humanos, Estado de Derecho y Constitución*, Madrid, Tecnos, 1984 (201812), 692-702.

smart contracts (*smart contracts*) written in virtual language, whose execution is autonomous and automatic, based on programmed parameters, and which offer conditions of security, transparency and trust to the contracting parties that are superior to those of traditional contracts in which the risk of misunderstandings, forgery or alterations is greater. This same binding nature of contracts and legal transactions which has entered into in the digital space can be seen in the growing field of cryptocurrencies (not exempt from the risk of speculation and consequent devaluation) and NFTs (non-fungible digital assets), created with cryptographic *tokens* just like cryptocurrencies to determine their authorship and uniqueness, and which have revolutionized the digital art market to the point that in the last year their sales and even their value have multiplied exponentially (in 2021, Jack Dorsey, co-founder of Twitter, sold the first tweet in the history of his company for 2.95 million dollars, and the digital artist Beeple sold an NFT at Christie's for $69 million dollars).

The metaverse is not a recent concept. May we recall that at the beginning of this century, *Second Life*, an online multimedia platform where users created an avatar and built a second digital life, was launched. Over time, this original metaverse designed by the technology company Linden Lab has become a metaverse archetype that would serve as a reference for other metaverses developed later in Web 2.0 and Web 3.0. In short, the metaverse is not about a unitary experience in a compact digital space, but about the migration of human experience from the physical world to numerous virtual worlds in which, as the authors of a recent study on the future legal framework of the metaverse argue, technology has the opportunity to bring content to these worlds in ways never before imagined and, with it, legal problems and challenges never before contemplated[51].

The progressive implementation of the metaverse (in the fields of entertainment, commerce, health and education) has generated a series of assumptions and novelties hitherto unknown in our legal experience. It is true that, in some cases, some existing laws could be adjusted to regulate novel issues raised by the irruption of the New Technologies. However, if one considers the incommensurability of the open space in which the metaverse expands, it can be reasoned that the legal and jurisprudential adaptation to this new virtual reality that is legally binding will not be easy, insofar as the existing laws are already insufficient to regulate the problems

51. T.K. Ara, M. Radcliffe, M. Fluhr, K. Imp, *Exploring the Metaverse. What Laws will apply?*, in *DLA Piper-Chambers TMT*, February 22nd 2022. Available at: *https://www.dlapiper.com/en/latinamerica/insights/publications/2022/02/exploring-the-metaverse/*.

caused in the digital space by a metaverse that has broken the seams of the existing legal systems.

Indeed, as the authors of the paper on metaverse regulation cited above point out, the scope of all the laws and regulations that could be involved in a metaverse is practically unlimited and can generate innumerable legal problems. Thus, for example, in intellectual property matters, the creation of new types of NFTs has caused quite a few controversies and legal queries regarding the scope of the right to use the content held by the owner of the NFT (in the most recent judicial praxis most of the claims regarding metaverse content concern copyrights, trademarks and publicity rights). Moreover, the use and exploitation of previously licensed or acquired intellectual property rights in the metaverse raise novel issues for licensees and acquirers around the extent and scope of the rights they have obtained under agreements that may have long preceded the internet and, to a lesser extent, the metaverse.

The problem of metaverse projects also extends to other legal areas, such as privacy and cybersecurity.

In relation to ensuring privacy in the process of collecting, using and transmitting personal data, metaverses have the ability to collect a wide range of information that can range from basic identifying information to collecting data about the user's movement and activities in the metaverse. In this regard, on the one hand, it is becoming increasingly evident that there is a need to pass legislation dedicated precisely to the protection of privacy in the metaverse and even, along with the opportunity to have a specialized jurisdiction in digital law and legal AI. On the other hand, the creators and developers of metaverse projects should also consider the implementation of measures to ensure compliance with legal requirements of privacy and the observance of minimum ethical-legal standards in the contents of metaverses[52].

Regarding the issue of cybersecurity, metaverse projects also pose new problems and questions for the technology companies that create and develop them, especially in terms of ensuring the protection of their

52. S. Moore, Schuyler, *Law in the Metaverse*, in *Forbes*, December 22nd 2021. Available at: *https://www.forbes.com/sites/schuylermoore/2021/12/22/law-in-the-metaverse/?sh=2a431fab45d1*.

information systems and the processing of their users' personal data in the event of a cyberattack[53].

In short, although the metaverse is still in an initial phase of technological implementation, as its use evolves and expands, both within the professional and private spheres, it is presumable that the number of incidents and claims among users will also increase. It is precisely for this reason that a regulatory framework which anticipates – as far as possible – legal responses to the new legal problems presented by the metaverse needs to be established[54].

IV. CONCLUSION

The impact of the technological revolution 4.0 on rights and freedoms goes beyond the scope of the three previous generations of rights and freedoms, because now contemporary man is not alone in the face of technology but coexists in the digital space with other entities and other types of intelligences that are not strictly human, but transhuman and/or artificial. The post-human scenario that is opening up before us is, therefore, more complex and uncertain than the one that responded to the humanist paradigm and the anthropocentric canon in which it was possible to give birth to a phase of splendor for the humanist project of modernity and which Norberto Bobbio defined as "the time of rights" (*l'età dei diritti*). This new post-human scenario brings us face to face with major questions and challenges such as human identity and the metaverse, the legal status of robots, the regulation of digital space, the foundations of an ethics of AI, or the metamorphosis of law and justice. In short, it places us before a world in which, as Luciano Floridi warns, humanity will try to transform a hostile artificial environment into a technologically adapted *infosphere* in which it will progressively lose its protagonism. Indeed, this author points out, in this new digital habitat we will share virtual space «not only with other forces and sources of natural, animal and social action, but also and above all with artificial agents[55].

The digital revolution, to paraphrase Antonio Gramsci, represents a form of *cultural hegemony* that has not only managed to impose itself on modern

53. R. Brighi, *Cybersecurity. Dimensione publica e privata della sicurezza dei dati*, in T. Casadei, S. Pietropaoli (eds.), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, Wolster Kluwer, 2021.
54. T.K. Ara, M. Radcliffe, M. Fluhr, K. Imp, *Exploring the Metaverse*, cit.
55. L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, Rafaello Cortina Editore, 2022, 58.

societies as a cultural universe of reference, but also as a dominant idea that we have all internalized and made our own in some way. The 4.0 revolution, which according to Floridi, dates back to Alan Turing, places us in a context of metamorphosis of the world where the preservation of the human essence is at stake in the face of the horizon of a technological singularity, in which "intelligence is no longer only a human prerogative but also artificial and digital"[56].

56. G. Balbi, *L'ultima ideologia. Breve storia della rivoluzione digitale*, Roma-Bari, Laterza, 2022, 42.

[1]Rights in the age of data*

[2]Thomas Casadei**

SUMMARY: I. FROM THE "AGE OF RIGHTS" TO THE "AGE OF DATA"? - II. RECONFIGURATION OF CONCEPTS AND/OR CONFIGURATION OF A NEW PARADIGM? - III. THE CHALLENGE OF TRUSTING (HUMAN) RIGHTS

ABSTRACT: The current age is often and repeatedly defined as the "age of data" (and of digitalisation, a digital age), a phase that, according to some interpretations, seems to have left behind what Norberto Bobbio called the "age of rights".

Given the pervasiveness of data, the human being can even be thought of as an 'open-air mine' that binds him or her to the logic of calculation, in which algorithms seem to be able to exercise unlimited power, which some read as an 'algocratic drift'.

However – so the thesis of the contribution – rights can be claimed, once again and in a new historical phase, as an ideal and institutional reference, thus underpinning and substantiating all the regulatory instruments available to public powers, as well as those that can be elaborated in response to new needs "whose recognition and protection is demanded".

Finally, according to Bobbio, rights are always historical, marked by struggles, and there are always only two ways of dealing with powers: "either to prevent their evils or to obtain their benefits".

---

* *I would like to thank once again Stefano Pietropaoli, an invaluable reader of my reflections on the impact of "information technologies" and "digital issues". I would also like to thank Adalgiso Amendola, Barbara G. Bello, Giovanni Bisogni, Raffaella Brighi, Anna Cavaliere, Ylenia Curzi, Alfredo D'Attorre, Antonio Di Stasio, Tommaso Fabbri, Gianluigi Fioriglio, Valeria Giordano, John Patrick Leech, Fernando H. Llano Alonso, Francesco Mancuso, Sandro Luce, Rosaria Pirosa, Iacopo Senatori, for their useful suggestions, which allowed me to clarify some points of the discussion.*

** Full Professor in Philosophy of Law, University of Modena and Reggio Emilia.

KEYWORDS: Norberto Bobbio; data; rights; regulation.

I. FROM THE "AGE OF RIGHTS" TO THE "AGE OF DATA"?

This chapter could have been titled "Rights in the (Big) Data Society"[1], or "Rights in the Global Digital Society"[2], or "Rights in the Algorithmic Society"[3], or "Rights in the Network Society", or "in the Information Society"[4], or even "Rights in the Knowledge Society"[5], although the latter title would have been a more appropriate title a few years ago.

However, I prefer "Rights in the Age of Data", in order to frame what is appropriately defined as an epochal transition that places data at the centre

1. N. Japkowicz, J. Stefanowski (eds.), *Big Data Analysis: New Algorithms for a New society*, Cham (CH), Springer, 2016; G.J. Petersson, J.D. Breul (eds.), *Cyber Society, Big data, and Evaluation*, with a foreword by C. Heider, London - New York, Routledge, Taylor & Francis, 2017; D. Talia, *Big data and the Computable Society: Algorithms and People in the Digital World*, New Jersey, World scientific, 2019; F. Faini, *Data society: governo dei dati e tutela dei diritti nell'era digitale*, Milano, Giuffrè Francis Lefebvre, 2019. Cf. A. Beaulieu, S. Leonelli, *Data and Society: A Critical Introduction*, London, Sage, 2022.
2. G. Borges, C. Sorge (eds.), *Law and Technology in a Global Digital Society: Autonomous Systems, Big data, IT Security and Legal tech*, Cham (CH), Springer, 2022. Cf. S. Faro, T.E. Frosini, G. Peruginelli (eds.), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, il Mulino, 2020.
3. M. Schuilenburg, R. Peeters (eds.), *The Algorithmic Society: Technology, Power, and Knowledge*, London, New York, Routledge, 2021; H.-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge, Cambridge University Press, 2022; G. De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge, Cambridge University Press, 2022; L. Lazzeretti, *The Rise of Algorithmic Society and the Strategic Role of Arts and Culture*, Cheltenham, Edward Elgar, 2023. Cf. L. Lazzeretti, *L'ascesa della società algoritmica ed il ruolo strategico della cultura*, Milano, Franco Angeli, 2021.
4. In addition to the landmark study of M. Castells, *The Rise of the Network Society, The Information Age: Economy, Society and Culture* (1996-1998), 3 voll., Malden (MA) - Oxford (UK), Blackwell, 2009-20102, see F. Webster, Theories of the information society, Abingdon, Routledge, 2002. Cf., most recently, C. Frigerio, F. Maccaferri, F. Rajola, ICT e società dell'informazione, Milano, McGraw-Hill Education, 20232.
5. Cf. M. Tallacchini, *Il "giusto posto" della scienza nella società: dalla "scienza come democrazia" alle "società democratiche della conoscenza"*, in M. Ostinelli (ed.), *Modernità, scienza e democrazia*, Roma, Carocci, 2020, 141-152; E. Bettinelli, *Società digitale/società della conoscenza: per una ulteriore analisi, tra progresso e crisi*, in *Studi di Sociologia*, 3, 2022, 493-508. N. Stehr, *Le moderne società della conoscenza*, Roma, Armando, 2023.

and in the foreground, thus putting into perspective the discourse on rights that was considered by many to be paramount just over thirty years ago.

It is, then, a question of understanding – this is the aim of this chapter – whether the primacy has irrevocably and definitively shifted from rights to data in today's society, or whether the protection of rights actually coincides with the protection of data, or whether rights are still paramount, but they also imply the protection and some form of governance of the data themselves[6] by the law, which is rightly seen as a perpetuum mobile[7].

My reflections on these questions are developed on the basis of Norberto Bobbio's book L'età dei diritti[8], published more than thirty years ago and the result of a research project that had began much earlier, in the late 1960s.

It is important to highlight two aspects of this book in the light of the working hypothesis that I will develop in what follows.

First, Bobbio's book – which is extraordinarily rich and evocative, full of definitions but also of some important ideal aspirations – can be considered a classic now and, like many classic texts, expresses the "spirit of the time", namely, the late 1980s and early 1990s. It was during this historical phase that the propulsive force of rights[9] was at its greatest and the sharing of the language of human rights, which had been progressively developing since the 1960s, was very much consolidated.

It is therefore, first and foremost, a classic that expresses the spirit of the times and at the same time spans the ages: in fact, the book ranges from the genesis of the very idea of rights and natural law to the French Revolution (and – a crucial aspect – its legacy), and finally to the Universal Declaration of Human Rights (today we rightly say 'human') of 1948 and its implications for the present day.

---

6. Cf., *ex multis*, F. Lazzini, *Etica digitale e intelligenza artificiale: i rischi per la protezione dei dati*, with a foreword by G. Cerrina Feroni, Torino, Giappichelli, 2022.
7. M. Arenas, *El perpetuum mobile del derecho a la protección de datos: no sólo mantenerlo, sino reforzarlo*, entravista a A.-E. Pérez Luño, in *La Ley Privacidad*, 6, 2020, 1-16.
8. The text was published in Italian in 1991 by Einaudi, Turin, and translated into English by A. Cameron: *The Age of Rights*, Cambridge, Polity Press, 1996.
   For a discussion of Bobbio's theses, see L. Baccelli, *Norberto Bobbio: An Age of Rights without Foundations*, in *Iris: European Journal of Philosophy*, 2, 2010, 401-422. On Bobbio's thought in general, see recently D. Ragazzoni, A. Craiutu (eds.), *Norberto Bobbio. A Life for Democracy on the Battlefield of Ideologies*, New York, Routledge, 2023.
9. See A. Schiavello, *Ripensare l'età dei diritti*, Modena, Mucchi, 2016.

Past and present eras are therefore at the centre of the study, but the gaze is also turned to the future[10], and it is on this latter temporal dimension that I will focus my argument below.

Second, precisely because this book was written at a time when the propulsive force of rights and the positive connotations of this expression were at their greatest, "rights" is accompanied by a certain optimism[11].

I recall these two aspects because in the following pages I will try to hold together a dual connotation of rights underlying L'età dei diritti, albeit in a rather asymmetrical form: on the one hand, Bobbio's book certainly focuses on "positive rights", that is of rights that have become "normative orders", even on a planetary, international, global scale; on the other hand, rights are also the expression of "ideal aspirations", of "claims" and responses to "material and moral needs"[12]. This latter aspect, on which I base my argument, emerges in the concluding part of the introduction to the book.

This is an argument about the status of rights, as well as about the evolution of rights themselves, in an age – the present one – which has been defined by many and repeatedly as the 'age of data' (and of digitalisation, the digital age[13]), rather than the 'age of rights'.

A methodological aspect that I find particularly interesting is the emphasis on the historical significance of rights, which Bobbio's book highlights from the outset.

Rights, says the philosopher, are born in "certain circumstances, from contingencies, needs, interests and struggles"[14].

---

10. N. Bobbio, *Presente e avvenire dei diritti dell'uomo*, in *La Comunità internazionale*, 1, 1968, 3-18 (trad. castilian in *Anuario de Derechos Humanos*, 1, 1982, 7-28; the text is also included in *L'età dei diritti*, cit., 17-44).
11. Perhaps this book expresses Norberto Bobbio's optimistic view, even though he used to say of himself that he was rather a pessimist.
12. N. Bobbio, *Introduzione*, in Id., *L'età dei diritti*, cit., XX.
13. K. Pistor, *Statehood in the Digital Age*, in C*onstellations*, 1, 2020, 3-18; T. la Quadra-Salcedo, J.-L. Piñar (eds.), *Sociedad digital y Derecho*, Madrid, Boletín Oficial del Estado, 2018. Cf. L. Taddio, G. Giacomini (eds.), *Filosofia del digitale*, Milano-Udine, Mimesis, 2020; F. Ciracì, Fabio, R. Fedriga, C. Marras (eds.), *Filosofia digitale*, Milano, Mimesis, 2021; G. Pezzano, *Pensare la realtà nell'era digitale. Una prospettiva filosofica*, Roma, Carocci, 2023; Id., *D1git4l-m3nte: antropologia filosofica e umanità digitale*, Milano, Franco Angeli, 2024. For a radical critique see a B.-C. Han, *Nello sciame: visioni del digitale*, Milano, Nottetempo, 2015, É. Sadin, *Io tiranno: la società digitale e la fine del mondo comune*, Roma, Luiss University Press, 2022.
14. N. Bobbio, *Introduzione*, in Id., *L'età dei diritti*, cit., XX.

From the speech that Bobbio delivered at the University of Madrid in 1987 it is evident that, starting from this dimension of historical significance and the generation of rights – which is a precise modality of approaching human rights[15], perhaps a 'new generation' of rights was emerging in those years, correlated with the development of new technologies.

This aspect is highlighted well in an essay by Antonio-Enrique Pérez Luño published in the same year. This Spanish scholar, who has made a fundamental contribution to the study of the impact of technologies on the legal dimension, maintains that, in that particular historical period, rights were undergoing a new "configuration", a "new generation" – which he defined as the "third" – closely linked precisely to the "development of new technologies"[16].

In another essay in the book on the age of rights, Diritti dell'uomo e società[17], Bobbio emphasises that "certain demands" arise only when "certain needs" arise. Needs are not always the same in different historical periods, but there are phases in which 'new needs' emerge. New needs, says Bobbio, "arise in accordance with changing social conditions and when technical development makes it possible to satisfy them"[18].

15. See, *ex multis*, F.J. Ansuátegui, *Storia e pluralità nella comprensione moderna del diritto*, in *Rivista di Filosofia del Diritto*, 1, 2017, 79-96.
16. A.E. Pérez Luño, *Concepto y concepción de los derechos humanos (Anotaciones a la ponencia de Francisco Laporta)*, in *Cuadernos de filosofia del derecho*, 4, 1987, 47-66, 56-59. Cf. A.E. Pérez Luño, *Las generaciones de derechos humanos ante el desafío posthumanista*, in T. la Quadra-Salcedo, J.-L. Piñar (eds.), *Sociedad digital y Derecho*, cit., 137-159.
In the same years, in Italy, Vittorio Frosini provided useful insights into the impact of the 'information society' with studies such as *Informatica diritto e società* (Milan, Giuffrè, 1988) and *Contributi ad un diritto dell'informazione* (Napoli, Liguori, 1991), within a research path that will result in the publication of the collection *La democrazia nel XXI secolo* (Macerata, Liberilibri, 2010, with a preface by A. Jellamo and an afterword by F. Riccobono). But the interest in the impact of information technology on legal practice and social organisation itself was already surprisingly early: just think of *Cibernetica, diritto e società* (Milano, Edizioni di Comunità, 1968).
17. N. Bobbio, *Diritti dell'uomo e società*, in Id., *L'età dei diritti*, cit., 67-86.
18. N. Bobbio, *Introduzione*, in Id., *L'età dei diritti*, cit., XVI.

The "technical development"[19] to which the Bobbio refers can be understood, in the current historical phase, as "technological development"[20].

A crucial theme emerges here, which concerns the relationship between rights and needs, the relationship between law and new technologies, and between law and the social transformations brought about by the widespread diffusion and use of new technologies[21]: these are the key issues that I wish to focus on in what follows.

II. RECONFIGURATION OF CONCEPTS AND/OR CONFIGURATION OF A NEW PARADIGM?

In the current historical phase – thus more than thirty years after Bobbio addressed these questions – we have to reckon with the impact of technologies: the "new technologies" that are now being developed are spreading in a pervasive and accelerated[22] manner so as to permeate

19. For a wide-ranging study that reconstructs the roots of the philosophical critique of technology in the twentieth century, see M. Nacci, *Pensare la tecnica. Un secolo di incomprensioni*, Roma-Bari, Laterza, 2000. For an overview of the relationship between technology and politics, see C. Galli, *Tecnica e politica: modelli di categorizzazione*, in Id., *Modernità. Categorie e profili critici*, Bologna, il Mulino, 1988, 79-106.

20. On the history of the concept of technology: E. Schatzberg, *Technology. Critical History of a Concept*, Chicago, Chicago University Press, 2018. Cf. R. Finelli, *Filosofia e tecnologia. Una via di uscita dalla mente digitale*, Torino, Rosenberg & Sellier, 2022, 75-104.

21. For an overview see Th. Casadei, S. Pietropaoli (eds.), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, second expanded and updated edition, Milano, Wolters Kluwer, 2024. Cf. E. Carpanelli, N. Lazzerini (eds.), *Use and Misuse of New Technologies*, Cham (CH), Springer, 2019.

22. On this aspect: J. Wajcman, *La tirannia del tempo. L'accelerazione della vita nel capitalismo digitale*, Roma, Treccani, 2020.
On this point, many scholars consider particularly relevant Carl Schmitt's contribution, according to whom the acceleration of the production of legislation in the 1940s created an alarming scenario in which laws often became nothing more than "orders that could be modified according to sudden changes in reality": C. Schmitt, *La condizione della scienza giuridica europea* (1944), Roma, Antonio Pellicani Editore, 1996, 26. On this point, see H. Rosa, W.E. Scheuerman (eds.), *High-speed Society. Social Acceleration, Power, and Modernity*, University Park PA, The Pennsylvania University Press, 2009, 65; E. Longo, *La legge precaria. Le trasformazioni della funzione legislativa nell'età dell'accelerazione*, Torino, Giappichelli, 2017, 12, and the PhD dissertation of Dott.ssa V. Chiesi, *Diritto e* sistema *nel tempo. Sul rapporto 'diritto-tempo' alla prova del sistema giuridico* prima *e* dopo *Luhmann*, Dottorato di ricerca in "Persona e Ordinamenti giuridici" - Ciclo XXXV (S.S.D. IUS/20), a.a. 2022-2023 (tutor: Prof. G. Bombelli), 24-29.

every aspect of our existence and are therefore calling for legal reflection transnationally[23].

This development is no longer connected to a "virtual" world, but is constantly fed by a gigantic production of data that crosses our lives, orients our choices, and defines our very existence: there are those who argue that "we are made of data" and that therefore datafication – one of the fundamental aspects of "digital grammatisation"[24] – is an unstoppable process, with relevant repercussions also in the world of law[25]. The collection of data and its transformation into information entails applications in several key areas: cybersecurity and privacy protection; digital health; human resources; artificial intelligence (AI); the market and the business world.

The constant permanent connection, interconnection, proximity to technologies, and interaction with them (almost as if they were extensions of the human body), has given rise to a new historical context: in order to deal with this, it is necessary to consider the status that technology and the digital have in contemporary life with respect to forms of politics, social interaction, and legal experience[26] and thus to the connotations of subjectivity[27], institutions, power (public and private), democracy and representation, the market, and the functions of law[28].

This basically opens up two paths in the analysis that, from my point of view, should be kept together. These are two levels, two parallel scenarios.

23. I. Stolzi, *Diritto e tecnologie: cronache di un eterno presente? (A proposito di recenti studi su intelligenza artificiale e società algoritmica)*, in *Quaderni fiorentini per la storia del pensiero giuridico moderno*, 51, 2022, 715-733, 715-716. Cf. G. Pascuzzi, *Il diritto nell'era digitale*, Bologna, il Mulino, 20205.
24. C. Giaccardi, M. Magatti, *Supersocietà*, Bologna, il Mulino, 2022, 65.
25. Cf., V. Berlingò, *Il fenomeno della* datification *e la sua giuridicizzazione*, in *Rivista trimestrale di diritto pubblico*, 3, 2017, 641-675; C. Sarra, *Il mondo-dato: saggi su datificazione e diritto*, Padova, CLEUP, 20222.
26. M. Durante, U. Pagallo (eds.), *La politica dei dati: il governo delle nuove tecnologie tra diritto, economia e società*, Milano-Udine, Mimesis, 2022.
27. M.N. Campagnoli, M. Farina, *Tec-no-identità? Percorsi, provocazioni e istanze delle nuove s/oggettività*, Milano, Key, 2022.
28. C.M. Lamberti, *Lemmi digitali. Verso la democrAI,* Milano-Udine, Mimesis, 2023; L. Torchia, *Lo Stato digitale. Un'introduzione*, Bologna, il Mulino, 2023.

II.1. RECONFIGURATION OF CONCEPTS

At the first level, the impact of technologies is studied and, to a certain extent, the focus is on "reconfigurations" or "reformulations of concepts", to use the words of Javier Ansuátegui's expressions in a fine essay[29].

In this way, we can understand how a whole series of concepts, including legal concepts[30], are being reconfigured in the 'data age' (which is also the age of the permanent 'acceleration' of the development of technologies[31]). From Ansuátegui's reconstruction a set of concepts emerges that examines the impact of technologies on the public sphere, on the identity of the subject, on power, on the relationship between technology and power, on democracy (which, incidentally, is no longer representative-deliberative democracy, but has become a kind of "continuous electronic democracy", to which the idea of new models of participation is also subordinated).

However, other very important profiles emerge from the analysis: e.g., the distinction between public and private space; the relationship between democracy and rights; the new forms of discrimination, digital and algorithmic[32]; belonging and citizenship (we live in an era in which the

29. F.J. Ansuátegui Roig, *Nuove tecnologie e spazio pubblico*, in S. Salardi, M. Saporiti (eds.), *Le tecnologie 'morali' emergenti e le sfide etico-giuridiche delle nuove soggettività/ Emerging 'Moral' Technologies and the Ethical-legal Challenges of New Subjectivities*, Torino, Giappichelli, 2020, 22-41.
Similarly, Isabella Consolati observes that the architecture of digital platforms, although based on numerical calculation, "is composed of words that echo key concepts of the modern political, legal and social lexicon: from social to communities, from recognition to government, from command to code" (I. Consolati, *Per una semantica del potere algoritmico. Prospettive e problemi*, in *Filosofia politica*, 2, 2023, 329-342, 329).

30. Cf. G. Saraceni, A.C. Amato Mangiameli (eds.), *Cento e una voce di informatica giuridica*, Torino, Giappichelli, 2023.

31. Although the relationship with technology cross-cuts all considerations relating to acceleration, the topic is specifically addressed by M. Castells, *La nascita della società in rete*, Milano, Università Bocconi Editore, 2014 [1996]; R. Hassan, R.E. Purser (eds.), *24/7. Time and Temporality in the Network Society*, Stanford, Stanford Business Books, 2007.
On the relationship between temporal changes and democracy: D. de Kerckhove (ed.), *La conquista del tempo. Società e democrazia nell'era della rete*, Roma, Editori Riuniti, 2003; R. Hassan, *Empires of Speed. Time and the Acceleration of Politics and Society*, Leiden, Brill Academic Pub, 2009. Cf. S. Bertman, *Hyperculture. The Human Cost of Speed*, Westport-Conn., Praeger, 1998; R. Avanessian Armen, #*Accelerate. The Accelerationist Reader*, Windsor Quarry-Falmouth, Urbanomic, 2014.

32. V. Barone, *La discriminazione ai tempi dell'intelligenza artificiale*, in Th. Casadei, S. Pietropaoli (eds.), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, cit., 285-296.

reference to "digital citizenship" is increasingly recurrent, but in which the forms of exclusion from its perimeter are also evident[33]); transparency (the myth of transparency for public administration, the need for transparency when we are confronted with the question of the protection of rights[34]); territory, sovereignty, community; and finally truth – we are in the era of the so-called "post-truth"[35], crime, and the market.

With respect to all these concepts and their reconfigurations, it is necessary to consider how they relate to data, to personal data. And this in the light of certain questions such as how data are collected? how they are

---

In addition to Ruth Rubio's contribution in this book, see: S.U. Noble, *Algorithms of Oppression. How Search Engines Reinforce Racism*, NYU University Press, New York, 2018; J. Kleinberg, J. Ludwig, S. Mullainathan, C.R. Sunstein, *Discrimination in the age of algorithm*, in *Journal of Legal Analysis*, 10, 2018, 113-174; C.R. Sunstein, *Algorithms, correcting biases*, in *Social Research*, 86, 2, 2019, 499-511; R. Xenedis, L. Senden, *EU Non-Discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges of Algorithmic Discrimination*, in U. Bernitz *et al.* (eds.), *General Principles of EU law and the EU Digital Order*, Wolters Kluwer, Alphen aan den Rijn, 2020, 151-182; R. Nunn, *Discrimination in the Age of Algorithms*, in W. Barfield (ed. by), *The Cambridge Handbook of the Law of Algorithms*, Cambridge, Cambridge University Press, 2020, 182-198; E. Falletti, *Discriminazione algoritmica: una prospettiva comparata*, Torino, Giappichelli, 2022; A.G. Grasso, *GDPR Feasibility and Algorithmic Non-Statutory Discrimination*, Napoli, Edizioni scientifiche italiane, 2023; B.G. Bello, *(In)giustizie digitali. Un itinerario su tecnologie e diritti*, Pisa, Pacini, 2023, 73-86; F. Casa, *Il filosofo del diritto e le discriminazioni digitali*, in *Ordines. Per un sapere interdisciplinare delle istituzioni europee*, 2, 2023, 228-246. Cf. *"L'algoritmo alla prova del caso concreto: stereotipi, serializzazione e discriminazione"*, in *Genius*, 1, 2022.

On prevention see: S. Vantin, *Il diritto antidiscriminatorio nell'era digitale. Potenzialità e rischi per le persone, la pubblica amministrazione, le imprese*, Milano, Wolters Kluwer, 2021; Ead., *Inteligencia artificial y derecho antidiscriminatorio*, in F.H. Llano Alonso, J. Garrido Martín (eds.), *Inteligencia artificial y derecho. El jurista ante los retos de la era digital*, cit., 367-384; G. Giorgini Pignatiello, *Il contrasto alle discriminazioni algoritmiche: dall'anarchia giuridica alle* Digital Authorities*?*, in *Federalismi*, 16, 2021, 164-185.

33. G. Pascuzzi, *La cittadinanza digitale: competenze, diritti e regole per vivere in rete*, Bologna, il Mulino, 2021. Cf. F. Oliveri, *Il "diritto a internet": ragioni e principi per democratizzare la rete*, in Th. Casadei, S. Pietropaoli (eds.), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, cit., 43-57; V. Pickard, D.E. Berman, *After Net Neutrality: A New Deal for the Digital Age*, New Haven, London, Yale University Press, 2019.
34. F. Corigliano, *I nodi della trasparenza*, Roma, Studium, 2018.
35. Cf., F. Martini, *Conoscenza digitale: l'attendibilità delle informazioni in rete*, Roma, Carocci, 2015; A. Condello, T. Andina (eds.), *Post-truth, Philosophy and Law*, London, New York, NY, Routledge, 2019; S. Giusti, E. Piras (eds.), *Democracy and Fake News: Information, Manipulation and Post-truth Politics*, London, New York, NY, Routledge, 2021.

organised? and how they are marketed? In short, how data are used in the 'data society'?

On closer inspection, these questions refer to a broader and more comprehensive question, i.e. what are the conditions and status of rights in the data society and in the digital space (of data production and permanent exchange).

Ansuátegui points out well that digital space – and so artificial intelligence itself – is not free and is not neutral, i.e. it is managed and governed by private agents, driven by special interests and a marked commercial dimension[36]. It has been observed that "the data [...] used to train a system carry with them, well hidden, all the nuances and biases they describe, [...] 'the biases are all around us and are part of the models because they are part of the data' (my translation)"[37].

In the age of data, the digital market is concentrated in a few hands, and an old, very old dilemma raises, which seeks to shape the relationship between rights (understood as the guarantees and protections that follow claims to rights) and private powers: the question of citizenship and, today, of digital citizenship, both of which are at a crossroads[38].

What does it mean, then, to follow this line of argument, and what does it mean from the point of view of the philosophy of law and legal reflection?

Essentially, it means considering technology in terms of regulation, or, first and foremost, with technology as an object of regulation[39].

---

36. For a closer look at this crucial aspect (and an extensive bibliography): A. D'Attorre, *La sovranità digitale. Poteri privati, intervento pubblico e diritti individuali nel cyberspazio*, in Th. Casadei, S. Pietropaoli (eds.), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, cit., 313-324.
37. N. Abriani, G. Schneider, *Diritto delle imprese e intelligenza artificiale*, Bologna, il Mulino, 2021, 40.
38. S. Pietropaoli, *Da cittadino a user. Capitalismo, democrazia e rivoluzione digitale*, in A. Cavaliere, G. Preterossi (eds.), *Capitalismo senza diritti?*, Milano-Udine, Mimesis, 2021, 31-41. More broadly: F. Fischbach, *La privation de monde*, Paris, Vrin, 2011. See anche: N. Srnicek, *Capitalismo digitale. Google. Facebook, Amazon e la nuova economia del web*, Roma, Luiss University Press, 2017; S. Mannoni, G. Stazi, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Napoli, Editoriale scientifica, 2021; M.R. Ferrarese, *Poteri nuovi. Privati, penetranti, opachi*, Bologna, il Mulino, 2022; M. Betzu, *I baroni del digitale*, Napoli, Editoriale scientifica, 2022.
39. Cf. A. D'Aloia (ed. by), *Intelligenza artificiale e diritto: come regolare un mondo nuovo*, Milano, Franco Angeli, 2020.

The reconfiguration of concepts under the technological firepower results in highly problematic regulation and, as a consequence, concrete difficulties in guaranteeing rights. As a result, the "masses" – a term that is rarely used in the age of data – risk being excluded from digital citizenship[40]. This last problem, one which is of great concern to us, was raised by Bobbio himself in his study on the development of new technologies during the above-mentioned phase of the propulsive force of rights. This lies at the heart of the problem of the digital divide, if we want to see it[41].

II.2. CONFIGURATION OF A NEW PARADIGM

On the other hand, it is possible to highlight another scenario that I believe we should bear in mind and one that is closely linked to this first approach.

This second scenario consists not so much in a reconfiguration of consolidated concepts, but as the configuration of a new context, a new paradigm, taking up some observations by Silvia Salardi in her *Intelligenza artificiale e semantica del cambiamento. Una lettura critica*[42].

What does a 'new paradigm' mean? It means that technology is no longer the only the object of legal regulation: technology can be presented, or even "presents itself"[43], as a regulatory agent, as a regulatory subject.

In a certain narrative of artificial intelligence, one which is now hegemonic[44], things seem to be exactly in these terms, translated into precise (and by no means neutral) outcomes: let the algorithm determine the allocation of resources; let the algorithm provide the services of public

40. E. Meligrana, G. Scorza, *La privacy degli ultimi*, foreword by A. Spadaro, Soveria Mannelli (CZ), Rubbettino, 2023.
41. Cf. P. Lupač, *Beyond the Digital Divide. Contextualizing the Information Society*, Bingley, Emerald Publishing, 2018; A. Peacock, *Human Rights and the Digital Divide*, London, Routledge, 2019; J. Van Dijk, *The Digital Divide*, Cambridge, Polity, 2020; S. Vantin, *I divari digitali nell'epoca della rete globale*, in Th. Casadei, S. Pietropaoli (eds.), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, cit., 297-311.
42. S. Salardi, *Intelligenza artificiale e semantica del cambiamento. Una lettura critica*, Giappichelli, Torino, 2023. Cf. A. Simoncini, S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1, 2019, 87-106.
43. *Ivi*.
44. Cf. F.H. Llano Alonso, *Technological singularity and personal identity. Reflections for an ethical-legal debate*.

authorities; let the algorithm determine the forms of relations between private individuals (for example, a citizen's access to a credit service of a bank); let the judge – who is still tied to his "old" (and fallible) approach based on the connection of causality – be replaced by the algorithm, with its *modus operandi* based on a statistical approach and focused on the collection of data and their correlation[45].

Further, in more operational and prosaic terms, it is an algorithm that prevents those who have not paid their car insurance from driving[46] (in such a way that the technology is no longer only functional for a possible sanction, but an automatic sanction itself)[47].

The algorithm, understood as "the fundamental mathematical and political structure of artificial intelligence, the Internet, digital platforms

45. For a more refined critique of this outcome, see F.H. Llano Alonso, *Justicia digital, algoritmos y derechode la predictibilidad del big data al mito del juez-robot*, in M.O. Sánchez Martínez (coord.), *El impacto de la inteligencia artificial en la teoría y la práctica jurídica*, Las Rozas (Madrid), Wolters Kluwer Legal & Regulatory España, 2022, 2019-244. As Sandro Luce aptly pointed out to me, some interpreters – including T. Berns and A. Rouvroy in *Gouvernementalité algorithmique et perspectives d'émancipation* (in *Réseaux*, 1, 2013, 163-196) – note the epistemological leap from a 'statistical' model, conventional in nature and subject to interpretation, to an algorithmic (governmental) model. In the latter, the collection of data has no purpose and is not subject to interpretation. It is therefore much more opaque and, above all, free from any possibility of criticism. Roberto Finelli's reflections are not far from this critical reading when, with regard to the algorithmic model, he speaks of "signals" (the binary system of computer code) that have no meaning of their own, that have rules without having semantics (R. Finelli, *Filosofia e tecnologia. Una via di uscita dalla mente digitale*, cit.). All this goes beyond the question of replacing the judge, but it reveals another element of opacity, in addition to the discriminatory risks linked to the construction of the algorithm referred to.

46. M. Benasayag, M. Régis, *La tirannia dell'algoritmo: conversazioni con Régis Meyran*, Milano, Vita e pensiero, 2020.

47. On the political and institutional dimension, see A. Cardone, *Decisione algoritmica vs. decisione politica? AI, legge, democrazia*, Napoli, Editoriale scientifica, 2021. Cf. Th. Casadei, *Istituzioni e algoritmi: tra strategie funzionali ed "effetti collaterali"*, in U. Salanitro (ed.), *Smart. La persona e l'infosfera*, Pisa, Pacini giuridica, 2022, 245-265.

and information technology as a whole"[48], acquires a power that can be without limits[49], that is, without regulations and without rules[50].

Power thus becomes "algorithmic power" in the digital society. In the new paradigm of the data society, data seems to have assumed an unparalleled preponderance: the scenario that is envisaged is that of a "global algorithmic government", which presupposes a "global technological system"[51], dominated by the transnational artificial intelligence industry and the incessant production of data.

In other words, algorithmic power is sovereign: it is an intermediary between individuals and their access to the social and political dimension. In this context, data 'colonises' lives, orienting and shaping them[52].

What has been defined as "algorithmic governmentality"[53] configures a mode of government through signals (raw data and metadata) addressed to "profiled" individuals. Each person is a statistical body; Deleuzian "dividuals" replace "individuals"[54].

48. I. Consolati, *Per una semantica del potere algoritmico*, cit., 330.
49. See most recently, M. Barberis, *Separazione dei poteri e giustizia digitale*, Milano-Udine, Mimesis, 2023. Cf., L. Avitabile, *Il diritto davanti all'algoritmo*, in *Rivisita italiana per le scienze giuridiche*, 8, 2017, 313-325; F. Pasquale, *The Black Box Society. The Secret Algorithms that control Money and Information*, Cambridge-London, Cambridge University Press, 2015; G. Fioriglio, *La società algoritmica fra opacità e spiegabilità: profili informatico-giuridici*, in *Ars interpretandi*, 1, 2021, 53-67; N. Lettieri, *Antigone e gli algoritmi: un approccio giusfilosofico*, Modena, Mucchi, 2021.
50. One of the first scholars to raise the problem of regulating cyberspace was, as is well known, Lawrence Lessig, who, in reviving a regulatory perspective, argued that legislative activity must update itself. In other words: in the Internet age 'the code is the law' and it is therefore necessary to adopt regulatory strategies that are modelled on the object of regulatory activity (L. Lessig, *Code and Other Laws of cyberspace*, New York, Basic Book, 1999).
51. Y. Hui, *Pensare la contingenza. La rinascita della filosofia dopo la cibernetica*, Roma, Castelvecchi, 2022, 36. Cf. B. Bratton, *The Stack. On Software and Sovereignty*, Cambridge, MIT Press, 2016.
52. Cf. N. Couldry, U.A. Mejas, *Il costo della connessione. Come i dati colonizzano la nostra vita e se ne appropriano per far soldi*, Bologna, il Mulino, 2022. On algorithms as objects of everyday life see D. Panagia, *On the Possibilities of a Political Theory of Algorithms*, in *Political Theory*, 1, 2021, 109-133, 117.
53. This category was coined in Antoniette Rouvroy and Thomas Bern's aforementioned essay, which has been at the centre of a broad international debate for several years now. Cf., most recently, G. Pisani, *Piattaforme digitali e autodeterminazione. Relazioni sociali, lavoro e diritti al tempo della "governamentalità algoritmica"*, Modena, Mucchi, 2023.
54. A. Rouvroy, *Transmediale – All Watched Over by Alghoritms*, conference presentation Berlin, 29 January 2015, *https://archive.transmediale.de/content/presentation-by-antoinette-*

If this narrative is questioned[55], the assessment changes deeply: technology, however powerful, does not become a regulator, but remains a tool, a means[56]. In fact, the algorithm does not generate itself, it is programmed by human beings: a series of elements (criteria) are constructed that refer to a programming phase and therefore to a human dimension[57]. The question of "who programs?" then becomes the digital version of "who decides?". The crucial question is whether institutions and public powers can exercise sovereignty in the field of planning (and regulation), also affirming a "public cognitive power"[58], or whether a whole series of processes will be irrevocably handed over to large multinational companies, i.e. to private powers[59].

And that is why I think it is necessary to question the narrative of technology as a regulatory agent, and to reposition it in a process that combines the human with the "machinic" (mechanical). Technology remains a means of execution, it can allow us to pursue new goals, it can also allow us to implement rules, but it is and remains a means.

In this context, the debate surrounding the 2017 European Parliament Resolution suggesting to attribute to a robot the characteristics and

---

rouvroy-all-watched-over-by-algorithms, quoted by C. Giaccardi, M. Magatti, *Supersocietà*, cit., 76-77. Cf. P. Vignola: *La funzione N: sulla macchinazione filosofica in Gilles Deleuze*, Napoli, Salerno, Orthotes, 2018; B. Stiegler, *La società automatica*, ed. by S. Baranzoni, I. Pelgreffi, P. Vignola, Roma, Meltemi, 2019, vol. 1: "L'avvenire del lavoro".

55. *Ex multis*: S. Salardi, M. Saporiti, *Perché l'IA non deve diventare Persona. Una Critica all'ineluttabile 'Divenire antropomorfico' delle Macchine*, in S. Salardi, M. Saporiti (eds.), *Le tecnologie 'morali' emergenti e le sfide etico-giuridiche delle nuove soggettività*, Torino, Giappichelli, 2020, 52-74.

56. However, it is important to take seriously the hypothesis that we are dealing with a "threshold where the technological artefact no longer seems to present itself as an instrument, as it has traditionally been conceived, but becomes a sort of 'machinic subject" (R. Finelli, *Filosofia e tecnologia. Una via di uscita dalla mente digitale*, cit., 11).

57. Cf. F. Pasquale, *Le nuove leggi della robotica*. *Difendere* la *competenza umana nell'era dell'intelligenza artificiale* (2020), Roma, Luiss University Press, 2021; G. Gigerenzer, *Perché l'intelligenza umana batte ancora gli algoritmi* (2022), Milano, Raffaello Cortina, 2023.

58. M. Falcone, *Ripensare il potere conoscitivo pubblico tra algoritmi e Big Data*, Napoli, Editoriale Scientifica, 2023.

59. As has already been pointed out, it was Carl Schmitt who noted this shift with reference to cybernetics: "That is the problem, who asks the question, who programs the machine itself, which is incapable of making a decision" (C. Schmitt, *Il compimento della Riforma. Osservazioni e cenni su alcune nuove interpretazioni del* Leviatano, in Id., *Sul Leviatano*, ed. by C. Galli, Bologna, il Mulino, 2011, 129-162, 162). Cf., I. Consolati, *Per una semantica del potere algoritmico*, cit., 333, n. 14.

connotations of a person (personality)[60] is particularly relevant: it follows the example of the United Arab Emirates, where a robot has been given a legal personality. This is certainly possible, but it is human beings who decide, in their institutional bodies.

It is not the hordes of robots, robotics and technologies that are so powerful as to conquer their dimension of subjectivity and regulators, as if their development automatically give rise to new legal configurations. On the contrary, human beings can decide to give legal personality to those who do not have it; this has been done in the past: think of slaves, children, "subjects" who were not considered as persons, as human beings with rights[61]. The possibility of the right to give personality is a recurrent one, absolutely possible for human beings: therefore, if we manage to give legal personality to something which does not have it today, means that it will be the result of a decision, a choice, after reflection and evaluation.

Personally, I think that it was and is very appropriate not to give personality to a robot, but the discussion is open and involves considerations not only of legal technique but of an existential nature[62].

The answer is affirmative, according to an anthropomorphic vision of technologies that ultimately leads to the replacement of human choice and deliberation by algorithms[63].

60. Cf. A.J. Sánchez Hidalgo, *Reflexiones en torno a la personalidad electrónica de los robots*, in F.H. Llano Alonso, J. Garrido Martín, R. Valdivia Jiménez (coord.), *Inteligencia artificial y Filosofía del derecho*, cit., 337-358.

61. Cf. R. Bodei, *Dominio e sottomissione. Schiavi, animali, macchine, Intelligenza Artificiale*, Bologna, il Mulino, 2019.

62. Cf. M. Innocenzi, B. Leucadito, G. Petrocco, *Il diritto tra digitale ed esistenziale*, Torino, Giappichelli, 2022.

63. On the other hand, the "personality" of machines, or rather of certain algorithms and software, could be legally recognised without too much difficulty. Cf. L. Perra, *L'antropomorfizzazione giuridica*, in *Diritto & Questioni pubbliche*, 2, 2020, 47-70, where the author recalls that in some countries, such as Ecuador, Bolivia, New Zealand, Colombia and in the Indian state of Uttarakhand, some rivers and landscape elements are considered "legal persons". In legal terms, the term 'person' refers to a centre of rights and interests, just as the law has long recognised 'personality' in corporations, associations, companies and foundations. In legal terms, one could perhaps speak of a 'silicic' personality, to paraphrase the title of this volume: R. Campione, *La plausibilidad del derecho en la era de la inteligencia artificial. Filosofía carbónica e filosofía silicíca del derecho*, Madrid, Dykinson, 2020. Cf. S. Pietropaoli, *En primera persona. Un réquiem por el derecho de la era digital*, in F.H. Llano Alonso, J. Garrido Martín, R. Valdivia Jiménez (coord.), *Inteligencia Artificial y Filosofía del Derecho*, Murcia, Ediciones Laborum, 2022, 217-233, 218-226.

III. THE CHALLENGE OF TRUSTING (HUMAN) RIGHTS

Let us recall, then, the two scenarios we have tried to outline: in the first, the issue of rights is certainly under pressure and concerns protection, guarantees and effectiveness, the very practice of digital citizenship, i.e. who is a citizen and who is not, and who therefore risks being marginalised; in the second scenario the issue is even more complicated. In fact, the dimension of citizenship (in relation to that of the person) is at stake and the reflection is centred on the interaction with devices, with robots, with data, which become commodities but can also, in some way, become the expression of a new "machinic" subjectivity.

A chapter of Kate Crawford's book *Atlas of AI. Power, Politics, and the Planetary Costs of Artificial Intelligence* highlights this data-commodity combination, which provides the ground for a critical examination of the relationship between the fundamental/human rights of human beings and the increasingly overwhelming availability of "goods"[64].A subject who is the "owner" of his or her own rights can use the data to increase the flow and gain a financial advantage (according to the perspective of "data patrimonialisation"). In this sense it has been observed that "an incessant work of data extraction through ever perfected algorithms sets the conditions of possibility of the subjects' behaviour – economic actors, ideally self-employees – and orients it towards the preservation of the system's dynamic stability"[65].

In the infosphere[66], the data subject[67] appears more and more as a "co-individual", i.e. a "heterogeneous multiplicity in time and space"[68],

64. K. Crawford, *Atlas of AI. Power, Politics, and the Planetary Costs of Artificial Intelligence*, New Haven and London, Yale University Press, 2021, chap. 3. Cf. D. Helbing, *Towards Digital Enlightenment: Essay on the Dark and Light Sides of the Digital Revolution*, Cham (CH), Springer, 2018.

65. A. Bardin, M. Ferrari, *Governing Progress: From Cybernetic Homeostasis to Simondon's Politics of Metastability*, in *The Sociological Review*, 2, 2022, 248-263, 255.

66. L. Floridi, *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, Milano, Raffaello Cortina, 2017; Id., *Pensare l'infosfera. La filosofia come design concettuale*, Milano, Raffaello Cortina, 2020.

67. Cf. Opinion 4/2015 "Towards a New Digital Ethics. Data, Dignity and Technology" (11 sept 2015), emerging from the emanate "European Data Protection Supervisor" (EDPS), where there is a perceived risk that the practices of governments and private individuals are reducing individuals to 'data subjects' and threatening their fundamental rights and freedoms.

68. C. Sini, C.A. Redi, *Lo specchio di Dioniso. Quando un corpo può dirsi umano?*, Milano, Jaca Books, 2018, 13, 20. Cf. S. Vantin, *Il diritto antidiscriminatorio nell'era digitale. Potenzialità e rischi per le persone, la pubblica amministrazione, le imprese*, cit., 39-41.

a depersonalised and fragmented entity in an explosion of "profiles, navigations, likes and cookies". He or she is dissolved and entangled in "aggressive marketing practices, in unfair negotiations, hidden behind formal requests for consent and acceptance of general terms and conditions, presented to unknowing subjects and trapped in an apparent freedom of choice in the resulting price discrimination and economic inequalities, unequal treatment and market distortions"[69].

In this perspective, identity is no longer a pre-existing fact, but rather a process that is "constantly in progress, open to a plurality of outcomes and constantly exposed to the capillary and pervasive interference of the various forms" (my translation) of digital interaction[70].

This phenomenon has been described as "hominescence"[71], in which the contours of the human are increasingly blurred and confused in a "decomposition" and "recomposition" that "risks losing and forgetting the 'human'"[72], even creating the danger that "traces and data form a kind of duplicate of the person, which we tend to trust more than the person himself or herself to make inferences and decisions" (my translation)[73].

According to some studies, therefore, it is not only the notion of the "person" that now seems inadequate in certain respects, but also the "performative" and "decisive"[74] nature of the "person", as the centre of legal

69. F. Faini, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, cit., 393 (my translation).
70. G. Resta, *Identità personale e identità digitale*, in *Diritto dell'informazione e dell'informatica*, 3, 2007, 511-531, 511. There is now no area of personal and collective life that has not been affected by "digitalisation": "research, health, mobility, logistics, public administration, education, money, production, work; as well as tracking, video surveillance, robotics, facial recognition, algorithmic regulation, artificial intelligence, etc." (C. Giaccardi, M. Magatti, *Supersocietà*, cit., 64-79).
Cf. M. Palmirani, M. Martoni, *Il cittadino elettronico e l'identità digitale nell'*e-governance, Bologna, Gedit, 2006; M. Bianca, *La* filter bubble *e il problema dell'identità digitale*, in *MediaLaws*, 2, 2019, 39-53; M. Martoni, *Note sulla vulnerabilità dell'identità personale digitale auto-rappresentativa*, in *Notizie di Politeia*, 136, 2019, 23-24.
71. M. Serres, *Hominescence*, Paris, Le Pommier, 2001.
72. F. Faini, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, cit., 394. Cf. R. Agote Eguizábal, *Inteligencia artificial, ser humano y derecho*, in *Claves de Razón Pratica*, 257, 2018, 40-45.
73. F. Faini, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, cit. 400. See also F. Faini, *Diritto all'esistenza digitale*, in *BioLaw Journal*, 3, 2019, 91-113.
74. R. Esposito, *Le persone e le cose*, Torino, Einaudi, 2014, 13, 18.

attribution and the rational subject of political action[75]. Hence the reliance on technology and algorithms as regulatory agents.

I believe that in both scenarios it is fundamental to keep in mind the function of rights and to ask ourselves what they can and should be in the current era by regulating, limiting and at the same time directing technological innovation[76]. And this is true in two ways: by following some principles and by developing some actions.

Principles are the fundamental prerequisite for guaranteeing the effectiveness of rights; more specifically, with regard to the development of digital technologies and the experiments to be associated with them, precaution and prevention – as is the case with environmental and safety issues – and accountability can be the lodestar to guide choices and evaluations, which, with regard to algorithms, means for example, knowing what the compositional elements and criteria are.

As far as actions are concerned, some of them seem to represent the prerequisites for ensuring a practice of rights that is consistent with the constitutional democratic state, and thus prefigure a kind of digital constitutional democratic state[77].

In particular, in order to be able to exercise all rights, it seems crucial to have a strategic plan for digital education and pedagogy[78], aimed at

75. S. Pietropaoli, *Persone non umane? Una riflessione sulla frontiera digitale del diritto*, in R.M. Agostino, G. Dalia, M. Imbrenda, S. Pietropaoli (eds.), *Frontiere digitali del diritto. Esperienze giuridiche a confronto su libertà e solidarietà*, Torino, Giappichelli, 2021, 1-22. Cf., F. Ranieri, *L'invenzione della persona giuridica. Un capitolo nella storia del diritto dell'Europa continentale*, Milano, Giuffrè, 2020, V. Frosini, *La giuritecnica: problemi e proposte*, in *Informatica e diritto*, 1, 1975, 26-35, 32.
About the machine as a "person": Elvio Ancona in the *Introduzione* to *Soggettività, responsabilità, normatività 4.0. Profili filosofico-giuridici dell'intelligenza artificiale*, in *Rivista di Filosofia del diritto*, 1, 2019, 81-86, 84. Cf. G. D'Anna, *Automi, responsabilità e diritto*, in *Rivista di Filosofia del diritto*, 1, 2019, 125-142.

76. Alain Supiot's reflections, developed from a critique of 'algorithmics', are particularly effective in this regard: A. Supiot, *La sovranità del limite. Giustizia, lavoro e ambiente nell'orizzonte della mondializzazione*, ed. by A. Allamprese, L. D'Ambrosio, Milano-Udine, Mimesis, 2020, 159.

77. A. Rouvroy, M. Hildebrandt (eds.), *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*, London, Routledge, 2011.

78. A.C. Amato Mangiameli, M.N. Campagnoli, *Strategie digitali. #diritto_educazione_tecnologie*, Torino, Giappichelli, 2020; B.G. Bello, *(In)giustizie digitali. Un itinerario su tecnologie e diritti*, cit., 87-112. Cf. P. Bonafede, *Connessioni e relazioni: filosofia dell'educazione e socialità digitale*, Roma, Anicia, 2020.

ensuring for each subject of rights the ability to operate, and act within digital environments in a conscious and proactive way, as a free citizen and not as a subjected human being (including the case of voluntary servitude)[79], rather than just computer literacy and the technical use of devices.

I would like to conclude these reflections by recalling Bobbio and his concept of rights, which also has an ideal dimension: to understand them, therefore, as what gives meaning to social and political life, to human coexistence, as well as to individual life, in relation to other elements (duties, responsibilities, the protection of dignity).

From this perspective, rights can still be a "promise to be kept", an ideal that also seeks concrete responses to new needs (and needs related to the proliferation of new technologies and the artificial intelligence they bring in contemporary society). In this phase, I think that the attitude proposed by Bobbio in his essay L'età dei diritti could be fruitful: starting from the focus on environmental crises, on the increasingly rapid and uncontrolled increase in the destructive power of armaments, he concludes his argument by stating: "we are already too late compared to the great aspirations of people of good will. Let's try not to make it worse with our mistrust, with our inertia, with our scepticism. We don't have much time to lose" (my translation)[80].

What follows is the result of a reasonable trust in rights and their potential, a necessary activism for their protection, for their guarantee, in order to extend the guarantees more and more, and even a certain optimism, in order not to give up even in the darkest times.

Ultimately, this means rethinking the subject of law as a subject who expresses a set of old and new powers, who is capable of modifying the conditions of production and reproduction of society, and who does not abandon the prospects of emancipation and autonomy[81], that is, of freedom, even in relation to technologies and machines. This also means to free the

79. S. Alegre, *Freedom to Think: Protecting a Fundamental Human Right in the Digital Age*, London, Atlantic Books, 2023.
80. N. Bobbio, *L'età dei diritti*, cit., 65.
81. A. Rouvroy, *Mise en (n)ombres de la vie même: face à la gouvernementalité algorithmique, repenser le sujet comme puissance*, in *Mediapart*, 27 August 2012; A. Rouvroy, Th. Berns, *Gouvernementalité algorithmique et perspectives d'émancipation*, cit.

subject from the realm of calculability and predictability[82], as well as from the primacy of data (and datafication).

In an age characterized by the pervasiveness of data, in which the person can even be conceived as "an open-pit mine"[83], binding him to the logic of calculation, and in which algorithms seem to be able to exercise limitless power (which some read as a "algocratic drift"[84]), rights can – once again and in a new historical phase – claim their centrality as an ideal and institutional reference. Rights thus support and substantiate all the regulatory instruments available to the public powers, as well as those that can be developed as response to new needs, "for which recognition and protection are requested"[85].

According to Bobbio, rights are always embedded in history, marked by struggles, and there are only two kinds of rights (differently from powers): rights that prevent their evils or that obtain their benefits[86].

82. In the semantics of algorithmic power, as has been observed, "the repetition of the past contains the key to the predictability of the future, an element that gives web concepts a specific temporal structure that should be brought to light beyond any apology for innovation that is disseminated in the field of so-called new media studies" (my translation); in this vein, see I. Consolati (*Per una semantica del potere algoritmico*, cit., 341). Cf. W.H. Kyong Chun *Programmed Visions: Software and Memory*, Cambridge (Mass.), London, The MIT Press, 2013; Ead., *Updating to Remain the Same: Habitual new Media*, Cambridge (Mass.), London, The MIT Press, 2016; Ead. *Discriminating Data: Correlation, Neighborhoods, and the New Politics of Recognition*, Cambridge (Mass.), London, The MIT Press, 2021.
83. Stefano Rodotà's expression is recalled by N. Abriani, G. Schneider, *Diritto delle imprese e intelligenza artificiale*, cit., 81.
84. N. Abriani, G. Schneider, *Diritto delle imprese e intelligenza artificiale*, cit., 15. J. Danaher, *The Threat of Algocracy. Reality, Resistance and Accomodation*, in *Philosophy and Technology*, 3, 2016, 245-268.
85. N. Bobbio, *Introduzione*, in Id., *L'età dei diritti*, cit., IX.
86. *Ivi*, XV.

Climate change and digitization: the role of AI from a "rights-based" perspective

[1]Rosaria Pirosa*

SUMMARY: I. - INTRODUCTION. II. THE BIOETHICAL UNDERSTANDING OF ARTIFICIAL INTELLIGENCE WITHIN THE THEORETICAL-LEGAL REFLECTION ON "CLIMATE CHANGE" - III. THE ROLE OF ARTIFICIAL INTELLIGENCE IN STRUGGLING CLIMATE CHANGE IN LIGHT OF THE PRINCIPLE OF BENEFICENCE - IV. SPARKS FOR A PHILOSOPHICAL-LEGAL PERSPECTIVE USEFUL FOR PROMOTING AI IN THE FIGHT AGAINST CLIMATE INSTABILITY - V. THE ADVANTAGES OF USING AI IN THE RESTRAINING OF THE EFFECTS OF CLIMATE CHANGE - VI. CONCLUSIONS

ABSTRACT: This essay intends to focus on the role of Artificial Intelligence in relation to climate change and, specifically, on the potential advantages that derive from a soft-ethics approach in the use of techno-scientific devices within the struggle against climate change.

The article will delve into the dimension of interaction between a scientific and interdisciplinary understanding of climate instability and a conception of this phenomenon – in the framework of the theoretical legal discourse – grounded on a "rights-based" approach.

Therefore, the text aims to highlight how the fight against climate change from the point of view of the violation of a relevant subjective legal situation conceptualized as the "right to the climate" – and the rights connected to it – can constitute a prerequisite for policy choices aimed at the enhancement of the social value of AI.

In this direction, the contribution tries to reinforce suggestions that a bioethical reading of AI in relation to climate change lads to a specific philosophical and legal reflection, in particular with regard to the possibility of a transition from a vision based on "climate law" as a goal to the central objective of the protection of subjective rights.

* Researcher in Philosophy of Law, University of Modena and Reggio Emilia.

KEYWORDS: Climate change; Digitization; Artificial Intelligence; Right to climate; Soft-ethics.

I. INTRODUCTION

The expansion of Artificial Intelligence increasingly concerns all fields of human experience and it is emblematic of the challenge, but also the most imposing threat, that human beings have to cope in this century: climate change[1].

The evaluation of the impact of AI on climate change, from a theoretical and legal perspective, primarily calls for the review, with regard to an epistemological and methodological approach, of the anthropocentric understanding. As a matter of fact, the very concept of sustainable development in all its implications – environmental, social and economic –, receives meaning within an analytical horizon based on the "biocentric paradigm"[2]. It is also oriented towards the relevance, in the fight against climate change, of "new forms of action"[3] and, therefore, of the opportunities connected to the use of techno-scientific devices.

To overcome anthropocentrism means, first, leaving behind the notion of health as a prerogative of individual, unrelated to their peers, to all non-human beings and to the planet. The fight against "climate change", therefore, is based on the idea of health as "one-health"[4], and includes the plurality of determinant factors that affect general well-being starting from the

1. Cp. J. Cowls, A. Tsamados, M. Taddeo, L. Floridi, *The AI gambit – Leveraging artificial intelligence to combat climate change: Opportunities, challenges, and recommendations*, in *SSRN Electronic Journal*, n. 38/2021, 283-307.
2. See S. Adelman, *The sustainable development goals, anthropocentrism and neoliberalism*, in D. French, L. Kotzé, *Sustainable Development Goals: Law, Theory and Implementation*, Cheltenman, Glos, Northampton, Massachussettes, Edward Elgar, 2018, 15-40. On these profiles: L. Palazzani, *Il concetto di persona tra bioetica e diritto*, Torino, Giappichelli, 1996 and M. Andreozzi, *Le sfide dell'etica ambientale. Possibilità e validità delle teorie morali non-antropocentriche*, Milano, Led, 2015.
3. L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, Raffaello Cortina Editore, especially 39-63.
4. This notion identifies the plurality of determinants – social, economic, geographical, cultural – that affect general well-being starting from the health of all living beings and the planet. This approach places emphasis on the conditions of disadvantage which, in a differential way, impact social groups. Cp. S.L. Deem, K.E. Lane-de Graaf, E.A. Rayhel, *Introduction to One Health. An Interdisciplinary Approach to Planetary Health*, Hoboken, Wiley-Blackwell, 2019.

protection of all living beings. This perspective emphasizes disadvantageous conditions and processes of vulnerabilization[5] which impact social groups in a differential way. It is also significant for climate change issue and, in particular, for the relationship between rights and climate emergency.

A philosophical-legal investigation into the advantages of AI implementation in the restraint of "climate change", indeed, brings into question the role of law and of legal theory and orients us the way in which these fields are interconnected with the protection of the rights of relevant subjectivities.

In this direction, a "rights-based" approach is linked to the postulability of subjective legal situations different from those typified by law and to a methodology that gives relevance to individual and collective requests arising from the activity of claiming.

Climate change no longer only recalls a dimension of emergency and urgency, but, with regard to some countries in the world, the need to deal with an existing phenomenon that can be classified as climate collapse. Since a critical perspective on climate change outlines an emblematic *spectrum* of the social and economic inequalities in the global dimension, such an analysis cannot be developed without a focus on these inequalities within a political-legal approach.

In climate change topic, the perspective of legal theorists should not be exhausted in a *pars destruens* and, therefore, in a "deconstructive posture" confined within the fences of *inertia* often justified by the awareness of irreversibility of some eco-systemic trends. Rather, it should consist of a *pars construens*, centered on the relevance of policies to combat climate change inspired by a *bottom-up* logic.

In the contemporary theoretical-legal debate, therefore, this approach, looking at the "right to the climate", cannot fail to delve into the affirmation of Artificial Intelligence and, above all with regard to the European Union, into the policies connected to its uses and different implementation areas. The

5. On the analysis of vulnerability as an etiopathogenetic process and not as an ontological condition, see C. Mackenzie, N. Stoljar, *Relational Autonomy. Feminist Perspectives of Autonomy, Agency and the Social Self*, Oxford, Oxford University Press, 2000; C. Mackenzie, *Vulnerability, needs and moral obligation*, in C. Straehle (ed.), *Vulnerability, Autonomy and applied ethics*, New York-London, Routledge, 2017, 83-100; C. Mackenzie, *Moral responsibility and the social dynamics of power and oppression*, in K. Hutchinson, C. Mackenzie, M. Oshana (eds.), *Social dimensions of moral responsibility*, Oxford, Oxford University Press, 2018, 59-80.

urgency of this last theme, at a global level, is then amplified by the fact that the interpretation of the relationship between climate change and growing digitization fits into the field sketched by the sustainable development objectives, classified as priorities by the United Nations[6].

II. THE BIOETHICAL UNDERSTANDING OF ARTIFICIAL INTELLIGENCE WITHIN THE THEORETICAL-LEGAL REFLECTION ON "CLIMATE CHANGE"

The analysis on the affirmation of techno-scientific devices and on the role of AI in the fight against climate change, or in the control of climate instability, identifies a central premise in a bioethical reflection on Artificial Intelligence that helps to understand its interaction with the field of law and subjective rights. In this sense, with respect to climate change, the approach of states or supranational organizations regarding "climate law" will be relevant, but even more so the very conceptualization of the idea of climate change in a legal discourse.

In general, a "rights-based" approach cannot only deal with the relationship between the phenomenon of climate change and – we could say – the legal dimension *tout* court, nor consist in a review of the rules that draw "climate law", but, rather, it has the goal to address climate change from the perspective of subjective rights.

In 2009, upon mandate of the Human Rights Council in the *Report on the Relationship between Climate Change and Human Rights*[7], the United Nations High Commissioner for Human Rights also expressed a position that offered a basis to this idea. In the broader framework of international environmental law and climate law, the Report focused on the impact of climate change on international stability, on the rights (women, children, indigenous peoples, migrants' rights) and on the ways in which a "based-rights" perspective could be useful in the struggle against anthropogenic climate change[8].

---

6. Sustainable Development Goals, 17 Goals to Trasform Our WorldAgenda 2030, *www.un.org/sustainabledevelopment/*.
7. Annual Report of the United Nations High Commissioner for Human Rights and Reports of the Office of the High Commissioner and the Secretary-General, *Report of the Office of the United Nations High Commissioner for Human Rights on the relationship between climate change and human rights*, in particular 20-78, *www.documents-dds-ny.un.org/doc/UNDOC/GEN/G09/103/44/PDF/G0910344.pdf?OpenElement*.
8. See "AR4 Climate Change 2007: Synthesis Report", *www.ipcc.ch/report/sixth-assessment-report-cycle/*.

The United Nations High Commissioner confirmed this position until the latest Report: *Panel discussion on the adverse impact of climate change on the full and effective enjoyment of human rights by people in vulnerable situations*, published on 27 December 2022[9].

The topic of human rights, in the fight against anthropogenic "climate change", however, is rather marginal in the normative documents that settles "climate law" and which are, then, better known: the United Nations Framework Convention on Climate Change (UNFCCC) adopted in follow-up to the 1992 United Nations Conference on Environment and Development in Rio de Janeiro Conference, the 1997 Kyoto Protocol and the 2015 Paris Agreement.

Therefore, there is a significant gap between a vision of law as an instrument for stipulating agreements or for attempting to conclude agreements between States and a theoretical reflection which, instead, makes a significant transition from the approach on law as a mere set of rules to a rights-based perspective, resulting, more precisely, in the relevance of the conceptualization of a subjective legal situation, at an individual and collective level: the right to climate[10].

In this direction, a bioethical understanding of the function and implementation of Artificial Intelligence constitutes a fundamental step to examine how the expansion of the use of techno-scientific devices can support a conception of the fight against climate change inspired by the centrality of the legal protection of subjective rights.

The application of AI significantly affects health as "one-health" and, within it, the development of eco-systems, the possibilities of control climate instability as a factor generating social and economic inequality between the different parts of the world, the need to relocate the idea of psycho-physical and social well-being in the global dimension.

In general, the AI implementation can be conceived starting from the centrality of legal goods of constitutional rank such as human dignity[11] or

9. Annual Report of the United Nations High Commissioner for Human Rights and Reports of the Office of the High Commissioner and the Secretary-General, *Panel discussion on the adverse impact of climate change on the full and effective enjoyment of human rights by people in vulnerable situations*, especially 10-12, *www.ohchr.org/en/documents/reports/ahrc5248-panel-discussion-adverse-impact-climate-change-full-and-effective*.
10. See A. Pisanò, *Il diritto al clima. Il ruolo dei diritti nei contenziosi climatici europei*, Napoli, Edizioni Scientifiche Italiane, 2022.
11. *Ibidem*.

environmental sustainability[12], in a perspective that assigns a basic role to relationality as the very premise of law[13].

Just having regard to the legal-theoretical basis of the conceptualization of subjective legal situations protected within the rule of law in light of technological development, we can identify the main opportunities connected to the Artificial Intelligence in an analytical horizon within the theoretical-legal reflection[14].

By way of example, the elaboration, found in the theory of "Western" law, of the principle of the development of the person – fundamental in human rights – focuses on the relevance of autonomous realization, on the promotion of human agency, on the capabilities of individuals and groups and on the importance of inter-individual interactions and the relationship between human beings and the planet.

With respect to each of these areas, the implementation of AI cannot be read according to a univocal interpretation, being able to intervene to promote the development of the human person and to increase his empowerment, or resulting in an under-use that frustrates the list of existing opportunities[15], or even consisting of an overabundant or insufficiently supervised recourse that could determine a greater potential risk for subjective rights.

This debate – we could say – strictly oriented towards, in general, the multiple values and applications of Artificial Intelligence, with specific respect to climate change, until very recently, was almost monotonous and aimed at excluding that the use of techno-scientific devices could constitute a tool to fight "climate change". Such positions can be traced back, mainly, to an exclusively technical framework of AI and, therefore, partly to the distance from a theoretical and scientific approach to Artificial Intelligence[16] or, also, to the idea that the expansion of AI, presenting – and also amplifying –

12. C. Ferlito, *L'ecologia come paradigma delle scienze sociali*, in *Teoria e Critica della regolazione sociale*, 2020, 37-59.
13. On this issue, see T. Greco, *La legge della fiducia. Alle radici del diritto*, Roma-Bari, Laterza, 2021; R. Pirosa, *Le ragioni della fiducia. Notazioni su un libro controcorrente*, in *Nomos*, n. 2/2022, 1-14.
14. L. Floridi, J. Cowls et al., *AI4 People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *National Library of Medicine. National Center for Biotechnology Information*, n. 28/2018, 689-707.
15. Cp. U. Pagallo, *Il dovere alla salute. Sul rischio di sottoutilizzo dell'Intelligenza Artificiale in ambito sanitario*, Milano, Mimesis, 2022.
16. See L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, cit., 297-317.

ethical and legal problems hard to solve, is always "virtually" in conflict with the protection of rights.

The thematization of AI implementation within the bioethical dimension focuses, however, more specifically on the evaluation of Artificial Intelligence different uses with regard to the principle of beneficence, non-maleficence, autonomy and justice and is therefore based on the bundle of relationships between disciplines and fields of knowledge that the bioethical perspective – as ethics applied to the world of life, in the interaction between technology, medicine, ethics and the environment[17] – implies.

In this sense, the link between the AI implementation and the effectiveness of the protection of the right to health, understood as "one-health", is crucial. This concept, developed since the main theoretical elaborations in Bioethics, became a shared idea only when the pandemic era expressed the binding connection between the human being as an individual and the social community, and its relationship with eco-systems as well[18].

The expression "one-health", therefore, is sufficiently capacious with respect to a complex idea of health, in which the scientific, and then institutional and legal, recognition of specific objective and subjective needs becomes central, and also the conceptualization of these needs as prodromal and crucial with respect to the effectiveness of the protection of relevant subjective situations.

This profile is particularly significant if we look at the differentiated nature of living conditions of individuals and groups, as there is an unbridgeable gap between the social groups that live, or rather try to survive, in areas of the planet burdened by climate instability and those who are affected by "climate change" effects, or whose descendants will be affected.

III. THE ROLE OF ARTIFICIAL INTELLIGENCE IN STRUGGLING CLIMATE CHANGE IN LIGHT OF THE PRINCIPLE OF BENEFICENCE

The idea according to which the creation of techno-scientific devices attributable to Artificial Intelligence is beneficial for humanity can be found in six different documents: "the principles on Artificial Intelligence established

17. Cp. H. Jonas, *Organismo e libertà. Verso una biologia filosofica*, Torino, Einaudi, 1999.
18. Cp. S. Rodotà, *Vivere la democrazia*, Roma-Bari, Laterza, 2018, esp. 132-152.

by the Asilomar Conference"[19]; the "Montréal Declaration for a Responsible Artificial Intelligence"[20]; the general principles established by the second version of the body of recommendations contained in "Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems"[21], better known as IEEE; the ethical principles codified by the "Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems", published by the European Group on Ethics in Science and New Technologies[22]; the five general principles for an Artificial Intelligence code provided for by the "UK House of Lords Artificial Intelligence Committee's Report"[23]; and, finally, in the fundamental rules regarding the "Partnership on Artificial Intelligence".

These are recent developments, directly relevant for the regulation of Artificial Intelligence implementation. The evaluation of AI practices on the basis of the principle of beneficence represents the least problematic area. According to the provisions of the Montreal Declaration, the development of Artificial Intelligence should promote the well-being of all sentient creatures, while the IEEE qualifies "human well-being" as a priority goal in all systems. The "UK House of Lords Artificial Intelligence Committee report" and the Asilomar Conference establish that AI must be developed for the common good and the benefit of humanity. The "Tenets of the Partnership on AI" provide the intention to ensure that techno-scientific devices benefit and enhance the subjective "empowerment" of as many people as possible in the world. The ethical principles codified in the "Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems" strongly recall human dignity and, at the same time, sustainability, essentially qualifying them as legal assets whose promotion and protection can be made even more effective by a regulated use of AI.

19. *Principles developed in conjunction with the 2017 Asilomar Conference on Beneficial AI*, 5-8 January 2017, *www.futureoflife.org*.
20. *The Montreal Declaration for a Responsible Development of Artificial Intelligence*, *www.montrealdeclaration-responsibleai.com*.
21. *Ethically Aligned Design, the IEEE Iniziative on Ethics of Autonomous and Intelligent Sis*tems, *www.ieeexplore.ieee.org*.
22. European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and 'Autonomous'*, *www.unapcict.org/resources/ictd-infobank/statement-artificial-intelligence-robotics-and-autonomous-systems*.
23. House of Lords, Select Committee on Artificial Intelligence, Report of Session 2017-19, *AI in the UK: ready, willing and able?*, *www.publications.parliament.uk*.

Beneficence as a key principle of bioethics, therefore, is inextricably linked to the promotion of psycho-physical and social well-being of people and planet through Artificial Intelligence.

In this framework, it is interesting to note that these documents offer an axiological basis for the idea according to which the development of Artificial Intelligence is conceived as an anti-discriminatory technique with retroactive and proactive effect in relation to the specific access to resources ensuring the psycho-physical and social well-being of people on the planet.

In particular, the ethical principles codified in the "Statement on Artificial Intelligence, Robotics and 'Autonomous' System healthcare" affirm the relevance of protection systems based on a solidarity approach and, therefore, the need to avoid disparities in health care and access to social benefits.

From an analysis of these documents the conformity of the use of techno-scientific devices with legal provisions appears necessary, but *per se* not sufficient, in the field of the implementation of Artificial Intelligence.

An "ethical approach" to AI performs two important functions: on the one hand, it allows us to assign centrality to axiological evaluations which could direct, for example, international bodies, public administrations and social organizations towards the goal of taking advantage of the social value of Artificial Intelligence; on the other hand, this perspective allows political, administrative and social groups to anticipate, avoid or at least reduce risks[24].

With regard to climate change, as mentioned previously, the use of techno-scientific devices was considered in relation to the risk of amplifying inequality between subjective categories and also opacity as an obstacle to fully intelligible and knowable processes.

In this direction, therefore, we note the need for a so-called "soft ethical approach" to AI[25] to permeate policy choices and decision-making processes, especially with reference to the European Union, in which this concept is recognized in relation to science, engineering, technology and innovation and where, starting from June 2023, it has received legal recognition[26].

---

24. L. Floridi, *AI and its new winter: from myths to realities*, in *Philosophy and Technology*, n. 33/2020, 1-3.
25. L. Floridi, *In poche battute. Brevi riflessioni su cultura e digitale 2011-2021*, Vellum, 2002, 299.
26. On June 14, 2023, the Artificial Intelligence Act was passed: *www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.pdf*.

IV. SPARKS FOR A PHILOSOPHICAL-LEGAL PERSPECTIVE USEFUL FOR PROMOTING AI IN THE FIGHT AGAINST CLIMATE INSTABILITY

The evaluation of the role of AI in the fight against climate change significantly concerns philosophical-legal reflection and its tasks. As a matter of fact, the promotion of Artificial Intelligence is intertwined with a theoretical-legal understanding of climate change and, in particular, to the function of law with respect to the protection of subjective rights. The legal dimension, in this sense, offers a context in which violations of individual and collective rights can be assessed starting from the conceptualization of a relevant subjective situation: the "right to climate".

It should be noted that the topic of right to climate is not limited to a speculative approach focused exclusively on the problem of the origin and foundation of such a right or, therefore, on its theoretical postulability, but rather grounded on the "claiming", on the "agency to claim" this right, conceived as the possibility of effective exercise[27].

First Norberto Bobbio[28], and later Luigi Ferrajoli, focused on the issue of human rights universalizability, distinguishing the possibility of universalizing their foundation from universalizing the condition of the subjects in law[29]. Ferrajoli, in particular, emphasises the success and strength vigor of a debate on universalism relating to the problem of rights foundation, highlighting, in the context of a critical reflection aimed at considering the aporetic profiles of the legal dimension, the paradox often inherent to subject in-law condition which, conceptualized as "universal", precisely when someone looks at this qualification, does not result in a full effectiveness[30].

In this regard, within the framework of an even more radical theoretical proposal, Danilo Zolo, rejecting a top-down logic, overcame passed the problem of the theoretical foundation of rights and highlighted a

27. Cp. L. Baccelli, *I diritti dei popoli. Universalismo e differenze culturali*, Laterza, Roma-Bari, Laterza, 2009, especially 99-103 and before J. Feinberg, *Duties, Rights, and* Claims, in *American Philosophical Quarterly*, 1966, 2, 137-144; Idem, *The Nature and Value of Rights*, in *Journal of Value Inquiry*, 1970, 4, 243-260.
28. See N. Bobbio, *L'età dei diritti*, Torino, Einaudi, 2014.
29. Cp. L. Ferrajoli, *I diritti fondamentali nella teoria del diritto*, in Idem, *Diritti fondamentali. Un dibattito teorico*, Roma-Bari, Laterza, 2001, 119-175.
30. *Ivi*, 277-370.

degradation of rights – in relation to some particular categories of rights – to services[31].

The idea of a "right to climate" does not imply hypotheses on the foundation of this relevant subjective situation, but firstly it can be developed considering the circumstance that this right, for example, has been implemented in concrete cases, at the initiative of associations and individual.

Focusing on the topic under discussion, therefore, Zolo's thought is important in a number of ways: firstly, as a legal philosopher he denies the opportunity of a foundationalist attitude of legal-philosophical reflection on fundamental rights[32]; secondly, since his reflection introduces the concept of "service" as a term that qualifies the degradation of social rights, but which, in disadvantaged countries, also identifies the diminished condition of subjects-in law in relation to the enjoyment of political rights and, also, to civil rights. The right to climate, therefore, could appear, in part, as a "service", which can be exercised where economic resources are available. For this reason, in the countries of the Euro-Atlantic area, "common sense" very rarely describes the phenomenon of climate change in terms of climate collapse.

The reference to Zolo's anti-foundationalist perspective coexists well, however, with the need to pay attention to the arguments which, in a technical sense, go towards the theoretical possibility to ground right to climate[33]. Some areas of interest, in the philosophical-juridical discourse, require a repositioning of the relationship between law and ethics; in particular, the perspective of subjective rights – or more specifically of human rights – highlights the centrality of axiological evaluation as a prerequisite for the legal recognition of relevant subjective situations[34].

The theme of the urgency of rights in the anthropogenic climate change creates an area into which law, politics and science flow and whose boundaries

31. D. Zolo (ed.), *La strategia della cittadinanza*, in Id. *La cittadinanza. Appartenenza, identità, diritti*, Roma-Bari, Laterza, 1999, 3-46; Idem, *Da cittadini a sudditi. La cittadinanza politica vanificata*, Milano, Edizioni Punto Rosso, 2007.
32. D. Zolo, *Humanitarian Fundamentalism*, in *Jura Gentium. Rivista di filosofia del diritto internazionale e della politica globale*, n. 1/2005, 12-27.
33. A. Pisanò, *Il diritto al clima. Il ruolo dei diritti nei contenziosi climatici europei*, cit., 27.
34. B. Pastore, *Semantica della vulnerabilità, soggetto, cultura giuridica*, Torino, Giappichelli, 32.

between the areas involving these sectors, central to the human experience, are constantly being redefined.

The recognition of "right to climate" as a relevant subjective legal situation connected with the idea of "one-health" – and, therefore, to the right to psycho-physical and social well-being – but also to conditions of existence in which this right can be effectively exercised and even claimed before the judge can be the premise for a thematization of the role of AI in relation to climate change. We can consider this last profile not only from a rights protection point of view, but also more centrally from a "right to climate" protection point of view, as a prerequisite for the effectiveness of other relevant subjective legal situations.

Climate change understanding, in the theoretical-legal discourse, can significantly influence, in light of the weighing up measurement of advantages and disadvantages in the use of Artificial Intelligence, national and international policies regarding AI implementation.

Furthermore, a "right to climate" conceived in relation to an "ethical foundation" offers a legal-axiological parameter useful for evaluating Artificial Intelligence's role within the framework of the principle of beneficence.

In this sense, it is possible to introduce an example. The theme of the urgency of rights with respect to climate change involves migration issue. Migration Theory, having regard to the people who most frequently "decide" to migrate and who survive a very dangerous journey, highlights a change in the paradigm of international mobility in which "migration projects", in the vast majority of cases, have no more the objective of stabilization, but the goal to survive and, then, to come back in the country of origin.

It implies attention to bilateral nature of the phenomenon and therefore, the need, to look not only at the perspective of the so-called countries of immigration, but also at the reasons of those who emigrate, at the experience of those who travel, being forced to do so several times[35]. In this sense, the prospects for using AI clearly outline the geography of the differences

35. Cp. A. Sayad, *La double absence*, Paris, Éditions du Seuil, 1999, it. transl. *La doppia assenza. Dalle illusioni dell'emigrato alle sofferenze dell'immigrato*, Milano, Raffaello Cortina Editore, 2002; Bordieu, L. Wacquant, *The Organic Ethnologist of Algerian Migration*, in *Ethnography*, 2000, 173-182.

between the so-called high-income countries and the medium-income and low-income countries, but also the specificity of implementation fields[36].

The reasons for emigrating are covered by jurisprudence and law: someone can ask for asylum, subsidiary protection or humanitarian protection if she or he proves that she or he is persecuted in your country of origin for political, racial, religious discrimination or for sexual orientation.

The recent relationship between law and issue of climate change, and a euro-centric perspective that has permeated its understanding gives rise to the fact that the Italian legislator or judge, for example, does not identify climate change as a legally relevant reason for where a person is forced to leave their country of origin. The doctrine has created "climate migrants" as a provision, but the law, *de facto*, does not provide specific protection. The person defined as a "climate migrant", in a critical theoretical-legal perspective, challenges the liberal construction of the subject in law, as a "permanent" subject holder of citizenship, as a *civis*.

In this regard, scientific AI implementation is a crucial tool for understanding some of the structural causes of the change of the paradigm of international mobility[37] and, even before that, for scientifically establishing the necessity and inescapability of migration experiences which, often, are not the outcome of a carefully thought-out project but rather derive from the need to survive climate collapse.

V. THE ADVANTAGES OF USING AI IN THE RESTRAINING OF THE EFFECTS OF CLIMATE CHANGE

The advantages deriving from Artificial Intelligence are, at the same time, scientific and practical[38]. The AI implementation, first of all, promotes scientific understanding of climate change by allowing the processing of macro-aggregates of data necessary for the study of present and future climate trends and for the development of political responses and normative solutions. The use of techno-scientific devices can determine the exact prediction of natural disasters which constitute some of the main and most recurrent manifestations of climate instability: hurricanes, heavy rains, forest

36. U. Pagallo, *Il dovere alla salute. Sul rischio di sottoutilizzo dell'Intelligenza Artificiale,* cit., especially 35-36.
37. Cp. A. Triandafyllidou (ed.), *Multicultural Governance in a Mobile World*, Edinburgh, Edinburgh University Press, 2017.
38. See: L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, cit., 298-299.

fires and, also, the socio-political consequences, like the constant increase in migratory processes. AI techniques also play a role in elevating the predictive potential of forecasting systems through the automatic qualification of climate model data[39].

In the area of interaction between science, politics and law, therefore, the improvement of the scientific understanding of climate collapse understood in its complex phenomenology and in relation to the causative factors, becomes crucial.

The favorable effects of AI implementation can be traced back, unavoidably, to a pragmatic dimension. In this field, the use of techno-scientific devices can mainly allow the reduction of anthropogenic climate-altering activities and, therefore, the achievement of energy efficiency in daily life and in industry.

AI techniques implementation can also consist of predicting carbon emissions based on social behavior and monitoring its removal from the atmosphere.

There are AI projects that have at their core the promotion of the sustainable development goals promoted by the United Nations. The Artificial Intelligence for Climate (AI for Climate) program of the AI development company ElementAI considers and offers partnership opportunities to improve energy efficiency[40]. The "European Lab for Learning & Intelligent Systems (ELLIS)" aims for full intelligibility of the Earth system through a machine learning program for Earth and climate sciences aimed at understanding the relevant processes[41]. The European Space Agency has established the Digital Twin Earth Challenge[42] to improve forecasting systems on the impact of climate change and support social and political responses.

The role of law and politics becomes fundamental in the development of normative solutions and policy choices suitable for optimizing AI implementation results. As a matter of fact, political decision-makers and legal actors can position themselves in a strategic and crucial way in order to address AI ecological footprint and policy choices aimed at its reduction.

The transition from the objectives that AI allows to achieve to Artificial Intelligence techniques' effectiveness shows how the main disadvantage can be connected to the increase in greenhouse gas emissions due to the high

39. *Ivi*, 299
40. *www.elemntai.com/ai-for-climate*.
41. *www.ellis.eu*.
42. *www.esa.int/Applications/Observing_the_Earth/Working_towards_a_Digital_Twin_of_Earth*.

computational power of techno-scientific devices. Other unfavorable aspects can be identified in the strengthening of "bias" in "augmented reality" which may derive from AI action on a reality already characterized by strong social and economic differences.

As an example, the placement of supplies for electric cars can be determined on the basis of existing demand which currently expresses an almost total diffusion of cars with low environmental impact among high-income population groups, because of, in addition to the vehicles cost, the location of the infrastructures that allow their use.

This last profile also confirms the importance of building a political and legal framework within which Artificial Intelligence implementation is directed towards maximizing favorable effects in combating climate change, in the framework of a more complex plan aimed at an AI sustainable use and at the neutralization – contraction – of its ecological footprint. The soft law sources at European level do reveal, on a programmatic level, this intent, giving value, within the principle of benefit, to the function of techno-scientific devices in protecting the environment and in the fight against climate change.

On a factual level, the progression in terms of effectiveness and efficiency which, in the abstract, would be determined by Artificial Intelligence is hindered by the scarcity of shared data resulting from the absence of Data Centers and by the lack of knowledge about the potentiality of AI implementation. There are research horizons that, through algorithmic improvements, aim to reduce the computational burden and energy consumption of AI techniques.

Some Artificial Intelligence models require considerable energy consumption, estimated, however, as lower than the amount of energy that would be necessary if the techno-scientific devices were not used. Even with regard to this profile, the role of political and legal decision makers is crucial to guide the strengthening of AI in the field of balancing the relevant instances.

VI. CONCLUSIONS

A broader awareness within theoretical-legal reflection on the extent of climate change and its impact on relevant subjective, individual and

collective situations, certainly calls for a deeper knowledge of the role of AI in combating climate change.

In this direction, authoritative proposals highlight the need to establish a global observatory to prove the evidence of the use of AI in relation to climate change, which could be the practical premise for the creation of a common data space global climate[43]. Within this context, the interaction between the scientific community and political decision-makers should reproduce the central goal to use data centers in order to contain climate collapse.

The European Union could fulfill a fundamental function in a global context in which climate-related policies essentially have a state-centric imprint, being aimed at defining the regulatory framework within which States implement, autonomously, their specific policies to combat climate change.

Notable outcomes such as the UE regulation of Artificial Intelligence implementation emblematize an attraction of soft law towards the orbit of hard law which, in some fields, expresses the revitalization of the legislative in the legal protection of relevant subjectivities, as opposed to a rights protection paradigm focused exclusively on the role of judicial courts.

Climate change, nevertheless, is connected to the environment and profoundly affects every aspect of human experience, demanding a change in the "ontological model". As a matter of fact, the fight against "climate change" implies a rethinking of the ontology in which human beings have placed themselves as part of the planet, but also as a superordinate entity compared to other living beings[44].

This complex deconstruction and ontological reconstruction, which is the basis of a biocentric perspective, concerns the individual's self-understanding on his or her approach to life, his or her concept of the world, the interpretation and management of public institutions, primarily the political, legal and economic ones, but also the perspective on education and scientific research.

The transition of human being towards this deconstructive and, at the same time, reconstructive experience cannot, however, be separated from the awareness of the expansion and relevance of the role of Artificial Intelligence

43. L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, cit., 300.
44. See A. Porciello, *Filosofia dell'ambiente. Ontologia, etica, diritto*, Roma, 2022.
Cp. L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, cit., 21-37.

in the "re-ontologization" of reality[45]. It is, therefore, up to human being to adapt to this epochal change towards an epistemological perspective able to govern its effects and to provide the opportunity to "(re-)situate herself or himself"[46].

Moreover: "It is precisely the ontic roots that challenge human beings, inducing her or him to limit her or his own purposes and assume responsibility for goods that go beyond her or his needs"[47].

45. A. Porciello, *Filosofia dell'ambiente. Ontologia, etica, diritto*, Roma, 2022.
Cp. L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, cit., 21-37.
46. Hans Jonas, emancipating himself from his mentor Martin Heidegger, conceived "Situated Being" as not simultaneously coexisting with death, interpreting "Dasein" not only as a fact, but as a value. On this issue, see: Becchi, R. Franzini Tibaldeo, *Principio umanità e ambiente. Una riflessione su Hans Jonas*, in *Diritti umani e ambiente*, Expressão Gráfica, Fortaleza, 2017, 115-139.
47. H. Jonas, *Il principio responsabilità: un'etica per la civiltà tecnologica*, Torino, Einaudi, 2009, 718.

Constitutional law

Non-discrimination and the AI Act

[1 2 3]Lucia Bosoer*, Marta Cantero Gamito†, Ruth Rubio§

ABSTRACT: The forthcoming EU AI Act is expected to be a comprehensive regulatory framework for human-centric artificial intelligence systems (AIS), ensuring the safe and ethical development, deployment, and use of AIS in the European Union. One of the key objectives of the AI Act is to prevent bias, discrimination, and unfair treatment in AI systems. This chapter summarizes and exemplifies the ways in which algorithmic discrimination can occur in AI systems and proceeds to critically examine the provisions related to non-discrimination in the AI Act and to assess their potential effectiveness in addresing such discrimination.

KEYWORDS: Non-discrimination; bias, fairness; AI Act; rights-based approach.

* Project Associate, Florence School of Transnational Governance, European University Institute.

† Professor of Information Technology Law, University of Tartu; Research Fellow, Florence School of Transnational Governance.

§ Professor of Constitutional Law, University of Sevilla.

I. INTRODUCTION

Artificial intelligence (AI) is permeating the technological, economic, and societal dimensions of our lives, offering unprecedented advances in efficiency, data analysis and problem-solving capabilities across different sectors. Despite the positive applications of this technology, public opinion is becoming increasingly sensitive to the use and effects of AI given its capacity to endanger democracies around the world and amplify discriminatory biases[1]. Accordingly, legislators around the world are trying to produce policy and legislative frameworks to address the important risks posed by AI systems, especially where they involve fundamental rights. Against this context, the European Union's forthcoming Regulation on artificial intelligence (henceforth, 'AI Act')[2] stands as a promising response, seeking to provide a robust legal framework that ensures that AI systems adhere to ethical and democratic principles.

Legal scholarship has sufficiently discussed the possibility of AI systems enabling direct[3] and indirect[4] discrimination, both illegal practices under EU legislation. On the occasion of the significantly anticipated regulatory framework, this chapter focuses on how the proposed AI Act deals with algorithmic discrimination and analyses if and how the forthcoming provisions might set a framework for preventing it.

A cursory glance reveals a complex landscape. Algorithmic discrimination challenges the traditional confines of protected groups, prompting scholars and policymakers to grapple with differentiating between unlawful discriminatory practices and those stemming from normal algorithmic

1. X. Ferrer, T. van Nuenen, J.M. Such, M. Coté, N. Criado, *Bias and discrimination in AI: a cross-disciplinary perspective*, in *IEEE Technology and Society Magazine*, 40(2), 2020, 72-80; S. Cave, K. Dihal, *Race and AI: The diversity dilemma*, in *Philosophy & Technology*, 34(4), 2021, 1775-1779. For a more practical report, see E. Constantaras et al., *Inside the Suspicion Machine*, in *Wired Magazine*, March 6, 2023.
2. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM(2021) 206 final.
3. R. Xenidis, L. Senden, *EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination*, in U. Bernitz, X. Groussot, J. Paju, S.A. de Vries (eds.), *General Principles of EU Law and the EU Digital Order, Kluwer Law International*, Kluwer Law International, 2020; F. Zuiderveen Borgesius, *Discrimination, artificial intelligence, and algorithmic decision-making*, Council of Europe, 2018. Available at *https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73*.
4. F.Z. Borgesius, *Price discrimination, algorithmic decision-making, and European non-discrimination law*, in *European Business Law Review*, 31(3), 2020.

operations, which are designed to systematically discriminate[5]. This inherent tension underscores the complex interplay between technological advancements and established legal principles.

This chapter proceeds as follows. First, we define AI and explain the underlying mechanisms that can lead to algorithmic discrimination. We illustrate this section with a variety of examples from different areas where an AI system yielded discriminatory results. Second, we critically examine how biases and discrimination are addressed by the forthcoming AI Act. Finally, we present the main challenges that the new legislation faces in terms of non-discrimination in the EU.

II. (NON-)DISCRIMINATION IN THE AGE OF AI

II.1. PRELIMINARY DEFINITIONS

Before examining non-discrimination in times of AI, it may be useful to provide some definitions. In the field of AI this becomes a particularly difficult task, as there is no universal consensus on what the definition of AI should actually encompass, and AI is often used as catch-all term that includes very different techniques[6]. Still, it is possible to find some baseline definitions in the efforts of various countries and international organizations to agree on certain principles for regulating AI.

According to the latest version of the AI Act, artificial intelligence "means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments"[7]. In a similar vein, the OECD considers an AI system as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments"[8]. The UNESCO Recommendation on the Ethics of Artificial Intelligence defines AI systems as "systems which have the

5. F. Pasquale, *The black box society: The secret algorithms that control money and information*, Harvard University Press, 2015.
6. T. Madiega, *Artificial Intelligence Act*, European Parliamentary Research Service, 2023. Available at *https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792#:~:text=The%20European%20Commission%20tabled%20a,AI%20systems%20and%20associated%20risks*.
7. *https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html*.
8. OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449. Available at *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449*.

capacity to process data and information in a way that resembles intelligent behaviour, and typically includes aspects of reasoning, learning, perception, prediction, planning or control"[9].

Over the last decade, one of the AI subfields that has evolved the most is machine-learning, which has led to the fact that there is almost no field of our lives that is not affected or will not be affected in the near future by AI. Machine learning is an AI technique that allows to discover "correlations (sometimes alternatively referred to as relationships or patterns) between variables in a dataset, often to make predictions or estimates of some outcome"[10].

According to the US Blueprint for an AI Bill of Rights – issued by the White House in 2022 – discrimination in AI occurs when machine-based systems "contribute to unjustified different treatment or impacts disfavouring people based on their race, colour, ethnicity, sex (including pregnancy, childbirth, and related medical conditions, gender identity, intersex status, and sexual orientation), religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law"[11]. For the purposes of this contribution, we shall leave aside the understanding of the concept of discrimination as differentiation between categories, which is often used in the field of computer science. Algorithmic discrimination can be understood as the result of an algorithmic bias, defined as "an anomaly in the output of AI systems, due to the prejudices and/or erroneous assumptions made during the system development process or prejudices in the training data"[12].

II.2. HOW CAN AI AND ALGORITHMIC DECISION-MAKING LEAD TO DISCRIMINATION?

Algorithmic discrimination can take place intentionally, i.e., when AI systems are used to discriminate deliberately, or non-intentionally. Non-

9. *https://unesdoc.unesco.org/ark:/48223/pf0000381137*.
10. D. Lehr, P. Ohm, *Playing with the data: what legal scholars should learn about machine learning*, in *U.C. Davis Law Review*, 51(2), 2017, 671. Available at *https://heinonline.org/HOL/Page?handle=hein.journals/davlr51&div=26&g_sent=1&casa_token=&collection=journals*.
11. White House, *The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*, *White House Office of Science and Technology Policy*, Washington DC, October 2022, 10. Available at *https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf*.
12. M. Estevez Almenzar, D. Fernández Llorca, E. Gómez, F. Martínez Plumed, *Glossary of human-centred artificial intelligence*, in *Publications Office of the European Union*, Luxembourg, 2022, *doi:10.2760/860665, JRC129614*.

intentional algorithmic discrimination is the most problematic as it is the most difficult to identify and correct. Moreover, the problem of black boxes – AI models whose reasoning process remains unexplainable to the user – makes it extremely difficult to spot a discriminatory pattern, because how the system arrived at a certain output or decision is unknown[13].

In a landmark article, Barocas and Selbst (2016) identified four ways in which an AI system can yield unintentionally biased results[14]. The first concerns the definition of the "target variable" and the "class labels". As the authors explain, "while the target variable defines what data miners are looking for, 'class labels' divide all possible values of the target variable into mutually exclusive categories"[15]. For example, in an algorithm that is set to detect spam, the target variable is spam, and the class labels are either 'spam' or 'non-spam'[16]. However, many times the target variables and class labels are not so obvious, and the programmer has to state in simple terms, understandable to a machine, a problem that emerges from a much more complex social reality[17]. This implies, evidently, a certain degree of subjectivity on the part of the programmer. As Crawford notes: "To create a training set is to take an almost infinitely complex and varied world and fix it into taxonomies composed of discrete classifications of individual data points, a process that requires inherently political, cultural and social choices"[18]. Take, for example, the case of an algorithm designed to identify good employees[19]. Clearly, what makes a "good employee" is not a given. It is the programmer who has to identify the measurable characteristics that make a good employee (productivity, timeliness, number of sales, years of service, availability, etc.). Thus, it is not difficult to see how human bias can affect this process and lead to discriminatory scenarios.

13. F. Pasquale, *The black box society*, cit. See also T. Cassauwers, *Opening the 'black box' of artificial intelligence*, 2020: *https://ec.europa.eu/research-and-innovation/en/horizon-magazine/opening-black-box-artificial-intelligence*.
14. S. Barocas, A.D. Selbst, *Big Data's Disparate Impact*, in *California Law Review*, 104(3), 2016, 671-732.
15. *Ivi*, 678.
16. *http://fra.europa.eu/en/publication/2018/brief-big-data-algorithms-and-discrimination*.
17. L. Cotino Hueso, *Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público*, in E. Gamero Casado, F.L. Pérez Guerrero (eds.), *Inteligencia artificial y sector público. Retos, límites y medios*, Tirant lo Blanch, 2023, 260-338.
18. K. Crawford, *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*, Yale University Press, 2023, 135-136.
19. S. Barocas, A.D. Selbst, *Big Data's Disparate Impact*, cit., 679.

The second way in which an AI system can unintentionally discriminate relates to the data from which the algorithm learns. As the old adage goes, "garbage in, garbage out", which is to say that if the machine-learning model learns from biased data, it will yield biased results. Barocas and Selbst go even deeper and differentiate between two ways in which this can happen. On the one hand, algorithms may be exposed to real-world cases already affected by human prejudice and thus the system will reproduce that prejudice in its results. On the other hand, algorithms may learn from a biased sample of the population, and thus the output of such an algorithm will skew against the underrepresented population[20]. The data from which the systems learn is not always representative of the whole society. If there is no data from a certain social group – for example, due to the persistent digital divides – the machine will tend to exclude that group from its results[21].

The third and fourth ways in which algorithmic discrimination can occur unintentionally have to do with feature selection and proxies, respectively. The authors note that "through a process called 'feature selection', organizations – and the data miners that work for them – make choices about what attributes they observe and subsequently fold into their analyses"[22]. This can lead to discriminatory outcomes if certain groups are not well represented in the categories the organization chooses to look at. This is the case, for example, of an employer who chooses to select its workers based on their education, and certain groups are automatically left out of the job because they were not able to access a well-ranked university.

Lastly, the problem of proxies, one of the most difficult to address, arises when "a particular piece of data or certain values for that piece of data are highly correlated with membership in specific protected classes"[23]. In other words, the algorithm is trained on data that seems to be neutral, but is nevertheless highly correlated with a protected characteristic, such as gender or race. Zuiderveen Borgesius et al. illustrate such a mechanism with an example from the banking sector[24]. Suppose a bank decides to grant loans based on the likelihood that the loan applicants will be able to repay them. For this, it uses an AI system that learns from data covering the last twenty years and comes up with the result that people living in a certain

20. *Ivi*, 680-687.
21. *https://www.derechosdigitales.org/fair-2023-en/*.
22. S. Barocas, A.D. Selbst, *Big Data's Disparate Impact*, cit., 688.
23. *Ivi*, 692.
24. F. Zuiderveen Borgesius, *Discrimination, artificial intelligence, and algorithmic decision-making*, Council of Europe, 2018. Available at *https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73*.

postal code have been more likely to default on the loan. Assume now that this postal code was correlated with a given racial origin. The bank would then end up denying loans to people with that postal code, and at the same time discriminating against a certain racial origin[25].

To these four ways of unintentional algorithmic discrimination, we should add the quite common scenario where an AI system creates discrimination problems because it is used in a different context or for a different population for which it was originally developed[26]. An algorithm may be fed with data that are representative of a certain population, but if that same algorithm is used in a different context, the same data could become biased. Latin American countries, for example, are increasingly using biometric identification systems imported from foreign companies that may have trained their algorithms with data from other regions[27]. Thus, a facial recognition system trained in Israel, for example, may be sufficiently accurate in that country, but not in Chile, Peru, or Bolivia, where many citizens are descendants of indigenous peoples.

Algorithmic biases pose an even more difficult challenge when considering automation bias, which basically refers to our tendency to rely excessively on automated decision-making systems, often ignoring one's own intuition[28]. The automation bias leads humans to uncritically accept the results or output generated by AI systems, without any type of supervision. There are plenty of cases that show that algorithmic discrimination is everywhere and can cause great harm. In the next section, we will provide a brief glimpse of some of these.

II.3. EXAMPLES OF ALGORITHMIC DISCRIMINATION

The number of instances in which an AI system has produced a situation of inequality are countless, and they are equally common in the public as in the private sphere. One of the public areas in which the biases introduced by these systems have been most evident is in that of justice and crime prevention. The most widely cited case is that of the "Correctional Offender

25. *Ivi*, 21.
26. R. Valle Escolano, *Transparencia en la inteligencia artificial y en el uso de algoritmos: una visión de género*, in L. Cotino Hueso, J. Castellanos Claramunt (eds.), 2022, 99: *https://www.uv.es/cotino/publicaciones/libroabiertotp22.pdf*.
27. AccessNow, Surveillance Tech in Latin America: Made Abroad, Deployed at Home, 2021. Available at: *https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf*.
28. See Article 14 "Human Oversight" of the AI Act.

Management Profiling for Alternative Sanctions" (COMPAS), an algorithmic prediction system used for the calculation of criminal recidivism in the US. The COMPAS software helps judges decide whether a person should be granted probation[29]. In 2016, a ProPublica investigation showed that the COMPAS algorithm was biased against black people. As the journalists explained, "the formula was particularly likely to falsely flag black defendants as future criminals, wrongly labelling them this way at almost twice the rate as white defendants. White defendants were mislabelled as low risk more often than black defendants"[30].

Also, in the field of policing, there are many cases in which facial recognition systems located in public spaces have yielded biased results. It has been widely proven that the accuracy of many of these systems is low, resulting in a large number of "false positives" and "false negatives"[31]. While false negatives can be a problem in terms of crime prevention, false positives can lead to serious discriminatory outcomes. In 2019, research conducted by the Security Observatory Network found that 90.5% of people arrested in five Brazilian states using facial recognition cameras were black people[32]. In countries such as Brazil, where a large part of the population is black, the poor accuracy of biometric identification systems is compounded by the fact that many of these are acquired from foreign companies that often train their algorithms on databases that are not representative of the population of the countries or cities that acquire their products.

One of the social sectors in which AI systems are being employed the most today is that of health. In 2019, an article published in Science showed how an algorithm widely used by the US healthcare system to target patients for "high-risk care management" programs were disfavouring Black patients.[33] The bias was explained by the fact that the algorithm used health costs as a proxy for health needs. Because black people had received less health care and thus had generated less costs, the system assumed that they needed

29. F. Zuiderveen Borgesius, *Discrimination, artificial intelligence*, cit., 23-24.
30. J. Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks*, 2016, in *www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing*.
31. See P. Grother, M. Ngan, K. Hanaoka, *Face recognition vendor test (fvrt): Part 3, demographic effects*, in *National Institute of Standards and Technology*, 2019.
32. P. Nunes, *Levantamento revela que 90,5% dos presos por monitoramento facial no brasil são negros. The Intercept*, 2019. Available at *https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/*.
33. Z. Obermeyer et al., Dissecting racial bias in an algorithm used to manage the health of populations, in *Science 366*, 2019, 447-453.

less medical care. But, as the authors put it, "there are many opportunities for a wedge to creep in between needing health care and receiving health care—and crucially, we find that wedge to be correlated with race"[34]. On the other side of the continent, in the province of Salta, Argentina, the local government made an agreement with Microsoft to implement an algorithm that would predict teenage pregnancy[35]. The Technology Platform for Social Intervention – as the AI system was named – used data such as age, ethnicity, country of origin, and access to hot water to reach its conclusions. However, it did not consider other variables that account much better for teenage pregnancy, such as sex education and contraceptive methods[36]. Due to the opacity that surrounded the program and its complete lack of accountability, it remained unclear how government authorities intended to use the information provided by the platform.

If we look at the employment sector, the picture is not much more promising. Increasingly, companies are implementing AI systems to find and hire workers, monitor their performance, and define payments and promotions, among other things. An algorithm used by the Public Employment Service Austria (AMS) looked at features such as gender, age, disability, and citizenship to classify job seekers into three groups, according to their chances in the labour market[37]. Group A consisted of people who had high changes on the job market, and therefore were not considered to need support from the AMS. Group B comprised job seekers with medium chances on the job market and that should benefit from full access to the AMS resources. Finally, those individuals who were predicted to have low chances in the labour market were assigned to Group C, in which the AMS did not have to allocate resources as it meant an investment in people who would not benefit from it[38]. The system gave the female category a lower score because, based on past data, it inferred that women were less likely to find a job. The fundamental problem with the AMS algorithm was that it inferred from data from the past an individual's chances for job placement

34. *Ivi*, 450.
35. D. Jemio, A. Hagerty, F. Aranda, *The Case of the Creepy Algorithm That 'Predicted' Teen Pregnancy*, in *Wired*, 2022: *https://www.wired.com/story/argentina-algorithms-pregnancy-prediction*.
36. *https://notmy.ai/es/project-item/plataforma-tecnologica-de-intervencion-social-es/*.
37. P. Lopez, *Reinforcing Intersectional Inequality via the AMS Algorithm in Austria*, University of Vienna, 2019.
38. *Ivi*, 291; see also *https://algorithmwatch.org/en/austrias-employment-agency-ams-rolls-out-discriminatory-algorithm/*.

on the labour market, thus perpetuating social exclusion[39]. In another case of algorithmic discrimination in the employment sector, a study published in 2019 showed that Facebook displayed ads for supermarket cashier positions primarily to women, while ads for jobs with taxi companies were primarily targeted to blacks[40].

In 2021, the Dutch government stepped down due to a scandal where the Dutch Tax and Customs Administration incorrectly accused individuals of fraud in childcare benefits, driven in part by a risk assessment algorithm. This algorithm factored in Dutch citizenship, treating non-citizens as higher risk. The Dutch Data Protection Authority (DPA) confirmed that using nationality in the risk model was discriminatory per Article 21 of the Charter of Fundamental Rights of the European Union and violated the fairness principle of the GDPR[41]. The Dutch DPA highlighted that non-Dutch citizens might face more intense scrutiny in their applications, as these applications had to be individually reviewed, putting them at a disadvantage.

We have seen cases of algorithmic discrimination in policing and crime prevention, justice, healthcare, employment, and advertising, but examples extend to many other areas of the analogue world, such as education[42] and banking[43], and the digital world, such as image search[44] and translation tools[45] – although these two worlds are increasingly intertwined. There is a great deal of debate around the question of whether AI systems generate greater discrimination or are simply a reflection of historical patterns of discrimination in society[46]. There are also those who argue that AI systems could actually contribute to identifying biases and overcoming structural

39. L. Cotino Hueso, *Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público*, cit., 266.
40. M. Ali, P. Sapiezynski, M. Bogen, A. Korolova, A. Mislove, A. Rieke, *Discrimination through optimization: How Facebook's Ad delivery can lead to biased outcomes*, in *Proceedings of the ACM on human-computer interaction*, 3(CSCW), 2019, 1-30.
41. Article 5 GDPR.
42. See T. Feathers, *Major Universities Are Using Race as a "High Impact Predictor" of Student Success*, in *The Markup*, 2021: *https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success*.
43. *https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.*
44. See M. Kay, C. Matuszek, S.A. Munson, *Unequal representation and gender stereotypes in image search results for occupations*, in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2021, 3819-3828.
45. See M.O. Prates, P.H. Avelar, L.C. Lamb, *Assessing gender bias in machine translation: a case study with google translate*, in *Neural Computing and Applications*, 2020, 6363-6381.
46. F. Zuiderveen Borgesius, *Discrimination, artificial intelligence*, cit., 31.

inequalities[47]. For example, in the area of employment, research has shown that recruiters tend to hire people with whom they share characteristics – a phenomena often referred to as "like-me bias" or "affinity bias"[48]. The deployment of well-designed algorithms could in this sense help to avoid this type of individual bias by identifying those candidates with the skills that match best with a given position, regardless of other personal characteristics. Certainly, AI systems offer many opportunities, which does not detract from the fact that they are already reproducing existing biases in society, amplifying them, and creating new instances of discrimination.

III. NON-DISCRIMINATION IN THE EU AI ACT

III.1. OVERVIEW: NON-DISCRIMINATION AND THE RISK-BASED APPROACH IN THE AI ACT

The AI Act, proposed by the European Commission in April 2021 ('AI Act proposal', 'AI Act' or 'Proposal'), introduced the first dedicated legal framework to regulate artificial intelligence. One of the core principles of this regulation is the risk-based approach, which categorizes AI systems into different risk levels, each coming with its own set of requirements and restrictions.

Unacceptable Risk: Under this category, AI systems that could intensify or perpetuate biases and discrimination are strictly prohibited. This includes, for instance, systems designed for social scoring or those that might unfairly target specific demographics such as social-behavior, socio-economic status, or other personal factors[49].

47. See H. Margetts, *Rethinking AI for Good Governance*, in *Daedalus*, 2022, 360-371.
48. D.J. Patil, C. Munoz, M. Smith, *Big Data: a report of algorithmic systems, opportunity, and civil rights*, Obama White House Archives, 2016. Available at *https://obamawhitehouse.archives.gov/blog/2016/05/04/big-risks-big-opportunities-intersection-big-data-and-civil-rights*.
49. Recital 16 a latest draft: "AI systems that categorise natural persons by assigning them to specific categories, according to known or inferred sensitive or protected characteristics are particularly intrusive, violate human dignity and hold great risk of discrimination. Such characteristics include gender, gender identity, race, ethnic origin, migration or citizenship status, political orientation, sexual orientation, religion, disability or any other grounds on which discrimination is prohibited under Article 21 of the Charter of Fundamental Rights of the European Union, as well as under Article 9 of Regulation (EU)2016/769. Such systems should therefore be prohibited". See also Article 5(1) let b) and c).

High Risk: AI systems in areas like critical infrastructure, job recruitment, border control management or loan approvals fall under this category. Given the significant societal impact of these systems, the AI Act sets out strict obligations to ensure fairness and prevent discrimination. Before these systems can be launched, they need to meet specific criteria ('essential requirements') that ensure that they do not inadvertently favor or discriminate against particular groups.

Limited Risk: AI systems under this category, such as chatbots, might not seem discriminatory at first glance. However, it is crucial for users to know that they are interacting with a machine. Therefore, for limited-risk AI systems, the AI Act establishes certain transparency requirements to ensure that users are aware of potential biases in the machine's responses or actions.

Minimal Risk: AI systems falling under this risk category, like music or book recommendation systems, typically have a lower potential for discrimination. Therefore, the rules do not place special consideration to AI systems with minimal risks. However, we examine below how these systems may still build on discriminatory data and/or produce discriminatory results.

III.2 EXAMINATION OF THE LEGAL FRAMEWORK FOR NON-DISCRIMINATION IN THE AI ACT

The AI Act is expected to become the first dedicated transnational regulatory framework for a human-centered and ethically developed AI. It is important to consider that the proposed regulation blends elements of market regulation based on product liability with the protection of fundamental rights[50]. This peculiarity and the risk-based approach adopted by the legislator involve two important considerations. First, the conceptual delimitation of risk categories under the AI Act is critical in the legitimation of certain (potentially discriminatory) technologies. And second, the AI Act requires stringent standards for certain AI systems but only light-touch rules for other AI applications. In particular, the requirements to place safe and trustworthy AI systems in the EU internal market only apply to high-risk AI systems.

50. The legal basis used by the legislator is Article 16 and Article 114 TFEU.

III.2.1. The problem of risk categorisation

The AI Act's approach to risk categorisation is both ambitious and controversial. By delineating AI systems based on perceived threats, the Act seeks to balance innovation with societal safety[51]. However, while well-intended, the risk-based approach, focused on context-specific assessments, presents complexities when applied to real-world scenarios, raising important concerns. First, the rapid evolution of AI technology might outpace the pre-determined categories, necessitating frequent updates or leaving newer, potentially riskier systems unaddressed, such as applications of general purpose, which may simulatenously fall into different risk categories. Indeed, the release to the general public of Generative AI has led the European Parliament to consider specific obligations for the provider of foundation modesl[52].

Second, the boundaries between certain categories, especially regarding banned systems, are porous, creating challenges for both AI developers and regulators. This is due to the fact that the classification relies on different conceptual categories which combine undesired effects (eg. AI systems which can intensify or perpetuate bias) with identified areas or applications forcing the system to include, among other, a set of problematic exceptions. Article 6 of the AI Act proposal attempts to delineate high-risk AI systems, identifying sectors (like critical infrastructure, education, and employment) and specific use cases, contained in Annex III of the forthcoming Regulation. However, the exact criteria for determining what makes an AI application high-risk within those sectors are not exhaustively detailed, leading to potential ambiguities. At the moment of writing, there are critical considerations raised by civil society organisations concerning the categorization of high-risk AI systems, as the latest wording of Article 6 introduces a set of problematic exemption conditions. These would allow developers to unilaterally decide whether an AI system falls under the high-risk category, undermining the effectiveness of the regulatory framework[53].

For example, as originally conceived, certain AI uses – such as monitoring students' activities, evaluating an individual's credit reliability, screening job

51. See Article 28 b AI proposal (European Parliament, Negotiating positiondraft of June 14, 2023).
52. C. Novelli, F. Casolari, A. Rotolo, M. Taddeo, L. Floridi, Taking AI risks seriously: a new assessment model for the AI Act, in *Ai & Society*, 2023, 1-5.
53. See the petition letter and list of the signatories at: *https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-109_EU_legislators_must_close_dangerous_loophole_in_AI_Act.pdf*.

applicants, or determining eligibility for welfare benefits – were considered high-risk. This means that developers and deployers must comply with certain requirements (Articles 9 to 15, see below). These requirements are aimed at ensuring that those systems are fair, free from discriminatory biases, and disclose information on the operational mechanisms. However, the effectiveness of these measures risk being compromised if the aforementioned loophole is eventually incorporated into the final text.

III.2.2. The effectiveness of the requirements on high-risk AI systems

The AI Act introduces a set of mandatory requirements for high-risk AI systems[54], although it recommends the application of these regulations to all AI systems where possible. These requirements involve the implementation of risk management systems[55], practices for data handling and its governance[56], specific guidelines for producing technical documentation[57], rules for record keeping[58], detailed transparency provisions[59], ensuring human supervision[60], and maintaining standards (quality criteria) for accuracy, resilience, and cybersecurity[61].

While the primary objective of these requirements is to protect against general risks caused by AI systems, these obligations strongly resonate with the need to prevent society from underlying biases and potential discrimination. Traceability and explainability are the tenet of these requirements as providers of high-risk AI systems are mandated to demonstrate the initiatives undertaken to prevent bias and associated risks during every phase of the AI's development and deployment before the systems can be placed on the market.

In view of the complexity around risk categorization, the latest draft of the proposal – the negotiating position adopted by the European Parliament on June 14 –, introduced a new provision (Article 4a) that contains a set of general principles applicable to *all* AI systems. These principles are human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness,

54. Article 8.
55. Article 9.
56. Article 10.
57. Article 11.
58. Article 12
59. Article 13.
60. Article 14.
61. Article 15.

and social and environmental wellbeing. The provision defines each of these principles and in doing so it defines the principle of diversity, non-discrimination and fairness as meaning "that AI systems shall be developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law".

Setting aside the discussion around the definition of important value-laden principles in a piece of EU secondary legislation, the principle of diversity, non-discrimination and fairness meritoriously differentiates between discriminatory impact (algorithmic discrimination) and unfair biases (algorithmic biases), which the literature has identified as two separate categories banned under EU non-discrimination law.[62] Moreover, the obligation for AI systems to be designed and developed to achieve an appropriate level of accuracy, robustness, safety, and cybersecurity[63], is also connected to non-discrimination, as algorithmic discrimination may occur as a result of inaccurate data. This provision requires putting in place technical solutions to prevent data attacks to manipulate datasets ('data poisoning') or to cause the system to make mistakes ('adversarial machine learning'), which may result in harmful (e.g. discriminatory) decision-making.

To combat direct discrimination the regulation includes a prohibition to use data related to ethnicity and other sensitive data[64]. This rule is exceptionally lifted for the purposes of bias monitoring, detection, and correction but only in relation to high-risk systems[65]. Since bias identification often requires information related to special categories of personal data[66], this limitation restricts the capacity of AI providers to eliminate and prevent biases in AI systems not categorized as high-risk[67]. The impossibility to identify and remove bias can perpetuate discrimination. Tracing algorithmic discrimination or underrepresentation in datasets that amplify harmful

62. R. Xenidis, L. Senden, *EU non-discrimination law in the era of artificial intelligence*, cit.
63. Article 15.
64. Article 9 GDPR.
65. Article 10(5).
66. M. Veale, R. Binns, *Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data*, in *Big Data & Society*, 2017.
67. M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, in *Computer Law Review International*, 2021, 97-112.

stereotypes, racism and objectification is indeed an important tool to mitigate intersectional discrimination[68].

The latest text of the proposal adds to the list of measures of data governance for AI systems the examination of biases that lead to discrimination prohibited under EU law. Here, the text refers explicitly to feedback loops where the algorithm's outputs are cyclically fed back as inputs[69], and adds 'appropriate measures to detect, prevent and mitigate possible biases' to the list of measures of data governance[70]. While positive, these evolutions may still be insufficient. On the one hand, these quality criteria are applicable only to high-risk systems. Moreover, bias identification is not enough to combat discrimination, since (discriminatory) machine learning algorithms may be built not only on sensitive data but also on statistical inferences relying on discriminatory correlations[71].

The specific transparency and provision of obligations, contained in Article 13, also point in the right direction but are also problematic. Both developers and users of AI systems ought to possess the capacity to elucidate the reasoning and methodology behind decisions made, substantiated with corroborative evidence to the greatest extent feasible. However, the effectiveness of transparency requirements, and the essential requirements in their entirety, have been called into question as an analysis of its application revealed significant drawbacks in terms of the AI Act's interplay with national legislation, the problem of transplanting a regulatory approach initially designed for product safety regulation, and enforcement deficiencies[72].

IV. GOVERNANCE CHALLENGES AND THE RIGHTS-BASED APPROACH AS AN ALTERNATIVE

To conclude, we summarize some of the govervance challenges that the model in AI act presents in relation to non-discrimination and how a rights-based approach could present a meaningful alternative.

First, a self-assessment risk-based approach relying on harmonized standards is not suitable for protecting fundamental rights. Self-assessment

68. R. Xenidis, *Tuning EU equality law to algorithmic discrimination: Three pathways to resilience*, in *Maastricht Journal of European and Comparative Law*, 2020, 736-758.
69. Article 10(2) lef f.
70. Article 10(2) lef f) a.
71. *Ibidem*.
72. M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, cit.

of operational risks is a convenient tool where the assessment does not involve an analysis of interference(s) with human rights, which could lead to requirements that are in conflict with companies' interests (eg. sacrificing the use of correlations which increase the predictive value of an algorithm but has discriminatory impact on segments of the population). Moreover, it is expected that conformity assessments for compliance with the AI Act provisions will be based on harmonised standards[73]. These standards, developed by private standard-developing organizations, will contain the technical specifications for complying with essential requirements outlined in the legislation[74]. including those aimed at preventing and mitigating discriminatory biases by high-risks AI systems. This means that the way in which bias identification and the definition of what constitutes a risk of discrimination will in the end depend on the interpretation of a private, less democratically accountable body[75]. The delegation of rulemaking power to standard-setting bodies has raised general legitimacy concerns[76]. In the case of AI, it is accepted that important normative decisions will be made by different governance actors, but these should all form part of a legitimate and democratic political processes[77]. Yet, participation of stakeholders in standardization has been often been considered rather limited[78]. Accordingly, the shortcomings resulting from the risk-based approach has led civil society to call for its reconsideration, advocating instead for a *rights-based approach* that would require human rights impact assessments and provide actionable remedies to users[79].

And second, the issue of an enforceable rights approach vs systemic privatized enforcement. The proposed AI act also raises important problems associated with its enforcement regime and whether it is indeed appropriate and sufficient for addressing algorithmic discrimination[80]. In this regard, it can be argued that the AI Act's enforcement system is complex and problematic. It involves several actors such as certification bodies and market surveillance

73. Article 40 AI Act.
74. M. Cantero Gamito, C. Marsden, *AI co-regulation* (forthcoming).
75. M. Cantero Gamito, *The role of ETSI…* (forthcoming).
76. M. Eliantonio, C. Cauffman (eds.), *The legitimacy of standardisation as a regulatory technique: A cross-disciplinary and multi-level analysis*, Edward Elgar Publishing, 2020.
77. C. Orwat, J. Bareis, A. Folberth, J. Jahnel, C. Wadephul, *Normative Challenges of Risk Regulation of Artificial Intelligence and Automated Decision-Making*, 2022.
78. BEUC and ANEC report. See also P. Larouche, J. Baron, *The European Standardisation System at a Crossroads*, 2023. Available at SSRN.
79. Access Now, *The EU should regulate AI on the basis of rights, not risks*. Available at *https://www.accessnow.org/eu-regulation-ai-risk-based-approach/*.
80. R. Xenidis, L. Senden, *EU non-discrimination law in the era of artificial intelligence*, cit.

authorities to monitor the market, a model that is borrowed from product regulation. However, only the requirements imposed on high-risk AI systems are subject to market surveillance, conformity assessment and accreditation[81]. Moreover, the AI Act does not provide sufficient enforcement mechanisms against rights' violations[82]. For example, individuals cannot directly seek judicial redress in case of infringement(s) of fundamental rights. Therefore, users will have to resort to the mechanisms available under national tort[83] and antidiscrimination law[84]. At the same time, the enforcement of the AI

81. M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence* Act, cit.
82. *Ibidem*.
83. P. Verbruggen, *Good governance of private standardization and the role of tort law*, in *European Review of Private Law*, 27(2), 2019.
84. Different authors have discussed the potential of EU antidiscrimination law, as framed in primary and secondary legislation, to combat algorithmic discrimination. All in all, while this body of law and its national incorporation offer important tools, several shortcomings have been rightly highlighted in terms of protected grounds and domains of application, as well as in terms of the conceptual and doctrinal categories developed around this body of law. As to the former, they include the lack of protection, in secondary legislation, against discrimination based on age, disability, sexual orientation and religion or belief in the area of goods and services and the exceptions in the Gender Goods and Services Directive (2004/113/EC) in relation to the media advertising and education. As for the conceptual and doctrinal categories of EU non-discrimination law, Gerard and Xenidis have argued that proxy discrimination questions the boundaries of the exhaustive list of protected grounds defined in Article 19 TFEU and requires that a new light be shed on the role of the non-exhaustive list of protected grounds under Article 21 of the EU Charter of Fundamental Rights. Moreover, algorithmic profiling based on granular analysis of personal behavior and data entails heightened risk of intersectional discrimination, beyond what the Court of Justice has recognized so far. Finally, the authors have argued that algorithmic discrimination challenges the standard doctrinal paradigms of both EU and national anti-discrimination law by blurring the frontiers between direct and indirect discrimination given that -due to the difficulty in tracking differential treatment in "black box" algorithms-, indirect discrimination might become a "conceptual refuge" that allows for the more simple assessment of discriminatory outcomes. The problem, however, is that this might reduce legal certainty if it leads to the generalization of the open-ended objective justification test (which is applicable in indirect discrimination) and also, as Hacker has argued, that this test might in fact be relatively easy to overcome when companies show that, to extent that it relies in "statistical truth", the system of correlations used by the algorithm optimizes its function (for instance, in terms of predictive value), even if it perpetuates bias and stereotypes. See the report on *Algorithmic discrimination in Europe: Challenges and opportunities for gender equality a non-discrimination law*, by Janneke Gerard and Raphaële Xenidis, European Commission, 2020 and P. Hacker, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination Under EU Law*, in *Common Market Law Review*, 2018, 1143-1186. The latter argues that, to overcome some of these and other shortcomings, anti-discrimination law should be combined with algorithmic audits and data protection impact assessments in an effort to unlock the algorithmic black box.

Act, a maximum harmonization instrument (EU Regulation), may in fact pre-empt the application of conflicting rules under domestic law which might potentially be more protective vis-à-vis victims of discrimination.

V. CONCLUSION

AI and algorithmic decision-making become deeply intertwined with social norms, challenging our established understanding of discrimination. The evolving landscape of AI reveals the complexities of algorithmic discrimination, pushing the boundaries of traditional legal paradigms. With AI's unparalleled capability to process vast datasets and create patterns, the risk of inadvertently perpetuating and amplifying social biases has grown exponentially. Viewed in this context, the EU's anticipated AI Act is a creditable step towards addressing these emergent challenges. It aims to safeguard fundamental rights in the face of rapidly advancing technology, including by mitigating biases in algorithmic operations that lead to unacceptable discriminatory practices. However, the line between normal algorithmic operations and unlawful discrimination is often blurred. As discussed, while the AI Act seeks to provide a comprehensive legal framework, it inevitably struggles with the nuances of algorithmic biases and the multifaceted nature of discrimination in the age of AI.

The chapter has identified existing challenges in the current configuration of the legislative initiative with significant implications for the purpose of combating discrimination. The AI Act's risk-based approach raises inherent concerns. Limiting certain conditions to high-risks systems which are to be self-identified and entrusting the complexities of human rights protection to private standard-developing organizations places a critical societal decision-making process into the hands of regulatory actors that might lack the accountability and transparency of more democratic and accountable bodies. The decision to allow private entities to determine the standards for bias identification and the delineation of discriminatory risks is, at best, a contentious move. The potential for these bodies to make determinations that affect society's moral fabric underscores the importance of fostering a more robust governance system to ensure broad stakeholder participation, transparency, and oversight in the standard-setting process. The call from civil society for a shift towards a rights-based approach, emphasizing comprehensive human rights impact assessments and actionable remedies for users, further increases the concerns over the current trajectory of the AI Act.

Digitized information and information sustainability

[1]Matteo Caldironi*

SUMMARY: I. THE DIGITAL ECOSYSTEM: AN INTRODUCTION - II. THE PROBLEM OF PLURALISM OF INFORMATION ONLINE - III. INFODEMIA - IV. INFORMATION SUSTAINABILITY - V. SOME CONCLUDING REMARKS

ABSTRACT: The essay addresses some of the issues inherent in online misinformation through social networks, which were particularly noted in the years of the Covid-19 pandemic. In this analysis, the paper delves into the main risks of the so-called digital greenhouse effect but also identifies some possible solutions that can be put in place to minimize these problems.

KEYWORDS: Digital ecosystem; Digital greenhouse effect; Information sustainability; Infodemia.

I. THE DIGITAL ECOSYSTEM: AN INTRODUCTION[2]

Digitized information passes mainly through social networks[1] that collect their users' preferences, and then follow an activity of profiling. In this way, social networks are able to offer a service related to the preferences of each subject. This mechanism favors the birth of echo chambers: environments where there is no confrontation with those who think differently, but where, on the contrary, they reinforce each other's positions, possibly radicalizing

* Research fellow, University of Modena and Reggio Emilia.

1. L. Solima, *Social Networks: verso un nuovo paradigma per la valorizzazione della domanda culturale*, in *Sinergie*, 2010, 48.

them. All this happens through a mechanism defined as *confirmation bias*[2], which indicates the tendency to selectively expose ourselves to content that is in line with our system of beliefs and preconceptions, thus seeking confirmation of our prejudices.

In this scenario, a particularly relevant role has been assumed by *fake news*[3], which, we can define as deliberately false and biased news, devoid of interest and social utility[4]. Naturally, the diffusion of false news was not born with the development of the web. However, this phenomenon has increased exponentially in recent years, in particular through social networks. These have allowed subjects who, according to the traditional scheme of the informative relationship, would have been mere users of information, to contribute personally to their production and dissemination[5].

More generally, the phenomenon of fake news can be included in the dynamics of what has been defined as *information disorder*. This phenomenon includes the diffusion of news, not necessarily false, through modalities suitable to pollute the information ecosystem. This concept includes three fundamental types: i) *disinformation*: the content of the news spread is intentionally false and transmitted ad hoc to cause harmful consequences; ii) *misinformation*: fragments of false content are accidentally spread by unaware users, real vectors, convinced to disclose valid and useful content; iii) *malinformation*: true information shared with the intent to create adverse consequences[6]. Some come to identify this element as consubstantial to the

2. Peter Wason, cognitive psychologist at *University College* London and pioneer of the psychology of reasoning.

3. The two dimensions on the basis of which it is possible to classify fake news are: 1) the level of factuality (*facticity*), *i.e.* the conformity of the news to the real facts, and 2) the level of intentionality (*deception*), consisting of the percentage of falsehood voluntarily introduced by the author. Depending on the combination of the above attributes, it is possible to classify information disorders. By way of example, a low level of factuality and a high level of intentionality make up those contents that do not have any real feedback, but that are built as if they were *news in* order to legitimize them: this is the information that is labeled as *fake news* in the strict sense, *i.e.* contents without adherence to reality (R. Bracciale, F. Grisolia, *Information Disorder: acceleratori tecnologici e dinamiche sociali*, in *federalismi.it*, 2020, 61).

4. A. Candido, *Libertà di informazione e democrazia ai tempi delle fake news*, in *federalismi.it*, 2020, 106.

5. M. Cavino, *Il triceratopo di Spielberg. Fake news, diritto e politica*, in *federalismi.it*, 2020, 36.

6. Claire Wardle, executive director of *First Draft,* and Hossein Derakhshan, Iranian blogger, in the 2017 *report* for the Council of Europe (CoE).

definition of fake news, and suitable to differentiate it from the fake news that also previously was (in other forms) produced and spread.

The phenomenon of *information disorder* is closely linked to another aspect that characterizes our information system today: the decentralization of information.

The production of information on the web can be considered strongly decentralized since anyone can create and spread news on the web. Moreover, it can be considered strongly "disintermediated"[7] as it is the users themselves who circulate information without the professional filter constituted by the journalistic profession. "Thanks to social media everyone can be his own media, because the media have become a Network of which everyone is part and on which everyone can publish, share, interact, express positive or negative feelings"[8]. The combined action of various elements of a technological nature (e.g., smartphones and social media apps) allows access to any type of information content (but also its *creation*) without recourse to forms of intermediation.

However, the "distribution" of information is strongly centralized as it is managed by a few "intermediaries": the internet service providers who provide users with the internet platforms through which information can pass. Although they were created with the purpose of providing access to the main electronic communication networks and to allow the passive diffusion of contents, providers have, with time, changed their function. They have abandoned, little by little, their role of "neutral intermediaries" in favor of a more active role, which is substantiated in the concrete intervention on the contents published by users to increase their visibility, increase the potential of interaction and allow them greater possibilities of diffusion. Today, in fact, they "select" the information to be proposed to individual users through the use of algorithms capable of adapting them to the preferences expressed, explicitly or implicitly, on the web. This is a "profiled" informative offer, in the sense that it does not select the most reliable and trustworthy news,

7. The concept of 'disintermediation' is perhaps one of the most interesting novelties of our contemporary times, and in fact concerns various aspects of everyone's life. Of course, here we are dealing only with what concerns information, but this phenomenon touches also other areas such as, among others, economy and politics. For example, through some political platforms, such as "*Rousseau*", the intermediation of the parliamentarian between the electoral body and the institutions of the state is no longer necessary.

8. G.L. Conti, *Manifestazione del pensiero attraverso la rete e trasformazione della libertà di espressione: c'è ancora da ballare per strada?*, in *Rivista AIC*, no. 4/2018, 205.

but aims to select news according to preferences and opinions[9], almost as if he were locked inside a bubble[10]. In fact, these "filtering bubbles" reduce the possibility that the individual user comes into contact with differing information, thus strengthening their ideas and "prejudices" due to the *echo chamber effect*[11]. In this way, algorithms have a concrete influence on online misinformation by implementing the dissemination of news and information on the basis of parameters other than truth or correctness, and rather based on their ability to confirm prejudices already present in society[12].

In this system, the U.S. principle of the information "market" as a *free marketplace of ideas*[13] goes into crisis for at least two reasons. First of all, the individual user is now hindered by the in-depth analysis of individual information, as well as by the verification of the reliability of sources, due to the amount of news he receives daily and the process through which information is shared that often "hides" the primary source. This differs from traditional media because the number of editors, as well as the information they can give, are limited. In other words, the flow of information published on the web makes it very complex, if not substantially impossible, for the user to carry out the necessary checks to ascertain the reliability and truthfulness of the news. Secondly, the algorithms used by search engines and social networks can place inaccurate and unsubstantiated news at the top of the displayed news only because it is in line with the user's thinking, which decreases the likelihood that the user will proceed to the above checks.

9. G.A. VELTRI, *La tempesta perfetta: social media, fake news e la razionalità limitata del cittadino*, in *Media Education*, 2018, 47.
10. The term was first used in E. Pariser, *Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, London, Penguin, 2011.
11. G. Avanzini, G. Matucci (eds.), *L'informazione e le sue regole. Libertà, pluralismo e trasparenza*, Napoli, Editoriale Scientifica, 2016, 254.
12. G. Marchetti, *Le fake news e il ruolo degli algoritmi*, in *MediaLaws*, 2020, 31-32.
13. This expression was used for the first time by the judge of the Supreme Court of the United States, William O. Douglas, in the decision of the case *United States v. Rumely* in 1953 and became frequent. However, it has much deeper roots: the authorship of the expression 'marketplace of ideas' is acknowledged to Supreme Court Justice Oliver Wendell Holmes, employed in a dissenting opinion in *Abrams v. United States* in 1919. The metaphor, commonly used to recall the dynamics and functioning of markets according to neoclassical economics, is applied to the world of information and communication.

II. THE PROBLEM OF PLURALISM OF INFORMATION ONLINE

A well-known aphorism of E.A. Poe said: "the enormous multiplication of books in any field of knowledge is one of the great evils of this time, since it represents one of the most serious obstacles to the acquisition of correct information and throws in the reader's face heaps of junk in which he has to search with painful groping for fragments of useful material". And if it might have seemed provocative at the time, today it seems to capture exactly the information paradox in which we find ourselves: the overabundance of information sources is not a guarantee of a correctly informed citizen, but on the contrary, risks being the source of their ignorance. This is because the web has certainly facilitated and contributed to a diffusion of information unknown before. At the same time, the web user, left without the tools to understand the algorithmic mechanisms at its base, is led to privilege sources that confirm their prejudices.

To better understand these dynamics, however, it is necessary to see, albeit in summary, the fundamental steps that allow gatekeepers to arrive at the personalization of online information.

The first phase is the collection of data that concerns users. This happens in the context of activities carried out by users in a computerized context. User activities, both online and offline, can generate large amounts of data[14]. Online services, in particular social networks, are an almost inexhaustible source of data[15]. Added to this is the collection of data generated by the functionality of users' personal devices, such as smartphones. Activities performed by users, even in the absence of direct interaction with an electronic device, generate offline data and can provide relevant information about individuals' behaviors and preferences[16].

14. Agcom, Agcm, Garante Privacy, *Indagine conoscitiva sui Big Data*, Rome, February 10, 2020, 10 (resolution no. 217/17/CONS).
15. See already in this regard, on the protection of personal data, the *caveats* contained in WP 148 Opinion 1/2008 of the Art. 29 on data protection aspects related to search engines, adopted on 4 April 2008, passim, even though the document was not expressly dedicated to the topic of big data; not differently, also in relation to the data processing permitted by the collection carried out by means of cookies, in order for the processing to be considered legitimate, the conditions set out in the judgment of the Court of Justice (Grand Chamber) of 1 October 2019, Case C- 673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v. Planet49 GmbH.*
16. Agcom, Agcm, Garante privacy, *Indagine conoscitiva sui Big Data*, cit., 11.

Then comes the real data analysis, which takes place through tools capable of transforming unstructured data into information susceptible to practical use[17].

The third phase is what we have so far called *profiling of users*. It consists of "any form of automated processing of personal data consisting in the use of such data to evaluate certain personal aspects relating to the natural person, in particular to analyze or predict aspects concerning the professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements of that natural person"[18]. With the activity of profiling, users are grouped in also defined as 'social silos', in such a way as to be able to address to them, more easily, announcements and advertisements[19].

Due to the continuous development and improvement of the mechanisms used by the algorithms, the hypothesis of N. Negroponte has become reality. As early as in 1995, he coined the expression *Daily Me* to describe a virtual newspaper tailor-made for each individual: an informative world in which only the news that the user wants to receive and hear is broadcast[20]. And this is what happens today with the use of social networks. So, the world we see represented by digital platforms, the world that is actually built in front of us, is nothing more than the mere result of what we have previously done on these platforms[21].

In 2011 E. Parier, in his *The filter bubble. What the Internet is hiding from you*, grasped what was happening in the world of the web: algorithms filter information and news coming from the outside world and project only those contents that consistently reflect their vision of reality. Therefore, the information received by the user is nothing more than an echo of the opinions, beliefs, tastes that he has expressed[22]. A first consequence of the effects of profiling and the preventive selection of the information offer on the pluralism of information sources is certainly the creation of *filter*

17. *Ibid.*
18. Guidance on Automated Decision Making Regarding Individuals and Profiling for the Purposes of Regulation 2016/679, adopted October 3, 2017, Amended Version and adopted February 6, 2018, 7.
19. G. Riva, *Fake news,* Bologna, il Mulino, 2018, 113.
20. F. Bridle, *The bespoke newspaper - will the Daily Me soon be delivered?,* in *The Guardian*, 13 July 2014.
21. E. Garzonio, *L'algoritmo trasparente: obiettivi ed implicazioni della riforma dello Spazio digitale europeo*, in *Riv. italiana di Informatica e Diritto*, 2021, 2.
22. A. Vernice, *Il letto di Procuste dei sistemi informativi via Web: un pluralismo falsato?,* in *Riv. italiana di Informatica e Diritto*, 2021, 97.

bubbles that enclose each user by selecting the contents of the network most similar to him. This seems to highlight a paradox: as much as we consider ourselves absolutely free to choose between different alternatives that the web provides us, on the contrary, we risk being trapped inside filter bubbles that obscure our view of everything else that the web could offer us[23].

Relative to what has been said, two issues can be highlighted that concern cognitive processes and information assimilation by users.

The first, already mentioned, consists of the confirmation bias, a cognitive shortcut the individual runs after when gathering and interpreting information[24].

The second problematic element accentuated by the mechanisms of online information is the *Dunning-Kruger* effect: a cognitive distortion that leads a subject, not fully competent in a particular topic, to draw wrong conclusions on delicate and complex issues without really realizing it. These issues, which exist regardless of whether or not the Internet is used, are accentuated by the automated mechanisms that social networks use[25] that, then, "instead of connecting individuals with different points of view and ideologies, [...] tend to strengthen prejudices, due to the echo chamber effect, i.e. the tendency of information to bounce within closed systems"[26]. The effect is that of *cyber cascades* or *group polarization*, natural and spontaneous within any social formation characterized by homophily – human propensity to establish links on the basis of affinity with similar individuals – but, within the social network can feed itself algorithmically[27]. Within the echo chambers, the opinions expressed are not only confirmed, but they are amplified immensely, becoming radical and extreme. According to the theory of the *two-step flow of communication*, the group and the *opinion leaders* within it are not only able to reinforce the approximate opinions of the individual, but also to exaggerate them[28]. Thus, "echo chambers amplify original conformism, depriving it of plurality that deviates from the homogeneous standard and undermining the pluralism of opinions, ideas and alternative

23. M. Bianca, *La filter bubble e il problema dell'identità digitale*, in *MediaLaws*, 2019, 44.
24. R. De Cicco, *Il bias della conferma: l'autoinganno che limita le nostre decisioni*, in *Riv. Economica comportamentale*, 2020, 1.
25. R. Montaldo, *La tutela del pluralismo informativo nelle piattaforme online*, cit., 226.
26. G. Avanzini, G. Matucci (eds.), *L'informazione e le sue regole. Libertà, pluralismo e trasparenza*, Napoli, Editoriale Scientifica, 2016, 254.
27. R. Bracciale, *Information Disorder: acceleratori tecnologici e dinamiche sociali*, in *federalismi.it*, 2020, 65.
28. R. Montaldo, *La tutela del pluralismo informativo nelle piattaforme online*, cit., 227.

visions, in the configuration of watertight bulkheads islands, detached from any crossbreeding contamination, with a multiplying effect of prejudices in search of confirmation"[29]. The echo chambers are, therefore, real digital greenhouses that, as a whole, contribute to creating a real greenhouse effect of the digital ecosystem, in which the user unconsciously becomes the source of his own information.

All this greatly increases the diffusion and capillarity of fake news. In fact, users are inclined to believe in fake news if it is consistent and conforms to their own and reflects their way of thinking; but also because they prefer to consider as true what is in line with their own opinions, thus remaining imprisoned within a bubble and encountering only a group of individuals who think in the same way and who do not question the truthfulness[30].

So, the "greenhouse gas" of misinformation bounces back into the echo chamber, trapping itself in the filter bubble layer that users themselves unwittingly create.

In light of what has been said above, it is possible to affirm that algorithms have a strong impact on online disinformation and the process of formation of public opinion, affecting the real pluralism of information. Through the application of algorithms, it becomes increasingly easy not only to orientate the different opinions of users but also to "manipulate" them, undermining the formation of public opinion on issues of particular relevance, including, most recently, health[31].

III. INFODEMIA

During the pandemic, scientific communication has also had to deal with the reactivity of social networks and, in particular, with the virality

29. S. Vaccaro, *Gli algoritmi della politica*, Milan, Elèuthera, 2020, 114.
30. G. Marchetti, *Le fake news e il ruolo degli algoritmi*, cit., 31.
31. The European Commission document *Tackling online disinformation: a European Approach*, states that misinformation understood as false or misleading information, produced, presented and disseminated with an economic purpose or aimed at diverting public opinion, can cause a public threat ("*public harm*"). This entails a danger to democracy and political debate, which has an impact on public goods such as health, the environment and the security of EU citizens (Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Tackling online disinformation: a European Approach, Brussels, June 26, 2018, COM(2018) 236 final).

of fake news[32]. According to the World Health Organization, the global spread of the SARS-CoV-2 infection would represent not only the first case of pandemic of the last decade but also the first case of infodemic[33] intended as "circulation of an excessive amount of information, sometimes not screened with accuracy, which make it difficult to orientate on a particular topic because of the difficulty to identify reliable sources"[34].

In this regard, on March 19, 2020, the UN *Special Rapporteur* on the promotion and protection of the right to freedom of opinion and expression, the OSCE High Representative on Freedom of the Media, and the *Special Rapporteur* of the Inter-American Commission on Human Rights issued a joint statement, noting that "human health depends not only on readily accessible health care. It also depends on access to accurate information about the nature of the threats and the means to protect oneself, one's family, and one's community. The right to freedom of expression, which includes the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers, through any media, applies to everyone, everywhere, and may only be subject to narrow restrictions", recommending that "first, it is essential that governments provide truthful information about the nature of the threat posed by the coronavirus. Governments everywhere are obligated under human rights law to provide reliable information in accessible formats to all, with particular focus on ensuring access to information by those with limited internet access or where disability makes access challenging"[35].

On June 9, 2020, in Italy the Agcom[36] stressed the importance of preventing and contrasting the distorting effect of the phenomenon of online

32. A. Altinier, *I vaccini: la necessità di una comunicazione strategica per ricostruire un rapporto di fiducia con i cittadini e sconfiggere la deriva delle fake news*, in *Culture e Studi del Sociale*, 2018, 3(2), 213- 219.

33. "Disinformation in times of the coronavirus can kill. We have a duty to protect our citizens by making them aware of false information and expose the actors responsible for engaging in such practices. In today's technology-driven world, where warriors wield keyboards rather than swords and targeted influence operations and disinformation campaigns are a recognized weapon of state and non-state actors, the European Union is increasing its activities and capacities in this fight" (J. Borrell Fontelles, available at the link: *https://ec.europa.eu/commission/presscorner/detail/fr/speech_20_1036*).

34. *TreccaniOnline.*

35. *Covid-19: Governments must promote and protect access to and free flow of information during pandemic - International experts*, in *www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729&LangID=E.*

36. Agcom's first intervention occurred on March 18, 2020, with Resolution No. 129. The Authority established that "audiovisual and radio media service providers are invited to ensure adequate and complete information coverage on the subject of the *covid-19*

disinformation on pluralism and the correctness of information[37]. On June 10, 2020, the EU Commission also reiterated that misinformation can cause serious consequences, leading people to ignore official health protection claims and adopt risky behaviors, or negatively impacting democratic institutions, society, and the economy[38].

Obviously, not even the topic of vaccination has remained immune to misinformation and fake news. In fact, numerous studies have shown that the spread of fake news and misinformation on social media has been the primary cause of *vaccine hesitancy* which, according to the WHO, represents one of the ten most important threats to global health[39].

In a recent survey on vaccines against Covid-19 of August 2, 2021, it has emerged that the percentage of those opposed to vaccination is tenfold. And this is also due to the ways in which information on vaccines has circulated: on the one hand in a way that was not always clear and precise from official sources, and on the other hand often polluted by untrue, false, or biased news. In fact, in two special issues of the Observatory on online misinformation dedicated to the theme of the epidemiological emergency by Covid-19[40], Agcom published an analysis from which it emerged that

---

coronavirus, making every effort to ensure the testimony of authoritative experts from the world of science and medicine in order to provide citizens/users with verified and well-founded information". While, as far as *web* operators are concerned, it is provided that "providers of video-sharing platforms shall adopt all appropriate measures to counteract the dissemination online, and in particular on social media, of information related to the *coronavirus that is* incorrect or otherwise disseminated from sources that are not scientifically accredited. The aforementioned measures must also provide for effective systems for identifying and reporting offenses and their perpetrators" (Resolution no. 129/20/CONS, Act of warning on compliance with the principles in force to protect the fairness of information with reference to the topic "*Covid-19 coronavirus*", March 18, 2020, 5).

37. Agcom Hearing of June 9, 2020, cited above, 8.

38. Joint Communication from the European Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Countering Misinformation on Covid-19 - Looking at the Facts, Brussels, 10 June 2020, JOIN(2020) 8 final, 2.

39. WHO, *Ten threats to global health*, 2019, *www.who.int/news-room/spotlight/ten-threats-to-global-health-in-2019.*

40. The realization of the second issue of the Observatory has benefited from the collaboration of some members of the *Table Digital Platforms and Big Data - Covid-19 Emergency*, in particular *Auditel* (for the in-depth analysis on online videos), *Comscore* (for the international comparison), *Newsguard* (for fact-checking of the main false news spread around the world), *Sensemakers* (for analysis of social content) and Sogei (as regards computer attacks linked to the coronavirus), as well as the first elaborations

from February 21, 2020 to March 22, 2020, thirty-eight percent of the news published in the average day by sources of misinformation concerned the epidemic. The survey highlights the emergence of prevalent narratives about the epidemic, such as risks, conspiracy theories, and news reporting, hinged on communication based on the recurring use of terms designed to appeal to negative emotions rather than the moderation and truthfulness of the news[41].

IV. INFORMATION SUSTAINABILITY

Up to now, we have underlined the most problematic aspects related to the role that algorithms assume in the diffusion of online disinformation; however, they could also represent useful tools for *fact-checking*[42]. The issue is not easy to solve because there are critical issues related to their intrinsic structure and operation. In fact, algorithms are *indirect* systems for the evaluation of news content through the verification and analysis of elements belonging to the social platform through which the content has been conveyed and of the textual. Moreover, even algorithmic systems can be flawed, incomplete, or biased with the risk of acting with a procedure also based on biases predetermined from the beginning[43]. This could lead to a generalized censorship of news which, even if it is not actually fake news, is considered as such by the algorithms.

It must be taken into account that Internet Service Providers certainly do not act to protect the truthfulness of information but, rather, by evaluating the economic aspects connected to the display of news and the time spent on their Internet platforms. Platforms cannot be expected to spontaneously go against their own interests[44].

It might be useful, then, "to undertake co-regulatory 'disclosure' paths [...] on these algorithms. That is to say: in collaboration with other stakeholders (operators and users), it could be hypothesized to conduct experimental (behavioural) sessions to test the algorithms on a regular basis in order to identify those that reduce the risk of bias. Such a procedure, transparent and participatory, would increase the disclosure and accountability in the

carried out by the Data Science Task Force, activated by Agcom on the subject of online disinformation during the Covid-19 emergency.

41. Agcom, Hearing of June 9, 2020, cited above, 16.
42. Verification of facts and sources to assess the validity of news or statements of public importance.
43. G. Marchetti, *Le fake news e il ruolo degli algoritmi*, cit., 33.
44. *Ibidem*, 34.

use of these algorithms, [these are] characteristics that are currently lacking and clamored for by EU institutions"[45] . Therefore, "a greater disclosure on the use of algorithms that define the order of appearance of news on social networks could reduce the propagation of fake news because: (i) it would limit the impact of cognitive biases (especially *confirmation bias*) thanks to experimentation; (ii) it would not imply any censorship of those who create fake news (subject to criminal and civil liability, if any); (iii) it would intervene at the moment of the spread of fake news (when implemented through botnets, fake accounts or artificial intelligence)"[46].

Another possibility, already tested by some subjects, including Facebook, is that of adopting a collaborative type of fact-checking[47]: a control, carried out by an open group of people, to ascertain and evaluate if a certain content is true[48]. The "human" report is filtered by an algorithm and shared in a partners-only dashboard, (a platform that can be consulted only by the platform and by fact-checking agencies). Subsequently, selected news stories are vetted by two of the five fact-checking agencies[49] participating in the partnership to determine their veracity[50].

More generally, it's a matter of imposing the presence of some reliable fact-checking mechanism by regulation, putting the costs on the platforms but not leaving the procedures and controls entirely up to them.

The importance of greater transparency of the operating mechanisms of the algorithms used to select news has also been the subject of European intervention. In fact, on January 12, 2018, the European Commission established the *High Level Expert Group on Fake News and Online Disinformation*: a task force composed of thirty-nine experts, including representatives of institutions, academia, and journalism, for the formation of a permanent comparison table with the task of studying the phenomenon of misinformation

45. F. Di Porto, *Fake news, una possibile soluzione: algoritmi più trasparenti*, in *Digital Agenda*, 2018, 6.
46. *Ibidem*, 8.
47. Ifcn has established a specific program, in relation to Covid-19, called the #*CoronaVirusFacts Alliance* that unites more than a hundred *fact-checkers around the* world on the publications, sharing and filtered facts hovering around the epidemic. The alliance was launched in January 2020, when the spread of the virus was still confined to China, but nonetheless was already causing global misinformation problems.
48. A. Russo, *Fake news ai tempi del Covid-19. L'uso del fact-checking per contrastare l'epidemia della disinformazione,* in *Riv. di Sociologia del Territorio, Turismo, Tecnologia*, 2020, 92.
49. *ABC News, Associated Press, FactCheck.org, PolitiFact, and Snopes.*
50. M. Monti, *Fact-checking partnership di Facebook: come funziona, pro e contro*, in *Agenda Digitale*, 2018, 2-3.

in order to limit it as much as possible[51]. Also in 2018, the EU Commission's Directorate-General for Communication Networks, Content and Technology, in coordination with the above-mentioned independent group of experts, produced a final report, entitled *European Approach to Countering Online Disinformation*, which identifies the most immediate and feasible solution: drafting a self-regulatory code in agreement with the most important internet platforms using a "self-regulatory approach based on a clearly defined multi-stakeholder engagement process"[52] and exclusively focused on combating the phenomenon of fake news[53]. *The Code of Practice on Disinformation* was published on September 26, 2019 and aims to achieve "from transparency in political advertising to the closure of fake accounts and demonetization of purveyors of disinformation"[54].

The Code brings together, on a voluntary basis, the most influential providers in the digital world and delegates to them the task of regulating and blocking misinformation by outlining a series of principles that can guide the action of these private entities in the fight against the widespread phenomenon of fake news. The Code also clarifies and redefines the notion of fake news: information that is "verifiably false or misleading information", adding that must be created and spread for economic reasons or to intentionally mislead readers and able to threat to political and democratic processes, as well as to prejudice public goods such as health, the environment or the safety of EU citizens. The notion of fake news, in addition to a positive connotation, is also clarified in the negative, excluding some content from the scope, due to the exceptional variety of online forms of expression: in fact, the notion in question does not include errors in the news, misleading advertising, satire, parody, communication and political propaganda[55].

The *Code of Practice* is a *soft law* instrument that "shall apply within the framework of existing laws of the EU and its Member States and must not be construed in any way as replacing or interpreting the existing legal

51. C. Magnani, *Libertà d'informazione online e fake news: vera emergenza? Appunti sul contrasto alla disinformazione tra legislatori statali e politiche europee*, in *Quaderni costituzionali*, 2019, 9.
52. Hleg, *A multi-dimensional approach to disinformation Report of the independent High Level Group on fake news and online disinformation*, 2018, 6.
53. G. Pagano, *Il Code of Practice on Disinformation. Note sulla natura giuridica di un atto misto di autoregolazione*, in *federalismi.it,* 2019, 5.
54. European Commission, *Code of practice on disinformation*, September 26, 2018 (available at: *digital- strategy.ec.europa.eu/en/policies/code-practice-disinformation*).
55. M. Monti, *Il Code of Practice on Disinformation dell'UE: tentativi in fieri di contrasto alle fake news*, in *MediaLaws*, 2019, 320.

framework"[56]. The Code delegates the regulation and operations to counter the spread of online disinformation entirely to the digital platforms, leaving to them any kind of control on correctness and efficiency. However, the choice of relying *entirely* on Internet platforms seems to be criticized, as no guarantees seem to be provided regarding independence from political or ideological prejudices in identifying (a not very precise range of) illicit expressions.

In short, the Code confers to the signatory Internet platforms[57] a hetero-directed self-regulation aimed at making the network *bigwigs* responsible for the paradigm of freedom of expression and information. However, this empowerment assigns a para-constitutional role[58] to the digital platforms that become a real arbiter of conflicts between fundamental rights. The absence of regulation, an adequate regulatory framework, and a control by public authorities and judges paradoxically leaves wide discretionary spaces to private interests[59].

V. SOME CONCLUDING REMARKS

The *infodemic* has highlighted some of the criticalities of the current information ecosystem but, at the same time, has proved to be an opportunity for institutions to experiment with possible solutions in the fight against online disinformation, both at national and supranational level. The *Code of Practice on Disinformation*, the *Digital Services Act*, and *the European Democracy Action Plan* are just some of the examples of interventions that have been made to implement a plural and diverse information system, in other words, a more sustainable information transition. Fact-checking (including collaborative fact-checking) is undoubtedly one of the tools from which to start to empower citizens and provide them with the means to limit the risks of misinformation. It is not only a process of fact-checking, but a way to propose to them a more complete and verified way of informing themselves.

56. European Commission, *Code of practice on disinformation*, September 26, 2018, 2.
57. On October 16, 2016, the *Code of Practice on Disinformation* is signed by Facebook, Google, Twitter, Mozilla, associations representing online platforms (EDIMA), and associations representing the advertising industry and advertisers (EACA, IAB Europe, WFA and UBA).
58. Expression used in O. Pollicino, *Google rischia di "vestire" un ruolo para-costituzionale*, in *ilsole24ore.it*, September 24, 2019.
59. M. Monti, *La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea (Code of practice on disinformation)*, in *federalismi.it*, 2020, 294.

However, what seems equally evident is that the phenomenon of *information disorder* should not be tackled only through a technological approach nor can it be totally contracted out to the self-regulation of individual internet platforms[60]. The problem seems to have to be answered also from an educational point of view with respect to the behavior of individuals on the network[61]. Media literacy seems an essential element in limiting the effects of misinformation.

In order to improve the quality of an ecosystem, it is not enough to have new technologies or new regulatory limits. Obviously, the active participation of those who are part of that ecosystem is necessary. In an environmental ecosystem, it is not enough to guarantee biodiversity if certain practices are prohibited, because given the global dimensions of that reality, there will always be a way to escape the expected "repressive" response (or at least this could happen in a minority of cases, however sufficient to put at risk that balance). It will then be essential to properly educate citizens to recognize and avoid malpractice, thus limiting its spread. Remaining in this example: to stem the effects of the greenhouse effect, it is good that citizens are informed of what activities to avoid or limit in their daily lives, such as the use of cars or heating/air conditioning, the use of chemicals, etc.

The same seems to apply to limiting the effects of the digital greenhouse effect: citizens should be put in a position to know which practices to avoid and which to prefer. They should be educated on how to recognize news that has characteristics that make one doubt its veracity, on the importance of sources and their verifiability, and they should be informed by internet platforms on the functioning of the mechanisms behind the circulation of news. All this could only start in schools, where measures could be implemented to educate students from the very beginning to be more responsible users of the internet and *social media*. However, it seems legitimate to think that those most "at risk" are those other than the so-called digital natives, precisely because they are new to this reality. For this reason, it seems essential that the journalistic profession regains its fundamental role, also through public contribution, that it acts as a "counter-information" to the spread of fake news and, above all, that it stops chasing the *fast-news* model.

60. On April 4, 2020, the Undersecretary of State to the Presidency of the Council of Ministers, with a decree, established a *Monitoring Unit to counter the spread of fake news related to Covid-19 on the web and social networks*, equipped with tasks of evaluation and surveillance of information on the contagion and identification of the most appropriate measures, including through the involvement of the main social platforms, to counter the spread of fake news online.

61. G. Marchetti, *Le fake news e il ruolo degli algoritmi*, cit., 35.

A premise for digitisation: the Right To Internet Access

1Valentina Cavani*

SUMMARY: I. INTRODUCTION - II. THE NATURE OF THE RIGHT TO INTERNET ACCESS - III. INTERNET ACCESS IN THE CONSTITUTION: WHERE AND HOW - IV. INTERNET ACCESS IN THE ITALIAN DEBATE - V. INTERNET ACCESS IN CONSTITUTIONAL JURISPRUDENCE: A COMPARATIVE VIEW - VI. INTERNET ACCESS IN THE JURISPRUDENCE OF EUROPEAN COURT OF HUMAN RIGHTS - VII. THE INTERNET AND THE ITALIAN CONSTITUTIONAL COURT: A CALL WAITING FOR ANSWER - VIII. SOME CONCLUDING REMARKS

ABSTRACT: The aim of this paper is to provide an overview of the status of the right of Internet access, from a national and comparative perspective, with a focus on the role of constitutional courts in recognising this legal situation.

KEYWORDS: Internet access; new rights; digitalisation; digital divide.

I. INTRODUCTION

From a constitutionalist perspective, the topic discussed in this work, that of "digitalisation", offers much food for thought.

Today, most of our fundamental rights are exercised "through" the Internet or rather "in" the Internet. The Net has become a place (the "cyberspace") where individuals develop their personalities and interact with each other.

* PhD Student, University of Modena and Reggio Emilia.

For this reason, before any reflection on cyberspace can take place, it is necessary to tackle the issue of the possibility for individuals to have access to it.

The right to Internet access is now unanimously recognised as "an essential element" for the exercise of many rights[1]: today, in order to be citizens and exercise rights, to be able to relate with other citizens and with the State, it is necessary "to live" (also) on the Internet. "Digito ergo sum"[2]: in today's society, to access means to exist[3].

The debate on the right to Internet access began in the early 2000s; however, it was above all what happened during the pandemic that showed more clearly than ever the potential of the medium and, at the same time, the risks it poses in terms of social exclusion.

In the emergency period due to Covid-19, the infrastructural, technological, economic and cultural digital divide has led to the compression, or even the denial, of many fundamental rights, first and foremost that to the full development of the individual personality and to an effective participation in the political, economic and social organisation of the country (as recognised by Article 3 of the Italian Constitution)[4].

It is only a few days before the time of writing that a Slovak court ruled that the State must compensate a child who, during the long closure of school facilities due to Covid-19, was unable to participate in distance learning because of insufficient Internet access[5]. The court concluded that Slovakia had discriminated against access to education, information and freedom of expression "by failing to take appropriate measures to guarantee the applicant equal access to education during the pandemic"[6].

---

1. P. Passaglia, *La problematica definizione dell'accesso a Internet e le sue ricadute su esclusioni sociali e potenziali discriminazioni*, in *MediaLaws*, n. 3/2021, 127.
2. Z. Zencovich, *Perché occorre rifondare il significato della libertà di manifestazione del pensiero*, in *Percorsi costituzionali*, n. 1/2010, 74.
3. Several years ago, ours was called the "age of access": J. Rifkin, *L'era dell'accesso. La rivoluzione della new economy*, Milano, Mondadori, 2000.
4. M.R. Allegri, *Il diritto di accesso a Internet: profili costituzionali*, in *MediaLaws*, n. 1/2021, 59.
5. Prešov District Court, 6 November 2023: *https://poradna-prava.sk/wp-content/uploads/2023/11/rozsudok-OS-Presov_online-vyucovanie-_covid-anonym.pdf*.
6. The existential damage caused by the digital divide was already hypothesised by italian case law long before the pandemic: GdP Trieste, 30 luglio 2012, n. 587: D. Bianchi, *Il danno da "digital divide" nella giurisprudenza*, in *Ilsole24ore.com*, 27 September 2012.

In the Italian legal system, the debate on the nature of the right to Internet access and on its possible introduction into the constitutional text has been going on for decades. There have also been several constitutional bills aimed at amending (in different ways) the Italian Constitution.

On 12 October 2023, was presented in the Italian Senate the proposal for an *Annual Digital Law* (Ddl n. 908/2023) according to which "technology must unite, not divide" and, for this reason, "people and all European citizens must have access to Internet"[7].

In foreign legal systems, regulatory approaches to the right to Internet access are different. Some countries regulate it by ordinary legislation. Others have expressly constitutionalised it. Finally, in some countries, the right to Internet access has been recognised by constitutional courts.

The purpose of this paper is to provide an overview of the *status* of the right to Internet access, at national and international level, in order to reflect on the growing relevance of this subjective legal situation and the most appropriate ways to guarantee it.

II. THE NATURE OF THE RIGHT TO INTERNET ACCESS

Before entering into the comparative analysis, it is necessary to reflect on the legal nature of Internet access, asking ourselves whether it is to be considered a new fundamental right or (as has been hypothesised) a new human right[8] and whether, in any case, it can be considered an autonomous right or represents a prerequisite for the exercise of other rights.

With regard to international law, the United Nations published several reports referring to the Internet as a human right and promoting active intervention by public authorities to guarantee access to the Net for all.

The first example is provided by the *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* issued on 16 May 2011[9]. Paragraph 85 states that: "Given that the Internet

7. *file:///C:/Users/user/Downloads/senato-disegno-legge-908-2023%20pdf%20(1).pdf*.
8. On the distinction between 'human rights' and 'fundamental rights' and on bringing Internet access into one of these categories, see O. Pollicino, *Right to Internet Access: Quid Iuris?*, in A. von Arnauld, K. von der Decken, M. Susi (eds.), *The Cambridge Handbook on New Human Rights. Recognition, Novelty, Rhetoric*, Cambridge, CUP, 2019.
9. *Report on the promotion and protection of the right to freedom of opinion and expression*: *https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*.

has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States".

A similar approach is adopted by the Organisation for Security and Cooperation in Europe (OSCE), which, in a 2011 report, stressed that: "Everyone should have a right to participate in the information society and states have a responsibility to ensure citizens' access to the Internet is guaranteed"[10].

More recently, in the 2016 UNHR *Resolution on The Promotion, Protection and Enjoyment of Human Rights on the Internet*, access to the Net was identified as a means "to ensure the protection of freedom of expression, freedom of association, privacy and other human rights online"[11].

From the above examples, it seems possible to imply as, in international law, there is the tendency to look at Internet access not as an autonomous "new right" but as a part of a right to participation of all citizens in the information society that can be achieved by the possibility for the citizens to have access to the Internet.

Yet, even recently, the call to recognise Internet access as a human right has come from several authoritative voices.

In 2019, Professor M. Reglitz, the coordinator of a research project at the University of Birmingham, highlighted how the instrumentality of the Internet to the exercise of other rights relates to the *justification* for the recognition of the right of access, not to the *content* of the right, which is entirely "sui generis": "because it is not reducible to, or encompassed by, any other individual right. Internet access is not simply a version of other rights i.e. either free speech, or free assembly, or free information, although it does digitally enable access to these rights"[12].

This was most recently confirmed at the highest level of the European institutions, which, at a meeting on 28 October 2020 (sponsored by the then-President of the European Parliament David Sassoli, with the participation of European Commission President Ursula von der Leyen, Professor Romano

10. *Https://www.osce.org/files/f/documents/e/f/80723.pdf*.
11. *Official Documents System of the United Nations*: *https://documents-ddsny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement*.
12. M. Reglitz, *The Human Right to Free Internet Access*, in *Journal of Applied Philosophy*, 2020, 314-331.

Prodi, web inventor Sir Tim Berners-Lee and activist Simona Levi) spoke about Internet access as a "new human right"[13].

III. INTERNET ACCESS IN THE CONSTITUTION: WHERE AND HOW

Notwithstanding what has been said in the previous paragraph, it must be noted that, although the essentiality of the Internet in the lives of individuals is by now an undisputed fact, this instance finds only limited corroboration when we proceed to a comparative analysis focused on the sources that are, by tradition and structure, those deputed to affirm or ascertain the existence of rights: there are very few constitutions that explicitly take a position on the Internet.

In Europe, only the Greek Constitution, amended in 2001, recognises the right of all citizens to participate in the information society by producing, exchanging and disseminating information by electronic devices, as well as the State's obligation to make this right effective.

In other European countries, the right to Internet access is regulated by sub-constitutional legislation (France, Estonia, Finland, Spain) or is not regulated at all.

On a global level, the most recent constitutions have revealed a greater permeability to issues related to the impact of new technologies. It is common to find the Internet in the constitutions of Latin American countries, where the protection of Internet access is combined with the remedy of *habeas data*[14]. Among the Charters that contemplate, in various ways, Internet access: the 1992 Constitution of Paraguay; the 1999 Constitution of Brazil; the 2003 Constitution of Honduras; the 2003 Constitution of Venezuela; the 2008 Constitution of Ecuador; the Constitution of Mexico, as amended in 2013[15].

13. *https://www.senato.it/documenti/repository/commissioni/dirittiumani18.pdf*.
14. For an overview of this constitutional remedy see T.E. Frosini, *Il diritto costituzionale di accesso a internet*, in M. Pietrangelo (ed.), *Il diritto di accesso a internet*, Napoli, ESI, 2011, 23-43.
15. Art. 6(3) of Mexican Constitution explicitly qualifies the right to Internet access as a social right: "El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios". Particularly interesting is the Constitution of Aguascalientes, a small State in the Mexican Federation, which – in a context of particular attention to social evolution – expressly recognises the right to

IV. INTERNET ACCESS IN THE ITALIAN DEBATE

In Italy, the doctrinal debate on Internet access began in the second half of the 1990s and focused on whether this right should be included in the Constitution.

On this point, there are still two opposing theories.

According to the first orientation, which is opposed to the reform of the Charter, the constitutionally relevant aspects of Internet access are already included within the existing provisions. In this view, it is believed that Articles 2 and 3 of the Constitution can also be extended to the digital environment or, alternatively, that the right in question can be derived from a combined reading of Articles 15 and 21 of the Constitution.

In the opposite direction is the doctrine according to which only the presence of a constitutional provision can limit the discretion of the ordinary legislator along with that of private market operators.

However, even in this second perspective, there is no agreement on the legal qualification to be given to the right to access and on the place it should have in the constitutional text.

In the first instance, the possibility of access to the Net was examined in connection with the rights of expression and information, and was therefore qualified as a "negative freedom". This doctrine stems from the first elaborations on the relationship between Internet and law, which considered the Internet as a means of communication, intended mainly to allow the expression of opinions, the circulation of ideas and the right to information[16].

Emblematic, in this perspective, are the constitutional bills stemming from the original proposal of Article 21-bis presented in 2010 by Stefano Rodotà[17].

Internet access: "El Estado y los Municipios garantizarán el derecho de acceso libre a internet, para tal efecto, establecerán los mecanismos y políticas públicas necesarias para asegurar progresiva y de manera gradual la efectividad de este derecho" (art. 6). On this point, in detail, P. Passaglia, *Alcuni spunti di riflessione offerti dalla lettura della Costituzione dello Stato di Aguascalientes*, in *DPCE Online*, n. 3/2020, 3801-3811.

16. G. D'Ippolito, *Il diritto di accesso a internet in Italia: dal 21(-bis) al 34-bis*, in *MediaLaws*, n. 3/2021, 88.

17. On 29 November 2010, during the third Italian edition of the Internet Governance Forum, Rodotà proposed the inclusion in the Constitution of an Article 21-*bis* dedicated to Internet access: "Everyone has the equal right to access the Internet, on

Over time, this reconstruction has appeared increasingly reductive: the Internet has now emancipated itself from its misunderstood role as a means of communication to become a "dimension" in which the multiple dynamics of human existence unfold.

For the protection of this dimension, the "negative" negative obligation to refrain from arbitrary interferences and limitations is no longer adequate. Rather, what is needed is a constant maintenance of the minimum levels of the guarantee of access to the Internet, which thus acquires a "positive" content as a social right.

In this perspective, since 2014, Internet access has found a reference in the proposal to introduce an Article 34-bis[18], which qualifies the right of access as a "social right", i.e. as a subjective claim to public services that, like health and education, institutions must guarantee through state investments and social and educational policies.

The option of placing the Internet within that group of rights that the Constitution qualifies as "ethical and social relations" seems to be the most appropriate for several reasons. Firstly, a *sedes materiae* other than that of negative freedoms would reinforce the constitutional emancipation of the right to Internet access from the scope of freedom of expression[19]. Secondly, such a formula also shows its usefulness insofar as it does not merely identify the content of the right and the holder of it, but also makes explicit the subject charged with the guarantee and the modalities of intervention, protecting citizens from potential backtracking by public authorities[20].

---

equal terms, with technologically adequate modalities that remove all economic and social obstacles". This proposal aroused much interest and resulted in numerous bills proposing the introduction of either an Article 21-*bis* or a new paragraph of Article 21 of the Constitution.

18. The first bill was presented in the Italian Senate (Senate Act No. 1561 of 10 July 2014): "Introduzione dell'articolo 34-*bis* della Costituzione, recante disposizioni volte al riconoscimento del diritto di accesso a Internet". In 2015, the same proposal was presented in the Chamber of Deputies (Chamber Act No. 2816 of 14 January 2015): "Introduzione dell'articolo 34-*bis* della Costituzione, in materia di riconoscimento del diritto universale di accesso alla rete Internet". Finally, the proposal for Article 34-*bis* was also presented during the 18th Legislature (Chamber Act No. 1136 of 4 September 2018): "Introduzione dell'articolo 34-*bis* della Costituzione, in materia di riconoscimento del diritto sociale di accesso alla rete Internet".
19. O. Pollicino, *Right to Internet Access: Quid Iuris?*, cit.
20. G. De Minico, intervention at *Tavola Rotonda su Art. 34-bis*, Chamber of Deputies, 8 May 2015.

Although the solution offered by Article 34-bis seemed to be the landing place of the theory in favour of the constitutionalisation of the right of access, a recent legislative initiative has once again mixed up the planes of the qualification of the right and its systematic placement.

On 13 October 2022, in the Italian Chamber of Deputies, was presented the constitutional bill no. 327/2022, which, while configuring Internet access as a social right[21], places it within Article 21 of the Constitution, in a new paragraph[22].

It is evident how the placement of a right in the constitutional text does not constitute a mere formalistic issue, since this choice affects (or – from another perspective – depends on) the legal qualification attributed to it.

The Italian legal system is therefore experiencing a "stalemate" with regard to the right to Internet access: the doctrine has already written extensively about it; the legislator does not seem to want to deal with it; for its part, even the Constitutional Court does not seem to want to offer its contribution.

V. INTERNET ACCESS IN CONSTITUTIONAL JURISPRUDENCE: A COMPARATIVE VIEW

As mentioned, the right to Internet access has been the subject of some important rulings by the constitutional courts of other countries.

An overview of comparative law must start with the US Supreme Court, which was the first to pronounce (with the 1997 Reno v. American Civil Liberties Union decision[23]) on the relationship between Internet and freedom

21. "[...] understood as the claim of citizens against the State to cover the national territory with an adequate telecommunications infrastructure in order to exercise rights online, fulfil duties and benefit from public and private services".
22. According to the text of the Proposal, the placement of the new right within Article 21 of the Constitution is intended to "underline its importance in the context of the constitutional principles of equality, free construction of the personality and conscious participation in public debate".
23. *U.S. Supreme Court, 521 U.S. 844 (1997), Janet Reno, Attorney General of the United States, et. al. V. American Civil Liberties Union et. al., n. 96-511*. The decision is available online at: *https://supreme.justia.com/cases/federal/us/521/844/*; for an Italian translation of the opinion of the Court see R. Tarchi (ed.), *Corso di diritto comparato. Casi e materiali*, vol. I, Milano, Giuffrè, 1999, 203 ss.; a full translation of the judgment can be found in *Foro it.*, 1998, IV, 23 ss.; *ibidem* the comment by A. Cucinotta, *"Communications Decency Act" per indecenza ciberspazio*.

of expression, declaring the unconstitutionality of the provisions of the 1996 Communication Decency Act that restricted Internet access, because they conflicted with the freedom of speech guaranteed by the First Amendment of the US Constitution.

Although, as has been noted[24], the relevance of the decision with respect to the configuration of Internet access is rather limited, it has the undeniable merit of having raised new questions about the nature of the Net, recognising the dangerousness of limitations to access not only with reference to certain specific rights, but rather to the democratic principle itself[25].

Particularly interesting is the Court's evolutionary interpretation of the First Amendment, which, in the 20th century, protects not only the traditional freedom of expression but also the "digital" version of this right[26].

In the European context, the leading case is certainly the so-called Hadopi ruling, provided by the French Conseil constitutionnel on 10 June 2009[27].

This decision is part of a "traditional'" jurisprudential strand, i.e. that of a reaction by judges to a censorious regulation by the political decision-maker, in the absence of appropriate constitutional guarantees: the classic case is that of copyright infringement.

---

24. L. Cuocolo, *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in *Politica del Diritto*, n. 2-3/2012, 271 ss.
25. The District Court of Pennsylvania (from which the judgment originated) had already stated: "It is no exaggeration to conclude that the content on the Internet is as diverse as human thought". According to P. Passaglia, *Diritto di accesso a internet e giustizia costituzionale. Una (preliminare) indagine comparata*, in M. Pietrangelo (ed.), *Il diritto di accesso a internet*, cit., 64, in the meshes of the decision one can grasp a new qualification of the Internet, which, although belonging to the *genus* of the media, constitutes an entirely new *species*, since "it cannot be assimilated to any other existing means of communication". According to P. Costanzo, *I diritti nelle "maglie" della rete*, in L. Bruscuglia, R. Romboli (eds.), *Diritto pubblico e diritto privato nella rete delle nuove tecnologie*, Pisa, Plus, 2010, 10, "the same judgement [...] stands out for a series of luminous statements that have underlined the exceptional and unpredictable contribution made by the Internet to the free marketplace of ideas (according to the famous formula of Judge Holmes) and therefore the need to safeguard the spaces of freedom".
26. T.E. Frosini, *Il diritto costituzionale di accesso a internet*, cit., 37. It is also worth mentioning the Supreme Court's ruling in *Packingham v. North Carolina*, 19 June 2017, which, twenty years later, picks up the threads of the Reno ruling (quoting it several times) and takes stock of what the Internet has in the meantime become for American society.
27. *Conseil constitutionnel, déc. n. 2009-580 DC*, 10 june 2009. For an Italian translation see *Dir. informazione e informatica*, 2009, 524 ss.

In the French case, under scrutiny were the sanctioning powers that the *Création et Internet* law attributed to Hadopi (*Haute Autorité pour la diffusion des oeuvres et la protection des droits sur l'Internet*), the administrative authority in charge of monitoring the respect of copyright on the Net.

From a strictly legal point of view, the Court does not go so far as to recognise a real fundamental right of access to the Web; it does, however, define Internet access as a condition for ensuring freedom of expression as set out in Article 11 of the 1789 *Déclaration*, thus linking the Internet to the more "solemn" document of the so-called "bloc de constitutionnalité"[28].

From a comparative perspective, the pronouncement is relevant in several respects.

- First, it is striking to note the evolutionary interpretation adopted by the Conseil with respect to fundamental rights, which are able to adapt to changes in reality, almost in a "Darwinian sense"[29].

- Secondly, particularly interesting is the concept of "non-dénaturation" of the fundamental right that the Conseil adopted when it has to reconcile different and conflicting (fundamental) rights[30]. In the case at hand, the competence granted to an administrative, and therefore non-jurisdictional, authority to restrict or prevent access to the Internet is illegitimate, since freedom of expression – from which the right to Internet access derives – does not withstand such limitations, even when these are aimed at protecting other rights.

---

28. The close link between freedom of expression and Internet access was reaffirmed, more recently, by another important decision of the Conseil (no. 2016-611 QPC, 10 February 2017) concerning the constitutionality of a Criminal Code provision that penalised habitual consultation of terrorist sites; this ruling, in its reasoning, reproduces in full the statement of principle of the Hadopi judgment: "in the current state of the media, and having regard to the generalised development of online public communication services and the importance assumed by these services for participation in democratic life and for the expression of ideas and opinions, [the right to free communication] implies the freedom to access these services". Even more recently, it is worth mentioning decision no. 2020-801 DC, 18 June 2020, which, in declaring the unconstitutionality of a provision requiring service providers to remove illegal content, still reiterates the "mother-decision" of 2009: on this point, see P. Passaglia, *La problematica definizione dell'accesso a Internet*, cit., 126.
29. B. Carotti, *Comment* to *Conseil Constitutionnel, Décision 10 giugno 2009, n. 2009-580*, in *Giornale di diritto amministrativo*, n. 6/2010.
30. E. Stradella, *I diritti fondamentali nelle Corti. Primi spunti per una definizione della "fondamentalità" dei diritti nel diritto comparato*, in *Rivista "Gruppo di Pisa"*, 2016.

- Finally, the role of judges comes into the light. Their contribution is fundamental in defining the legal status of the Net. It is no coincidence that in November 2021, in the French legal system, was introduces a constitutional bill for the incorporation into the Constitution of Internet access, which precisely recalls the Hadopi ruling[31].

The most significant of the decisions on Internet access can be found across the ocean.

In 2010[32], the Costa Rica Sala constitucional – expressly recalling the decision of the French Conseil, in a "transnational dialogue between the Courts"[33] – recognised Internet access as a fundamental right, which public authorities have the task of ensuring, also in order to bridge the digital divide[34].

In doctrine, it has been correctly pointed out how, despite the reference[35], the access analysed by the Sala differs from that analysed by the Conseil:

31. Constitutional bill 10 November 2021 - *Introduction of a new paragraph to Article 1 of the Constitution*: "The law guarantees free, fair and universal access to open digital networks and the training of citizens in their use". It should be emphasised that, in France, the relationship between law, in particular constitutional law, and the digital (the so-called 'numérique') has been attracting the attention and reflection of institutions and scholars for more than twenty years now. Already in 2008, in fact, the Comité Veil, charged with reflecting on the revision of the Preamble of the 1958 Constitution, had posed the question of whether the Preamble should explicitly protect the digital environment. Also interesting on this point are the two annual studies that the French Conseil d'Etat has devoted to the subject: see Conseil d'Etat, *Etude annuelle 2014*, *Le numérique et les droits fondamentaux - Etude annuelle 2017*, *Puissance publique et plateformes numériques: accompagner l'"ubérisation"*, both available online.
32. *Sentencia* 30 July 2010, n. 12790.
33. G. De Vergottini, *Il dialogo transnazionale fra le Corti*, Napoli, Editoriale Scientifica, 2010.
34. Specifically, in this ruling, the Court upheld a *recurso de amparo* in which the plaintiff complained about the Government's failure to implement the obligation set forth in 2008 *Ley General de Telecomunicaciones* to make the telecommunications market competitive.
35. P. Passaglia observes how the inference that the Supreme Court of Costa Rica drew from the Conseil's decision regarding the fundamental character of the right to Internet access is "far from automatic", and that, indeed, even taking into account the context in which the French Court's decision intervened "would have been to be excluded" (see P. Passaglia, *La struttura delle decisioni dei giudici costituzionali: un confronto fra la tradizione di civil law e quella di common law*, in D. Dalfino (ed.), *Scritti dedicati a Maurizio Converso*, Roma, Roma Tre Press, 2016). According to the author, this example serves to testify how "where there is a lack of a common legal language and tradition, explicit reference to foreign law requires the constitutional judge to be brave: no matter how

the French court pronounced on the constitutional legitimacy of specific measures aimed at preventing the use of the Net, whereas the Sala reasoned on the generic possibility of individuals to access the Net. Moreover, the Sala ruled on the infrastructural component of the digital divide, while the Conseil's ruling addressed the gap resulting from regulatory instruments that may prevent, by way of sanction, access to the Internet.

In any case, the Costa Rican decision has the merit of having framed the role of the Internet not so much as a mere means of communication, but as a dimension for the development individuals personality, thus providing a vision of the Internet closely linked to the personalist principle.

VI. INTERNET ACCESS IN THE JURISPRUDENCE OF EUROPEAN COURT OF HUMAN RIGHTS

The interpretation of Internet access provided by the Hadopi decision – as a negative freedom, instrumental to the exercise of other fundamental rights – is also confirmed by the case law of the European Court of Human Rights.

Leaving aside the (large part of) cases in which the Court has ruled on issues related to the inhibition of access in specific cases, the most relevant rulings are those that have concerned Internet access in general and, specifically, Internet access limitations imposed on prisoners.

The issue is interesting because, in the case of individuals in detention, the Internet represent an instrument not only for social inclusion, but also for the realisation of the re-educative purpose of punishment. Exclusion from the Net, in this case, leads to a digital divide that is not "de facto" but "de jure"[36].

The first judgment that deserves to be analysed is the case Ramanaz Demir v. Turkey, of 9 February 2021, concerning a Turkish prisoner's request to have access to the Internet in order to follow, as a lawyer, his clients and prepare his defence; a request that had been rejected by the national authorities. In this case, the European Court of Human Rights – defining the Internet as a "public service" essential for the exercise of other human rights – declared

---

thorough the research may have been, the risk of incurring errors or inaccuracies cannot be avoided".

36. It can be debated whether Internet rights should be restricted as a consequence of certain offences. However, the case where there is a ban on access to the Internet is very different. We can discuss the limitation of rights on the Internet only if access to the Internet is allowed.

the national court's refusal unlawful and linked the right of access to Article 10 of the ECHR, which guarantees freedom of expression, in all its forms[37].

The 2021 judgment, moreover, recalls two relevant precedents (Kalda v. Estonia and Jankovskis v. Lithuania). In the first case (19 January 2016), the European Court addressed for the first time in its history the issue of the right to Internet access of prisoners (specifically, to gather information useful for the exercise of their right of defence), considering the limitation of this right unnecessary in a democratic society and therefore in violation of Article 10 ECHR. In the second case, of 17 January 2017, the Court states that, although access to the Internet cannot be considered a right guaranteed by the ECHR *ex se*, nevertheless, in the context of Article 10 of the Convention, the Internet may constitute a means of obtaining information that cannot otherwise be obtained, thus being worthy of legal protection, especially if the purpose pursued is related to educational and cultural needs.

VII. THE INTERNET AND THE ITALIAN CONSTITUTIONAL COURT: A CALL WAITING FOR ANSWER

The foreign decisions mentioned above qualify access to the Internet either as a mere development of freedom of expression or as prerequisite for the exercise of other rights.

As already pointed out, it is precisely on the legal qualification of Internet access and its autonomy with respect to other rights (especially that of the freedom of expression) that the Italian debate is at a standstill.

The Constitutional Court, for its part, has not so far contributed to providing definitive indications as to how Internet access should be considered.

In addition, the (few) circumstances in which the Constitutional Court has had the opportunity to express its opinion on issues related to the Net are all to be ascribed to the category of "missed opportunities"[38].

37. The referral of the matter to conventional protection is "obligatory", since the ECtHR can only pronounce on States' compliance with the rights enshrined in the 1950 European Convention and, consequently, can only interpret the right to Internet access in the light of the Convention.

38. It should be emphasised that most of the decisions were taken in the context of disputes between the State and Regions. Therefore, even when the issue concerned the Internet, the dimension of the protection of rights was placed in an ancillary position with respect to that of the allocation of power among the State and the Regions: see P. Passaglia, *Corte costituzionale e diritto dell'Internet*, cit.

An example is provided by the well-known decision no. 307 of 2004, in which the Court rejected as unfounded the questions raised by Emilia-Romagna Region in relation to State provisions that instituted financial aid for the purchase of PCs by young people or persons with certain income requirements.

On that occasion, the Court did not fully endorse the interpretative line proposed by the State's Attorney – for which access to information media was to be considered a social right – but rather linked the matter "to purposes of general interest, such as the development of culture as referred to in Article 9 of the Constitution".

Rather than a missed opportunity, it is perhaps more correct to speak of an opportunity only partially exploited. After making the connection between the development of "digital culture" and Article 9 of the Constitution, the Court did not complete its reasoning, failing to clarify the consequences that flow from the adopted value approach. In particular, the Court did not clarify whether and how the connection between Article 9 Const. and Internet can reverberate on the rights of the individual and, in particular, whether it is possible to configure a social right of access to the Internet anchored to the value of "digital culture".

More recently, there has been another occasion that authoritative doctrine has qualified as "not to be missed" by the Court[39].

In 2014, the Lazio Regional Administrative Court raised two questions of constitutional legitimacy concerning the ordinary rules allowing AGCOM to adopt a special injunction procedure to protect copyright on the Internet[40].

Although the questions raised by the Administrative Court allowed the judges to pronounce themselves "on the role and function of the Internet in the contemporary constitutional state"[41], the Court preferred to declare them inadmissible, without entering into the merits of the questions submitted to it.

In October 2022, the Italian Supreme Court made to the Constitutional Court another assist on the Internet[42].

39. P. Passaglia, *Corte costituzionale e diritto dell'Internet*, cit.
40. The provision (D.lgs. No. 70/2003) allows AGCOM to initiate a special injunction procedure aimed at forcing the service provider to remove "digital works" available on the Internet in breach of copyright law.
41. A. Morrone, *Internet come spazio pubblico costituzionale. Sulla costituzionalità delle norme a tutela del diritto d'autore deliberate dall'Agcom*, in *Federalismi.it*, n. 3/2014, 3.
42. Supreme Court, Referral Order no. 46076, 16 december 2021.

In this case, the subject of constitutional review was the preventive measure of the Questore's oral warning prohibiting the possession or use of any means of access to the Internet; a prohibition that would appear to be in conflict with the freedoms of communication (Art. 15 Const. and Art. 8 ECHR) and of expression (Art. 21 Const. and Art. 10 ECHR)[43].

Also in this case, the Court did not directly address the issue, declaring the measure illegitimate because it conflicted with the constitutional guarantees on communication (art. 15 Const.) and considering the questions "inherent to the alleged violation of the right to Internet access" to be absorbed.

VIII. SOME CONCLUDING REMARKS

In order to draw some initial conclusions on the *status* of the right to Internet access, it is useful to go back to the interpretation of Article 9 Const. provided by the Constitutional Court in the 2004 ruling as a norm that guarantees the development of "digital culture", a value to which constitutional dignity is thus acknowledged.

This "evolutionary" approach evokes the hermeneutic paths taken by the Court on the subject of environmental protection.

As is well known, the environment has recently been constitutionalised and, in this process of recognition at the highest level of the hierarchy of sources, a fundamental role has been played by the Constitutional Court, which have always made your own, valuable, contribution. As early as the second half of the 1980s, the Constitutional Court recognised the environment as a "primary" and "absolute" constitutional value (no. 151 of 1986, no. 641 of 1987) whose protection has a foundation other than that of the "mere" allocation of power among the State and the Regions (no. 407 of 2002).

The connection between Article 9 Const. and the Internet has also been emphasised by doctrine from a different perspective[44].

This provision, as is well known, is designed to protect the Nation's historical and artistic heritage, one of the aspects of what has been defined

43. In the referral order, the Supreme Court also recalls the case law of the Strasbourg Court mentioned above.

44. M. Rospi, *Il diritto "alla cultura", l'accesso ad Internet e la pubblica fruizione del patrimonio culturale ai tempi del Covid-19: Se non ora, quando?*, in *MediaLaws*, 15 july 2020.

as the "right to culture"[45], as the freedom of each individual to access culture, to make culture and to share their art and knowledge.

It is quite evident how today the access to (increasingly digitised) cultural heritage depends (also) on adequate access to the Net.

In order to effectively protect the right to culture, it is therefore necessary for public authorities, at all levels of government, to recognise the importance of digitisation of cultural heritage and to facilitate its access via the Internet.

Moreover, it should not be forgotten that the guarantees of Article 9 Const. are today also addressed to "future generations". And precisely to protect the latter, the European Union has launched the Next Generation EU programme, an instrument to rebuild Europe "from" and "for" the new generations, whose investments focus precisely on "green" and "digital".

The digital transition is also one of the so-called twin transitions (together with the environmental sustainability) that will characterise our country, and many others, in the coming years, and it is a constraint also posed by the Italy's National Recovery and Resilience Plan (NRRP).

From this perspective, the right of access can be considered as one of the main practical applications of the principle of solidarity (in its "digital" declination[46]), essential for the realisation of a European Union that matches the economic and political ambitions that not only the present, but also the future, imposes on it.

In order to guarantee an effective usability of the Net in the future, the right of access must not be resolved in a mere statement of principle, but implies (in the present) economic and material investments aimed at the creation of networks capable of satisfying, almost immediately, the demand for connectivity of those who will come after us[47].

The right to Internet access is thus placed at the crossroads between the rights of "new" generation and the rights of "the new" generations.

45. A. Pizzorusso, *Diritto della cultura e principi costituzionali*, in *Quad. cost.*, n. 2/2000. For an overview of the status of so-called "cultural rights" (including the "right to the Internet") see M. Carcione, *Diritti culturali: dalle convenzioni UNESCO all'ordinamento italiano*, in L. Zagato, M. Vecco (eds.), *Citizens of Europe, Culture e diritti*, Venezia, Edizioni Ca' Foscari, 2015, 357-380.

46. G. Scotti, *Alla ricerca di un nuovo costituzionalismo globale e digitale: il principio di solidarietà "digitale"*, in *Forum di Quad. Cost.*, n. 2/2021.

47. This refers to so-called 'scalable networks': P. Damiani, *Repubblica digitale, fallimenti di mercato e diritto di accesso a Internet delle generazioni future*, Pesaro, Edizioni Intra, 2023.

Digital Democracy. Risks and opportunities of the technological revolution: e-voting in the Italian and European context

1Carmine Andrea Trovato*

SUMMARY: I. E-VOTING: A DEFINITION - II. THE SPREAD OF E-VOTING IN EUROPE - III. ELECTRONIC VOTING IN ITALY - *III.1. The Italian experimentation of electronic voting - III.2. First practical cases - III.3. Digitisation of preliminary election procedures* - III.3.1. Electronic signature for referendums - III.3.1. Electronic signature for referendums - III.3.2. The appointment of list representatives - IV. THE ADVANTAGES OF ELECTRONIC VOTING - *IV.1. The simplicity of exercising one's right to vote - IV.2 The anti-abstentionist effect - IV.3. Savings* - V. WHAT RISKS? - VI. SOME PROPOSALS TO MITIGATE RISKS: COUNCIL OF EUROPE, EDPS AND ENISA OPINIONS - VII. CONCLUSIONS

ABSTRACT: This paper explores the complexities and implications of electronic voting (e-voting) in the Italian and European contexts. Beginning with a definition of e-voting and its various forms, the paper examines the spread of e-voting across Europe. The advantages of e-voting, such as increased accessibility, potential for higher voter turnout, and cost savings, are discussed. However, the paper also delves into the risks associated with e-voting, including concerns about security, privacy, and the integrity of the democratic process such as cyberattacks, manipulation of votes, and breaches of voter privacy.

Various proposals to mitigate these risks are examined, including recommendations from the Council of Europe, the European Data Protection Supervisor, and the European Union Agency for Network and Information Security (ENISA). Overall, while the potential benefits of e-voting are evident, the paper suggests that

* Italian Data Protection Authority, Legal Advisor to the Vice President.

the current technological and legal landscape may not yet be conducive to its widespread adoption in Italy and Europe.

KEYWORDS: e-voting; democracy, security, data.

I. E-VOTING: A DEFINITION

What exactly is meant by electronic voting? In essence, it refers to participation in suffrage through the use of technological devices, such as, for example, smartphones or networked physical workstations. Thus, having a digital identity and having access to a computing device would be the only two requirements needed to cast a vote online.

On the other hand, from a purely technological point of view, the term *e-voting* refers to a variety of different approaches for modernizing the conventional electoral process, including the use of systems for optical reading of the paper ballot paper, the use of assisted voting machines with direct registration, and the exploitation of electronic voting on the public network, i.e. via the Internet.

Voting procedures have a wide range of variables, which makes for a rather thorny picture. However, despite the structural difficulties, it must be admitted that it also guarantees the possibility of numerous benefits and advantages, which will be examined in more detail in the following paragraphs.

II. THE SPREAD OF E-VOTING IN EUROPE

In the European context, there are numerous legislative initiatives aimed at promoting e-voting. With its Communication COM (2021) 118 final, entitled '*2030 Digital Compass: the European way for the Digital Decade*' of 9 March 2021[1], the European Commission presented its guidelines for the digital transformation of Europe by 2030. One of the goals of the EU is to ensure that by that time democratic life and online public services are accessible to all citizens, including through e-voting. Indeed, this measure would promote increased civic engagement among the population.

1. Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions, *2030 Digital Compass: the European way for the Digital Decade*, Brussels, 9.03.2021.

In Europe, few countries have chosen to rely on e-voting due to the still unreliable and acerbic development of this system.

In particular, to date the only European country in which e-voting is used on a stable basis in parallel with the traditional method is Estonia; here, in fact, the exercise of the right to vote via the Internet has been permitted since 2005. However, the multiplicity of technical requirements discouraged voter turnout in the last European round, which remained poor. Problems and difficulties related to the logical security of the electronic voting process also emerged[2].

In contrast to the Baltic experience, other Northern European countries opted for a conservative choice. Norway's experience is emblematic: first implemented a series of trials of electronic voting in order to test the system's response and then suspended the test after ten years of use due to the low degree of reliability in protecting electoral operations[3]. The incident demonstrates the wide scope for improvement of such systems.

Since face to face voting is still required for national, regional and local consultations, Germany and Great retain instead employ the electronic voting system for smaller consultation. In 2009, the German Constitutional Court declared the constitutional illegitimacy of e-voting[4], because – according to the German judges – it does not guarantee that every stage of the electoral process is public (as opposed to the classic ballot papers and polling places)[5].

III. ELECTRONIC VOTING IN ITALY

In the Italian legal system, the experimentation of electronic voting was provided for by the 2020 Budget Law[6], which established the Fund for Electronic Voting, with an allocation of € 1 million for the year 2020. The Fund is aimed at the experimental introduction of digital voting in

2. A.H. Trechsel, *Internet Voting in Comparative Perspective: The Case of Estonia*, in *Political Science & Politics*, 42(03), 2009, 497.
3. S.B. Segaard, H. Baldersheim, J. Saglie, *The norwegian trial with Internet voting: results and challenges*, in *Revista general de derecho publico comparado*, 2013.
4. BVerfG 2 BvC 3/07 of 3.03.2009. For the full text: *https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html;jsessionid=08D155D78A24BF9D65C85FCB33CA337F.2_cid*.
5. A. Gratteri, *Germany: the minimum necessary guarantees for electronic voting according to the Constitutional Tribunal*, in *Forum di Quaderni costituzionali*, 2009.
6. Law No. 160 of 27 December 2019, Art. 1, paragraphs 627-628.

European and political elections and for referendums. The experimentation refers to the vote of Italians abroad and of voters temporarily away from their municipality of residence for reasons of work, study or medical treatment. This provision, as we shall see, was later amended by Law Decree no. 77/2021 (art. *38-bis*, par. 10), which extended the experimentation to regional and local elections as well.

III.1. THE ITALIAN EXPERIMENTATION OF ELECTRONIC VOTING

Following the long-awaited adoption of the decree on the experimentation of electronic voting by the Minister of the Interior and the Minister of Digital Transition for the voting of outsiders in general elections, referendums and European elections[7], in July 2022 the approach to the e-method in Italy received a significant boost.

In detail, the Italian legislation specifically called for a phased experimentation: an initial phase of simulation without legal validity and a subsequent phase where voting would take place in a real electoral context with legal recognition.

In both phases, the vote should be cast through a specially created *web application* – which the voter can access through any digital device with an Internet connection – and through the Spid, thanks to which the citizen will be identified by the *e-voting* system.

The electronic vote will be integrated with the Sistema Informativo Elettorale (SIEL), the management of which is entrusted to the Ministry of the Interior, which will then publish the results of the test phase.

The decree provides for the secrecy of the vote and its preparatory operations, including the anonymity of the citizen.

Article 6, paragraph 3 of Decree-Law 41/2022, however, postponed the aforementioned experiment from 2022 to 2023[8]. It will be limited to two specific categories of voters: Italians abroad and those who, for reasons of work, study or medical treatment, are in a municipality of a region different from that of the place in whose electoral rolls they are registered.

7. Decree-Law No. 77 of 31 May 2021.
8. Digitisation of the electoral process and experimentation with electronic voting (*www.camera.it*).

In spite of the safeguards aimed at safeguarding the regularity of the procedure, the country's digital infrastructure currently appears backward and creates quite a few difficulties in handling such transactions smoothly. Moreover, due to the *digital divide*, difficulties may arise among segments of the population who, due to unfamiliarity with electronic devices or the mediocre quality of the available connection, will have to deal with unforeseen events and uncomfortable situations[9].

III.2. FIRST PRACTICAL CASES

At the local level, an experiment in electronic voting was conducted during the regional referendum on the so-called differentiated regionalism held in Lombardy on 22 October 2017[10]. The referendum was innovative because consisted in voting on electronic media called '*voting machines*' and the subsequent ballot, also in digital mode. However, it should be pointed out that the vote was not held remotely, but rather in person, in special polling stations.

Also worth mentioning is the decision of the Garante per la protezione dei dati personali (Italian Data Protection Authority), which issued an opinion on the draft decree of the Ministry of Foreign Affairs and International Cooperation, concerning the experimentation of electronic voting in elections for the renewal of the Committees of Italians Abroad[11]. In the case covered by the opinion, voter involvement in the experimentation of electronic voting was optional and did not produce any legal effects, but was in addition to the traditional postal vote using a paper ballot. In giving a positive opinion, the Authority requested that the text be supplemented to reflect the Ministry's involvement as well as the other subjects involved in the processing of personal data connected with the experiment (e.g. *Cloud service providers*), and highlighted the need for the term of retention of data, both by the Maeci and the Cloud service provider, to be indicated and justified by the

9. T.E. Frosini, *Internet and Democracy*, in *Sovranità e rappresentanza nell'era della globalizzazione*, in P. Miras, E.C. Raffiotta, G.M. Teruel Lozano, F. Vecchio (eds.), Naples, Editoriale Scientifica, 2021, 187-202.

10. The law, entitled Introduction of electronic voting for the advisory referendum. Amendments to Regional Law No 34 of 28 April 1983 (Nuove norme sul referendum abrogativo della Regione Lombardia), amended the previous legislation by introducing a new Article 26-bis.

11. Opinion on the draft decree of the Ministry of Foreign Affairs and International Cooperation on Maeci's experimentation with electronic voting for the renewal of the Committees of Italians Abroad 2021 (Com.It.Es) of 19 November 2021, no. 9721434.

performance of specific purposes to be made explicit in the text of the decree (and not only in the technical documentation).

The Maeci also had to take additional measures in the case of the transfer of personal data to countries outside the European Union to ensure a level of protection of personal data substantially equivalent to that provided for in Regulation (EU) 679/2016[12], including the encryption of personal data by the data controller, with encryption keys in its exclusive availability. Finally, with regard to the future viability of e-voting, the Ministry will have to take into account the critical issues highlighted by the Authority and the possible risks looming, more generally, on e-voting procedures also highlighted in the documents adopted in the European context.

III.3. DIGITISATION OF PRELIMINARY ELECTION PROCEDURES

Legislative efforts for the computerization of preliminary election procedures have also been envisaged in recent years in the Italian legal system.

The Electoral Reform Law (Law 165/2017) has delegated (Article 3, paragraph 7) to a ministerial decree, to be adopted within six months from the date of entry into force of the Law, the definition, on an experimental basis, of the collection in digital mode of the subscriptions necessary for the presentation of lists of candidates, including through the use of digital signatures and qualified electronic signatures. The decree, however, has not yet been adopted at the time this contribution is being prepared.

It is also worth mentioning, through d.l.. 77/2021 (*Governance of* the PNRR and simplifications) the introduction of a series of measures aimed at digitisation in the field of electoral preparatory procedures.

III.3.1. Electronic signature for referendums

Regulations for electronic signatures and popular initiative bills have also been introduced with regard to referendum. These regulations complement the provisions of the 2021 Budget Law (art. 1, paragraphs 341-343) which provided for the establishment of a platform for the collection of digital signatures.

12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

A transitional rule stipulates that – starting on 1 July 2021 and up until the platform becomes operational – the signatures required for one of the referendums referred to in Articles 75, 132 and 138 of the Constitution, as well as for proposing draft laws, can also be collected using an electronic document that has been qualified for electronic signatures.

As far as the amendments are concerned, the scope of the platform is extended, which – as a result of the amendments – covers the collection of voter signatures to be carried out also through SPID and similar systems for one of the referendums provided for in Articles 75 (abrogative), 132 (territorial variations) and 138 (constitutional amendments) of the Constitution and for the proposal of popular initiative bills (Article 71 of the Constitution).

III.3.2. The appointment of list representatives

Lastly, with reference to the appointment of list representatives, Article *1-bis* of Decree-Law No. 25 of 5 March 2021, which postponed the elections scheduled for 2021, already allowed the designation of list representatives to be submitted to municipal offices by certified email, instead of the forms provided for by the legislation in force (written declaration on unstamped paper authenticated by a notary). The provision, which only concerned the 2021 elections, was adopted in view of the continuing epidemiological situation related to the spread of Covid-19 with the aim of ensuring the necessary social distancing in the context of the voting operations in question.

IV. THE ADVANTAGES OF ELECTRONIC VOTING

IV.1. THE SIMPLICITY OF EXERCISING ONE'S RIGHT TO VOTE

First, remote voting is easier and more convenient than the traditional, ordinary method that requires citizens to go to the polling station or look for a mailbox. In fact, a person can cast his ballot while at home using any technological device with an Internet connection.

It is very clear how direct digital democracy can become a current[13] fact, credible, possible and contingent, allowing voters to express themselves on national energy policies, on whether or not an international agreement is appropriate, on the *impeachment* even of one or more members of the

13. On all, S. Rodotà, *Sovereignty in the Time of Techno Politics. Electronic Democracy and Representative Democracy,* in *Politica del diritto*, 1993, 569.

executive, at breakfast time and without the need for intermediaries is now a viable reality[14].

IV.2. THE ANTI-ABSTENTIONIST EFFECT

Such simplicity would also increase the influx of voters, especially older people who very often find it difficult to travel to polling stations[15]. Electronic voting would make it possible to overcome the logistical and organisational difficulties that arise in voting by residents abroad: difficulties have often been reported by voters who received their voting material later than the legal deadline. Moreover, from the point of view of the legitimacy and correctness of votes, electronic voting would cancel out invalid ballot papers due to human error in filling them in: a choice, and possibly a relative preference, in a fully electronic system would be sufficient to cancel out invalid ballot papers[16].

IV.3. SAVINGS

Moreover, the fully electronic approach would produce substantial cost savings compared to traditional voting dynamics. The time required to count the votes cast would be shortened, since no human verification would be needed. However, the prospect of legitimising electronic voting is not reflected in reality. Many countries, both European and non-EU, have attempted to approach the issue of remote voting on several occasions over the last decade, without definitively overcoming technical-legal difficulties and criticisms that have emerged systematically.

V. WHAT RISKS?

Despite the benefits in terms of higher turnout and less organisational challenges, the empirical approach centered on the theoretical conception of e-voting offers a scenario that is not without its criticalities. The possible negative consequences that could arise from the implementation of e-voting – due to issues related to computer security, privacy and legitimacy and, as a consequence, to the resilience of the democratic system of states themselves –

14. N. Bobbio, *The Future of Democracy,* Turin, Einaudi, 1995.
15. On the positive effects of *e-voting,* see, P. Carlotto, *Il voto elettronico in Italia: sperimentazioni e difficoltà*, in *Nuova Rassegna*, n. 1/2012.
16. L. Trucco, *Will new technologies save the Italians' vote abroad?,* in *Forum di Quaderni costituzionali*, 2013.

are of such a significant nature that we must ask ourselves whether a correct balancing of rights of this magnitude is really possible, a balancing to which the admissibility and lawfulness of e-voting is subject.

While e-voting may be thought of as a way to speed up and reduce the cost of elections, it may end up being less efficient and secure than traditional voting. For instance, it would be much easier, in the absence of 'on sight' checks, to carry out forms of voter manipulation, particularly with regard to the most vulnerable (e.g. due to poverty or illnesses that impair their capacity to vote).

This would lead to the possibility that the independence of voters would not be protected, as the isolation of the voting booth could not be guaranteed, thus encouraging an increase in phenomena such as vote rigging. Other risks could include attempts by other states to interfere with the results or cybercriminals stealing personal data.

The secrecy of suffrage then serves a practical purpose in relation to freedom, as a necessary – though not sufficient – condition for its effective guarantee[17].

In order to ensure the efficiency and security of e-voting, anonymity, authenticity and secrecy of the vote should be guaranteed and it should be verified that the vote is only cast once per person[18]. Furthermore, the voting platform should be equipped with very high security standards to protect users' personal data and prevent any computer tampering with the results. However, any manipulation of the voting software could be difficult to detect and, as happened in Russia in 2019, platforms could easily be hacked if not equipped with state-of-the-art encryption systems.

It is the scientific community itself that considers electronic voting to be inadequate with respect to the technological infrastructure offered by contemporary society. What raises serious doubts are the fundamental elements of expression, representation and guarantee that permeate the representative democratic system in the legal-informatics context. Indeed, the institutional implementation of technology must be democratically oriented, i.e., carried out with respect for fundamental democratic principles and values[19].

17. E. Bettinelli, *Voting Rights* (voce), in *Dig. disc. pubbl.*, 1990, 228.
18. G. Pitruzzella, *Elezioni politiche: elettorato* (voce), in *Enc. giur.*, XII, Rome, 1989, 4.
19. G. Fioriglio, *Electronic Democracy. Presupposti e strumenti,* Milan, 2017, 8.

The debate on the issues that remote electronic voting raises involves enormous topics ranging from the protection of participants' personal data, to the internal transparency of platform operators, from the reasonableness of the rationale for counting the preferences expressed, to the correct or incorrect interpretation of the electoral participation that they imply, from the proportionality of the decision-making prerogatives between those who pose the question and those who are called upon to respond to it, to the actual freedom of the preference that can be expressed, from the equality of substantial opportunity of the actors in the decision-making process, to the concreteness, finally, of the interest regarding the most disparate and complex issues that can be resolved by typing a binary alternative.

There are many facets to the negative consequences in terms of the legitimacy of voting: think, for instance, of the frequency of logical attacks capable of compromising computer systems. Impacts in the context of e-voting can result in a potentially catastrophic scenario.

A bug in a server, used to collect the votes cast, for example, could easily erase some, if not all, of the choices made. A disaster capable of invalidating the voting process of any democratic system, with the result of completely distorting the election results.

In addition, there could be a context of systematic alteration of the votes cast. Certain countries could go so far as *to* carry out *cyberwarfare* operations in order to contaminate the representative elections of other states in exchange for economic, geopolitical and strategic advantages.

The scenario outlined, therefore, would mortgage two cornerstone principles in guaranteeing the democratic method: the integrity and confidentiality of the vote. Moreover, intrusion by unauthorised parties would also compromise the privacy of voters.

The latter aspect should not be underestimated, as any dissemination of personal data would also have repercussions on the individual daily lives of citizens, paving the way for attacks through *social engineering* techniques.

Nowadays, and in a context where electronic voting is not yet the reality, *phishing* operations against both individuals and structured organisations are frequent.

It can therefore be said, from a constitutionalist-political point of view, that the possible permanent implementation of the e-voting system thus represents a potential threat to representative democracy itself.

VI. SOME PROPOSALS TO MITIGATE RISKS: COUNCIL OF EUROPE, EDPS AND ENISA OPINIONS

On 14 June 2017, the Committee of Ministers of the Council of Europe, in its Recommendation CM/Rec (2017) on standards for electronic voting, in view of concerns about potential problems with the security, reliability or transparency of the systems used for electronic voting[20], drew attention to the need for the fundamentals of democratic elections to be respected and, in particular, that:

secrecy of the vote is guaranteed throughout all the stages of the procedure,

only personal data necessary for the purposes of electoral consultations are processed,

the security of the authentication data is ensured against improper access by unauthorised persons,

the voter is not provided with proof of the content of the vote cast in order to prevent its misuse by third parties,

it is impossible, at the ballot stage, to reconstruct a link between the unsealed vote and the voter,

the persons entrusted with the responsibility of the voting procedure identify the persons authorised to access the systems, ensure the proper functioning of the voting system, carry out updates and maintenance, comply with appropriate security measures and manage security incidents, ensure data integrity and the protection of personal data and the correct identification of voters.

Similarly, the European Data Protection Supervisor issued an opinion on the Commission's package of measures to ensure free and fair European elections (*Opinion 10/2018 on the Commission Package on free and fair European elections*), as did the *European Union Agency for Network and Information Security* (ENISA, *Opinion paper 02/2019, Election cybersecurity: Challenges and opportunities*), issued a document drawing attention to the high level of risk in the current context to all information systems used for the entire cycle of electoral management (from the keeping of electoral rolls to the counting and compilation of voting

20. M. Mcgaley, J. Mccarthy, *Transparency and e-voting. Democratic vs. commercial interests*, in A. Prosser, R. Krimmer (eds.), *Proceedings of the 1st international Workshop on Electronic Voting in Europe* (Lecture notes in informatics), 2004, 153.

results), arising from suspected or actual attacks on the integrity, confidentiality or availability of these systems and networks (which can be used to undermine the credibility and question the legitimacy of the vote):

emphasise that these risks are much higher when the voting process is carried out electronically,

point out that the electronic voting systems generally used, in third countries and in the EU, have significant vulnerabilities, and that the distinction between online and offline electronic voting systems (so-called *ballot stations*) is relevant, as the former are likely to involve a higher level of cyber security risk than the latter,

Finally, they endorse the recommendation to Member States to conduct a comprehensive assessment of the risks associated with the European Parliament elections in order to identify potential cyber incidents that could affect the integrity of the electoral process.

VII. CONCLUSIONS

Electronic voting is a rather complex prospect to implement, both from an IT and legal point of view. Indeed, there are fears of several instance of fraud and logistical difficulties. The case that recently occurred concerning the election of Russian President Vladimir Putin is emblematic, having highlighted all the inconsistencies of the remote voting system: the multiple reports of violations in the guarantee of secrecy and confidentiality of the suffrage have provoked reactions all over the world, raising accusations against the Russian political system of not having guaranteed the transparency necessary to ensure the fairness of the voting procedure. Despite the assurances of the Russian authorities, it is clear that more than something went wrong during the election round.

The Russian example serves as a cautionary tale for all those jurisdictions that are planning to experiment with electronic voting, with Italy leading the way. The Italian infrastructure – both from the point of view of IT security and the quality of electronic communications -, as the technical remarks of the Garante in the recent opinion issued on the subject also highlight, would not appear to be able to support the implementation of an alternative voting process to the traditional one.

The absence of a cryptographic standard – capable of guaranteeing the confidentiality of electronic transmissions – is currently an insurmountable

obstacle to the implementation of remote voting. Even other more evolved European countries, from a technological and digital point of view, do not seem to be in a position to offer structural solutions capable of satisfying all the legal requirements to allow qualified and certified suffrage, and such as to guarantee subjective control by the citizen throughout the electronic voting process[21]. At least for now, the time does not seem ripe for the full introduction of electronic voting in Italy and, more generally, in Europe.

21. T.E. Frosini, *Internet and Democracy*, cit., 187-202.

Ius publicum europaeum

Digital rights and public powers: a European perspective on digital citizenship

1Marina Caporale*

SUMMARY: I. PREMISE - II. THE PROGRESSIVE DEFINITION OF EUROPEAN DIGITAL CITIZENSHIP. THE "EUROPEAN DECLARATION ON DIGITAL RIGHTS AND PRINCIPLES FOR THE DIGITAL DECADE" AND THE CENTRALITY OF INDIVIDUALS - *II.1 Previous experiences of the Italian and Spanish Internet Declaration of Rights* - III. CONCLUDING REMARKS. EUROPEAN DIGITAL ADMINISTRATIVE CITIZENSHIP. RIGHTS AND DUTIES

ABSTRACT: The European Union law and politics are increasingly putting more and more efforts in the digitalization of public administration in the member states and within European institutions itselves. As the digitalization of public administration evolves, changes also the relation between individuals and PAs in terms of rights and duties, traditionally connected to the concept of citizenship. In that way it seems to emerge a proper concept of digital citizenship in a European legal framework, that is already taking form in Italian law.

KEYWORDS: European Administrative Law; Digital Citizenship; Digital Administration.

I. PREMISE

The term "citizenship" always raises very particular sensitivities, as it immediately evokes the classical and constitutional meaning of belonging to a specific system and the consequent special relationship between individual

* Associate Professor in Administrative Law, University of Modena and Reggio Emilia.

and nation, historically comprising a complex set of rights but also duties, active and passive situations, shaped by the contents, methods and legal jurisdictions determined by the same legal system[1]. For citizens of the member states of the European Union, citizenship as recognized within national normative frameworks implies, moreover, by law, the recognition of European citizenship, which qualifies the special relationship between citizens and member states of the Union and citizens and the European Union itself[2].

In times featuring migration and the ensuing complexities, as well as limits to freedom of movement induced by the health emergency and public safety concerns, the topic of citizenship has assumed special relevance in public discourse, in its main meaning but also in the other definitions that have emerged over time. This variety of meanings can be referred to the progressive recognition of a core of fundamental rights and different juridical positions even for non-citizens, in the various systems, whereby there has been a transition from "citizenship" to "citizenship rights", where citizenships are determined, one could say, "with variable geometries", or, better yet, according to a "multiple-dimension citizenship" model[3].

1. The scholarly literature about the concept of citizenship is impressively sizeable. For the sake of economy of the text here we will refer only to some references, mainly Italian: G. Azzariti, *La cittadinanza. Appartenenza, partecipazione, diritti delle persone*, in *Dir. Pubbl.*, n. 2/2011, 426; G. Berti, *Cittadinanza, cittadinanze e diritti fondamentali*, in *Riv. Dir. Cost.*, 1997, 3; G. Biscottini, *Cittadinanza* (voce), in *Enc. dir.*, VII, Milano, Giuffrè, 1960; R. Clerici, *Cittadinanza*, in *Dig. Pubb.*, III, 1989; P. Costa, *Cittadinanza*, Roma-Bari, Laterza, 2005; F. Cortese, G. Santucci, A. Simonati (eds.), *Dallo status di cittadino ai diritti di cittadinanza*, Napoli, Editoriale scientifica, 2014; M. Cuniberti, *La cittadinanza. Libertà dell'uomo e libertà del cittadino nella Costituzione italiana*, Padova, Cedam, 1997; A. Morrone, *Le forme della cittadinanza nel terzo millennio*, in *Quad. Cost.*, n. 2/2015, 303.
2. M. Cartabia, *Cittadinanza europea*, in *Enc. Giur.*, Roma, Treccani, 1995; M. Condinanzi, B. Nascimbene, *Cittadinanza dell'Unione e libera circolazione delle persone*, in M.P. Chiti, G. Greco (eds.), *Trattato di diritto amministrativo europeo*, Parte generale, I, Milano, Giuffrè, 2007, 87; V. Lippolis, *Cittadinanza dell'Unione europea*, in S. Cassese (ed.), *Dizionario di diritto pubblico*, II, Milano, Giuffrè, 2006, 932; A. Tizzano, *Alle origini della cittadinanza europea*, in *Il Diritto dell'Unione Europea*, n. 4/2010, 1031; A. Pinelli, *Cittadinanza Europea*, in *Enc. dir.*, Annali, I, Milano, Giuffrè, 2007.
3. A. Bartolini, A. Pioggia, *Le cittadinanze amministrative. Percorsi e prospettive, dell'amministrazione tra diritti e doveri a 150 anni dalle leggi di unificazione amministrativa*, in A. Bartolini, A. Pioggia (eds.), *Cittadinanze amministrative*, VIII, in L. Ferrara, D. Sorace (eds.), *A 150 anni dall'unificazione amministrativa italiana,* Firenze, FUP, 2016, 14 ff.

In this way, the adjectives that have progressively been placed alongside the term citizenship, distinguishing it from its main meaning, have engendered new legally relevant definitions which are used, in particular, to identify novel and different ways in which the relationship between public powers and individuals could be expressed: administrative citizenship (including the European variant)[4], active citizenship[5], global citizenship[6]. These "other" citizenships all dialogue with historically understood citizenship within the context of a bond of belonging to one's own national legal system, but also with European citizenship.

Perhaps a further "citizenship" could now be added to these meanings: digital citizenship, which currently lacks a distinct legal standing and definition. In fact, the relevant debate oscillates between the recognition of digital citizenship as having its own legal status - also in the light of the recognition of "new" digital rights - and its possible ascription to the "other" mentioned citizenships, as a result of technological evolution and therefore as their simple corollary.

With reference to the digital dimension of citizenship, it is necessary first of all to consider the issue of the recognition, by major international organizations and, progressively, in various national systems, of "new" digital rights, including the acknowledgment of access to the internet and freedom of online expression as fundamental human rights[7]. These new rights are affirmed, in a broader and more detailed sense, in recent documents, in particular the "European Declaration on digital rights and principles for the digital decade"[8], which seems to contribute, with other European Union

4. G. Arena, *Il principio di sussidiarietà nell'art. 118, u.c. della Costituzione*, in *Studi in onore di Giorgio Berti*, I, Napoli, Jovene, 2005, 215; A. Bartolini, A. Pioggia (eds), *Le cittadinanze amministrative*, cit.; C.E. Gallo, *La pluralità delle cittadinanze e la cittadinanza amministrativa*, in *Dir. Amm.*, 2002, 483; R. Cavallo Perin, *La configurazione della cittadinanza amministrativa*, in *Dir. Amm.*, 2004, 204.
5. G. Arena, *Il principio di sussidiarietà*, cit.; Idem, *La cittadinanza attiva nella Costituzione*, in F. Cortese, G. Santucci, A. Simonati (eds.), *Dallo status di cittadino ai diritti di cittadinanza*, cit., 241; E. Grosso, *Le vie della cittadinanza. Le grandi radici. I modelli storici di riferimento*, Padova, Cedam, 1997.
6. R. Cavallo Perin, *L'ossimoro della locuzione "cittadinanza globale"*, in *Dir. Amm.*, 2005, 211; R. Romano Tassone, F. Manganaro (eds.), *Dalla cittadinanza amministrativa alla cittadinanza globale*, Milano, Giuffrè, 2005.
7. See the United Nations Human Rights Council Resolution of 5 July 2012. See at least L. Cuocolo, *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in *Politica del Diritto*, n. 2-3/2012, 263 ff.
8. European Declaration on Digital Rights and Principles for the Digital Decade, 2023/C 23/01, Joint Declaration of the European Parliament, the Council and the Commission.

sources, to the progressive definition of a European dimension of digital citizenship.

The affirmation, in public debate, of these rights and the theme of digital citizenship must certainly be read in the light of technological progress and its implications for the relationship between individuals and the digital environment in general, especially as concerns major internet service providers. Above all it is important, for the argument developed here, , for the special relationship between public powers and individuals. This relationship, in its the digital dimension, is mediated by private providers of digital services, and exposes citizens and public authorities themselves to new challenges, and it has different implications than those deriving from pre-existing citizenship statutes. Also, in the light of this mediation, the attention of international bodies and European and national legislators has focused mainly on the difficult balance between the protection of individuals' rights - primarily the protection of personal data - and the promotion of digital services, when the latter benefit individuals and society. The involvement of public administrations in this process has been parallel and slower in a first phase, but today it is one of the main intervention pillars underlying European Union efforts to achieve a qualitative leap in the digital economy. It is in fact clear that the use of the most advanced technological tools by public authorities is also an essential part of economic growth, increasingly based on digital systems and the information digitization. The creation and reliability of adequate digital public services for people and businesses, the interoperability of digital solutions and systems within the same national system and also between different, national and transnational systems, the use and reuse of data held by public administrations, are all fundamental parts of the development and competitiveness of the UE, but they pose unprecedented questions in terms of the security of the systems themselves and the protection of individuals, which call for a more thorough reflection on the bond of belonging, the pact that lies at the basis of this special relationship between individuals and public powers encompassed in the concept of "citizenship". In these areas, therefore, European Union legislation intervenes in different ways and with progressive strength and extension, mainly in light of the creation of a digital single market but also to foster a fuller and more effective enjoyment of European citizenship rights and therefore to exercise the right to free movement and residence and the right to non-discrimination. These rights has to be considered under the perspective of Art. 41 of the European Charter of Fundamental Rights, the right to a good administration.

In this context, regulatory interventions in progress, an at least dual meaning of digital citizenship emerges.

The first meaning identifies a series of fundamental and non-fundamental rights of individuals in the use of digital services and the interaction with other (especially private but also public) subjects. This meaning is closer to the approach that promotes awareness of individual rights as a basic feature in the acquisition of digital skills, through digital education initiatives (also called digital citizenship education).

The second meaning interprets "new" digital rights, recognized in international sources and national legal systems, within the grammar of the relationship between individuals and public powers and in particular between public administrations and administered subjects, on which we will mainly focus.

II. THE PROGRESSIVE DEFINITION OF EUROPEAN DIGITAL CITIZENSHIP. THE "EUROPEAN DECLARATION ON DIGITAL RIGHTS AND PRINCIPLES FOR THE DIGITAL DECADE" AND THE CENTRALITY OF INDIVIDUALS

As anticipated, until now, there is no legally univocal meaning of digital citizenship, but there is no doubt that lawmakers and scholars are focusing with increasing attention on this lemma[9].

Looking at supranational sources, we can refer first of all to the definition of digital citizenship given by the Council of Europe as a set of citizens' digital skills, to be promoted and supported to overcome the digital divide to the broadest possible extent[10]. This approach is most reflected in the first

9. M. Caporale, *Dalle smart cities alla cittadinanza digitale*, in *Federalismi.it*, 22 january 2020 and also M. Caporale, *Dalla smart citizenship alla cittadinanza digitale*, in R. Cavallo Perin (ed.), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Quaderni del Dipartimento di Giurisprudenza dell'Università di Torino, 2021, 261; F. Costantino, *La c.d. cittadinanza digitale*, in *Dir. Pubb.*, n. 2/2023, 143; P. Costanzo, *Avete detto "diritti digitali"?*, in *Diritto Mercato Tecnologie*, n. 2/2016, 145; T.E. Frosini, *Il diritto costituzionale di accesso ad internet*, in *Rivista AIC*, n. 1/2011; P. Marsocci, *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, in *Rivista AIC*, n. 2/2015.

10. Council of Europe, *Digital Citizenship Education Handbook,* Strasbourg, Council of Europe Publishing, 2019. Similar initiatives, aimed at promoting digital citizenship education, intended as digital skill acquisition, are implemented by other international organisations, in particular Un, Unesco e Unicef, Oecd. Furthermore, there are various

of the two considered meanings of digital citizenship, although, in its turn, it also constitutes an essential part of the second one.

In reference to the meaning most connected to the relationship between individuals and public powers, the theme of digital citizenship originally emerged in the last century from the perspective of e-democracy, in its different senses embracing transparency, participation and vote expression through digital tools, and then transitioned into the concepts of e-government, as a possibility for citizens and public administrations to interact through digital services.

Since then, e-government policies have changed their approach, moving from the definition of e-government/electronic government[11], to that of digitization of administrations, to the more recent definition of digital government. At the same time, the perspective on those who interact with the public administration's online services has changed. A government-/ / administration-centred approach has transitioned to a system increasingly oriented towards the needs of the user/citizen (user-/citizen-centred). The next stage, which is already a reality in some countries or in individual initiatives, is that of a "people-citizen driven" or "user voices" dimension, which starts from people's needs, their voice as the driving force of public administration activities[12]. The application of these models, going beyond what may appear to be a certain rhetoric, has a significant impact on the organization and the activities of public administrations, as well as on

meanings of the same term "digital divide", v. J. van Dijk, *The digital divide*, Cambridge, Polity, 2020.

11. In the definition given, for the first time, by Gartner Group, Western Europe Government Sector: IT Solution opportunities, 2000. To date there is no single definition of e-government. With reference to Italy, see F. Merloni (ed.), *Introduzione all'e-Government*, Torino, Giappichelli, 2005.

12. See Oecd, *Recommendation of the Council on Digital Government Strategies*, 15 july 2014, where Digital Government is defined as: "…[it]refers to the use of digital technologies, as an integrated part of governments' modernisation strategies, to create public value. It relies on a digital government ecosystem comprised of government actors, non-governmental organisations, businesses, citizens' associations and individuals which supports the production of and access to data, services and content through interactions with the government". More recently see Oecd, *Digital Government Strategies for Transforming Public Services in the Welfare Areas, Comparative Study*, 2016, in which is reported: "The challenge is not to introduce digital technologies into public administrations (digitisation); it is more transformative. The challenge is to integrate the use of digital technologies into public sector modernisation efforts (digital government)". See again Oecd, *Strengthening Digital Government*, *https://www.oecd.org/going-digital/strengthening-digital-government.pdf*, 2019.

how citizen participation is understood and implemented. These models have been largely rethought in the debate on smart cities (and therefore on smart people and smart citizenship), at the international level and also the European and national levels. Experiments conducted in cities have had an innovative character, and have often served as a driving force for reflections on digital citizenship.

Mainly in this perspective, but then in a more general sense, digital citizenship has been compared to administrative citizenship, as "belonging to a community other than the sovereign one, with legitimation of subjective positions that do not depend on the status of citizen-sovereign... as legitimation, which in public services, however, has always been recognized to each person administered", legitimation of ownership of subjective legal situations towards public administrations, including European ones, thus defining European administrative citizenship. Even in the meaning of European citizenship, in fact, intermediate statuses can be found which do not refer exclusively to European citizens, mainly on the basis of the rights of movement, establishment, and non-discrimination based on nationality, and which more often than not can be asserted against public administrations, from a market perspective rather than as recognition of social rights[13].

The centrality of individuals appears to be the distinctive and common feature of the measures adopted by the EU in the digitalisation of public administrations, even in the absence of a definition of digital citizenship. This centrality should be considered as referring to the European administrative citizen, and here too, it seems, in a perspective more consistent with the objective of creating a digital single market than recognition of rights per se. On the other hand, the structure of European competences appears to favour this perspective. The EU's interventions in the field of digitalisation therefore reflect a serious consideration of the rights of European citizens but above all the need to affirm a role for the EU in the digital economy which, at the moment, is weak compared to that exercised by other countries. This approach is also crucial in the pursuit of e-government and the creation of European digital single market policies. It also results from a series of declarations that have followed one another with growing intensity in

13. R. Cavallo Perin, *La configurazione della cittadinanza amministrativa*, cit.; G. Arena, *Il principio di sussidiarietà*, cit. See again the argumentation in in M. Caporale, *Dalla smart citizenship*, cit. See also E. Fragale, *La cittadinanza amministrativa al tempo della digitalizzazione,* in *Dir. Amm.*, n. 2/2022, 471. About the european administrative citzenship see A. Bartolini, A. Pioggia, *Cittadinanze amministrative*, cit., 25 ff.

recent years[14] and prepared the ground for the approval of the "European Declaration on Digital Rights and Principles for the Digital Decade"[15].

The European Declaration is not legally binding, but programmatic[16], defining a framework of fundamental rights and principles intended to inspire European and national legislators in the implementation of the European Digital Decade. So, it's a declaration of rights with an expiration date, connected to an explicit time horizon. The Declaration also explicitly places people at the centre of a digital transformation that is intended to be

14. We refer to *Ministerial Declaration on eGovernment approved unanimously in Malmö*, Sweden, on 18 November 2009; Tallinn, *Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU* on 6 October 2017; *Lisbon Declaration – Digital Democracy with a Purpose*, Lisbon, 1° June 2021.

15. The EU, in particular after the Lisbon Council of 2002, has adopted several Action Plans for e-government, the latest referring to the period 2016-2020, *Accelerating the digital transformation of public administration, Communication from the Commission to Parliament European Council, the European Economic and Social Committee and the Committee of the Regions, EU Action Plan for eGovernment 2016-2020*, Bruxelles, 19 April 2016 COM(2016) 179 final. In 2018 te European Commission has presented a financing programme "Digital Europe" 2021-2027, *Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Program and repealing Decision (EU) 2015/2240*. To date, e-government plans are an integral part of the programs prepared by the EU for digital Europe and in particular the creation of a *Digital Single Market, Communication from the Commission to the European Parliament, the Council, the European Econo d Social Committee and the Committee of the Regions a Digital Single Market Strategy for Europe*, COM/2015/0192 final. The more recently approved UE *e-government* plan (*E-Government Action Plan 2016-2020*), unsurprisingly, is an integral part of the strategy for the Digital Single Market. The "European Digital Decade" consists of a strategic programme that identifies concrete digital objectives, to be achieved by 2030, based on four cardinal points: digital skills, digital infrastructures, digitalisation of businesses and digitalisation of public services. This last point is pursued through three key objectives that the Commission intends to achieve within the digital decade: online availability of 100% of the main public services; online access to their medical records by all citizens; use of digital identity solutions by 80% of citizens: digital-strategy.ec.europa.eu/en/policies/europes-digital-decade infra. One should also underline the primary importance of actions financed, in the various member states, through the Next Generation EU initiative and therefore the associated national plans.

16. See preamble, par. no. 10 of the Declaration. However, the Declaration is directly referred to by one of the most significant regulations recently adopted by the European Union, see Recital 7 of the approved text of the Artificial Intelligence Act (P9_TA(2024)0138, European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

"anthropocentric"[17], with the objective and urgency, on the part of the EU, of specifying how consolidated fundamental values and rights currently applied offline in the EU legal system should be implemented in the digital, online environment. On the other hand, the Declaration opens with an affirmation of the rights and values of the Union which follows and recalls almost entirely the one contained in the Preamble to the European Charter of Fundamental Rights, which also states that the EU places people at the centre of its actions by establishing citizenship of the Union[18]. It therefore seems important to underline the connection between anthropocentric digital transformation, affirmed by the European Declaration, and the centrality of the people also stated in the European Charter of Fundamental Rights, from which the institution of European citizenship is derived.

Individuals are therefore at the centre of both documents, which evidently have different legal value, and this legitimizes even more the recognition of digital rights as a corollary of European citizenship. Particularly relevant is the passage in the European Declaration in which the EU asks its institutions and member states to commit to creating instruments that are closely linked to European citizenship, freedom of movement, prohibition of discrimination and equal treatment, which is what the EU means when it intends to apply European fundamental values and rights, already established offline, , in the digital environment[19]. The interpretation of a digital citizenship, also

17. According to the first draft of the Declaration: "Putting people at the center of the digital transition is a key priority for the European Commission. The digital transformation should be shaped according to our European values and norms. Today the Commission proposes to establish a set of principles for an anthropocentric digital transformation"; *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the establishment of a European declaration on digital rights and principles {SWD(2022) Bruxelles, 26.1.2022 COM(2022) 27 final*.

18. European Declaration on Digital Rights and Principles, par. 1: "The European Union (EU) is a 'union of values', as enshrined in Article 2 of the Treaty on European Union, founded on respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. Moreover, according to the Charter of fundamental rights of the European Union, the EU is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity. The Charter also reaffirms the rights as they result, in particular, from international obligations common to the Member States".

19. See especially Preamble, par. no. 3: "…With the acceleration of the digital transformation, the time has come for the EU to spell out how its values and fundamental rights applicable offline should be applied in the digital environment. The digital transformation should not entail the regression of rights. What is illegal offline, is illegal online. This Declaration is without prejudice to 'offline policies', such as having access to key public services offline…" and Preamble, par. no. 12: "…The promotion and implementation

in a dimension of European administrative citizenship, which essentially represents a corollary, is here confirmed. Furthermore, as already previously argued, in the Union itself, it was hoped that European citizenship should be strengthened through the use of digital tools, starting with electronic identification, which would allow access to online public services and participation throughout the whole Union[20].

II.1. PREVIOUS EXPERIENCES OF THE ITALIAN AND SPANISH INTERNET DECLARATION OF RIGHTS

The European Commission, in adopting the first draft of the Declaration, claimed that it was the first declaration of its kind in the world. The adoption of an "Internet Bill of Rights" had actually been discussed for some time in Europe[21], also thanks to the debate raised, at an international level, by Stefano Rodotà's far-sighted proposal, within the Internet Governance Forum, of an Internet Bill of Rights[22], a proposal that was never followed up. As precedents with respect to the European Declaration, in addition to these unsuccessful attempts, we have to mention two declarations of internet rights, adopted in Italy and Spain: for Italy, the Declaration of Internet Rights, adopted in 2015; for Spain, the Carta de Derechos Digitales, adopted in 2021[23]. These documents share the same perspective expressed by

---

of the Declaration is a shared political commitment and responsibility of the EU and its Member States within their respective competences and in full compliance with EU law…".

20. Report on Parliamentarism, European citizenship and democracy, 25 July 2023 - (2023/2017(INI)), European Parliament, Committee on Constitutional Affairs, Rapporteurs: Alin Mituța, Niklas Nienaß.
21. European Parliament recommendation of 26 March 2009 to the Council on strengthening security and fundamental freedoms on the Internet (2008/2160(INI)).
22. S. Rodotà, *Una Costituzione per internet?*, in *Politica del Diritto*, n. 2/2020, 342 ff.
23. For Italy: *Dichiarazione dei diritti in internet*, 28 july 2015, text developed by the *Commissione per i diritti e i doveri relativi a internet, istituita dalla Camera dei Deputati*, chaired by Stefano Rodotà himself, 28 july 2014; the charter is not binding for the legislator but the Chamber of Deputies approved the motion "Quintarelli and others", n. 1-01031 and the motion "Caparini and others", n. 1-01052, aimed at committing the government to activate every useful initiative for the promotion and adoption at national, European and international levels of the principles contained in the Declaration: *https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf*; for Spain: *Carta de Derechos Digitales*, 2021, developed by the Grupo asesor de Expertas y Expertos constituido por la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital: *https://derechodigital.pre.red.es/documentos/CartaDerechosDigitales_04_ENG.pdf*.

the European Declaration, albeit with some differences, partly determined by the different periods of elaboration of the three texts. Like the European Declaration, the Italian and Spanish Declarations are not binding and adopt the general approach of affirming online digital rights in a broad sense even if, in the Spanish and European Declarations, digital public services are also expressly considered. The Italian Declaration lacks an article expressly dedicated to digital public administration but does outline a strong role to public authorities in the promotion and protection of established digital rights; also, individual rights connected to public administrations (e.g., accessibility to public information, reuse of data and public information…, art. 14, c. 5 and 6) are expressly mentioned.

In any case, as for the Italian and Spanish Declarations, even rights and principles of a general nature, also cited in the European Declaration, have a value in the "digitalised" relationship between public authorities and citizens: the right to education and training in the acquisition of digital skills, the overcoming of every digital divide (economic, gender, age...), the principles of inclusiveness, the perimeter placed on artificial intelligence (pending the approval of the European regulation on artificial intelligence) and citizens' freedom of choice...

The European Declaration contains, as anticipated, a paragraph expressly dedicated to online digital public services which expresses the relevance of the digitalisation of public administrations for the full affirmation of digital rights, and in which the core of a true European digital administrative citizenship can be glimpsed. In fact, it affirms the right of every person to have online access to main public services in the EU as well as the principle according to which no one should be asked to provide personal data more often than necessary when accessing and using digital public services.

The Declaration therefore refers to every person, not just EU citizens, thus confirming the proposed interpretation about a possible affirmation of a European digital administrative citizenship.

And the next point should also be read in this sense, in reference to the need to provide the possibility of enjoying a digital identity to all people living in the EU[24].

24. On the element of the habitual residence in the configuration of administrative citizenship, see at least R. Cavallo Perin, *La configurazione della cittadinanza amministrativa*, cit. With reference to the same requirement for the purposes of European administrative citizenship and for the jurisprudence of the Court of Justice see A. Bartolini, A. Pioggia, *Cittadinanze amministrative*, cit.

The next point states the commitment to facilitate and support seamless, secure and interoperable access across the EU to digital public services designed to meet people's needs efficiently, including, in particular, digital health and care services.

Comparing the rights defined in the European Declaration with the Italian law framework, the Declaration seems to echo the choices that have been made in Italy also with reference to digital citizenship, which however has its explicit legal recognition through the "Digital Citizenship Charter"[25], to be placed within the framework of the constitutional principles of good performance of public administration (art. 97, Italian Constitution) but also of information rights (art. 21, Italian Constitution). According to the Digital Administration Code (DAC), anyone has the right to use, in an accessible and effective way, the solutions and tools provided by the same Code, also for the purposes of exercising rights concerning access and participation in administrative procedures, in relation with the public administrations (art. 3, DAC).

This recognition must be read as complementary to the obligation that establishes the so-called principle of digital priority, or "digital first" or even "digital by default", according to which the Italian State, the Regions and local authorities ensure the availability, management, access, transmission, conservation and usability of information in digital forms and organize and act for this purpose using information and communication technologies in the most appropriate and in the most suitable ways, to satisfy the interests of the users (art. 2, c. 1, DAC). This perspective is completed by the right of anyone to use services provided by the public administrations in digital modes and in an integrated way, through the services made available by the public administrations; moreover, these services must be organized and updated on the basis of a prior analysis of the real needs of the users (art. 7, DAC).

Furthermore, once again in a similar way to the Italian solutions[26], the European Declaration indicates some essential tools through which the

25. D.lgs. n. 82/2005, Codice dell'Amministrazione Digitale, CAD, sezione II "Carta della Cittadinanza Digitale" – Digital Administration Code, DAC, Section II, "Digital Citizenship Chart". The Code does not provide a definition of digital citizenship, which however can be inferred from articles. 3 and 11 and the set of digital tools contained in the same section, according to an affirmation of digital citizenship strictly connected to the tools developed from time to time and progressively integrated into the digital administration, especially digital identity.
26. See again M. Caporale, *Dalla smart citizenship*, cit.

digital transformation of public services must take place in the digital decade and that is, in summary: digital identity; reuse of public data; digital health.

The idea of a sphere of rights to be recognized and promoted online is therefore supported, both at an Italian and European level, in general and in particular in digital public services, and that, for the realization of these rights, it is necessary to create specific digital tools, to be implemented in all European countries in compliance with the principles established by the Declaration itself. The mentioned tools and services are the subject of various regulatory interventions, which are currently underway for all the areas considered[27].

III. CONCLUDING REMARKS. EUROPEAN DIGITAL ADMINISTRATIVE CITIZENSHIP. RIGHTS AND DUTIES

Digital citizenship therefore arises, in the proposed reading, in the relationship between public authorities and people as a corollary of administrative citizenship, including European administrative citizenship, made necessary by technological evolution.

But, if the digital dimension is considered as an attribute, an element capable of strengthening European citizenship, in which the recognition of European administrative citizenship is placed, it is important to underline that, precisely for the digital dimension, an essential element is missing. In fact, like any legally defined citizenship status, European citizenship should also express a dimension of rights but also of duties.

On the other hand, the general provision contained in the art. 20 TFEU ("citizens of the Union enjoy the rights and are subject to the duties provided for in the Treaties") as a matter of fact has remained isolated, given that the

27. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final). A provisional political agreement was reached between the Council and the European Parliament on the original text, and therefore some proposals for amendments to the draft regulation, *https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/it/pdf*; for the reuse of public data, see Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and re-use of public sector information (recast) but also on data Governance Act, Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 relating to European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation); for digital health, see the Proposal for a Regulation of the European Parliament and of the Council on the European health data space, COM(2022) 197 final of 3 May 2022.

Treaties do not cite any specific duties for citizens. Nor is it enough to invoke, for transversal coverage, the Charter of Fundamental Rights of the European Union, which in the Preamble (and therefore not in the binding part) affirms the indivisible and universal values on which the Union itself is founded, places the person at the centre of its action by establishing citizenship of the Union but also specifies that the enjoyment of the rights guaranteed by the Charter "gives rise to responsibilities and duties towards others as well as the human community and future generations".

Reflecting this characteristic of European law, the European Declaration also lacks any identification of duties that integrate the provision of recognized and promoted rights, also towards public administrations.

It may be considered unpopular, in the specific context of digital citizenship, to talk about duties, given the complexity of the digital transformation and the various existing divides, and therefore the burden of change, which is often, in some way, borne by citizens.

Considering, however, that European citizenship rights cannot, evidently, ignore the duties envisaged by national administrative citizenships, we can refer to the solution adopted by Italian legislation, according to which private individuals must respect the DAC and the related Guidelines concerning electronic documents, electronic signatures, document reproduction and conservation, digital domicile and electronic communications, digital identity - in short, the digital tools identified by the "Digital Citizenship Charter" of the DAC itself (Art. 2, co.3., DAC)[28], those same digital tools through which the first realization of digital citizenship passes and on which, to a large extent, the EU is currently intervening with its own regulations and directives.

In any case, outside the rights-duties scheme, in light of the modulation of European digital administrative citizenship, in the various implications associated with administrative citizenship, passive situations are contemplated, borne by citizens, other than duties, such as burdens. It may therefore be unpopular but it is fundamental, in this historical phase, to invoke the burden of citizens who interact with administrations through digital systems, to respect and therefore, in the Italian perspective, to favour, to prefer the use of digital tools and to act responsibly. To therefore become "good digital citizens" by also making themselves available to train in

28. The Italian Declaration of Internet Rights adopted in 2015, however, does not refer to any duty or obligation, even if the commission established to draft it was called the *Commission for Internet Rights and Duties established at the Chamber of Deputies*.

the digital dimension, mainly via tools (and resources) provided by the regulations and on which the Declaration also focuses significantly. We therefore close by returning to those two previously identified dimensions of digital citizenship, one more focused on education and the acquisition of digital skills, which is autonomous but also fully integrates the other meaning, that of a digital administrative citizenship, the European dimension of which we intended to highlight here.

Algorithmic enforcement on cyberspace: legal boundaries of the use of automated content moderation on the European Union legal framework

1Mario Santisteban Galarza*

SUMMARY: I. INTRODUCTION - II. THE GENERAL FRAMEWORK ON ALGORITHMIC CONTENT MODERATION: THE PRINCIPLE OF NO MONITORIZATION AND SAFEGUARDS AGAINST ALGORITHMIC CURATION ON THE DSA - III. AUTOMATED MODERATION UNDER THE DIRECTIVE ON COPYRIGHT IN THE DIGITAL SINGLE MARKET AND ITS COMPATIBILITY WITH THE PRINCIPLE OF NO GENERAL MONITORING - IV. THE PRINCIPLE OF NO GENERAL MONITORING AND THE DSA DUE DILIGENCE OBLIGATIONS

ABSTRACT: The Internet enables the rapid dissemination of unlawful speech, posing the need for new forms of crime prevention. One method of counterfeiting illegal content is relying on private prevention by social media, specifically on algorithmic content moderation. Nonetheless, these algorithmic tools have been criticised for diminishing lawful speech. Accordingly, if some legal frameworks do contemplate the use of algorithmic content moderation, safeguards have been implemented to protect freedom of speech in the digital age. This contribution explores algorithmic content moderation in the European Union legal framework, highlighting some of the key changes presented by the Directive on Copyright in the Digital Single Market and the Digital Services Act.

KEYWORDS: Content moderation; algorithmic filtering; cybercrime; Digital Services Act.

* Investigador Predoctoral, University of the Basque Country.

I. INTRODUCTION

Society has moved to cyberspace, notoriously influencing the way we consume information. The Internet has made a vast amount of information accessible to the public and has turned the public into a potential author of messages and content, creating a model of mass self-communication, in which a vertical flow of information coexists with horizontal communication[1]. However, the Internet, as a "free and borderless" space, is used for criminal purposes, revealing a dark side of this technology[2]. Following the landmark case of the ECHR *Delfy v. Estonia*[3], the Internet enables unlawful speech to be disseminated like never before, worldwide, in a matter of seconds, remaining persistently available online.

With a large part of our activities and criminality shifted to cyberspace, the guardians of the new digital spaces play a role in the persecution of illicit behaviors[4]. States rely on platforms to curate content in a sort of "delegated enforcement"[5]. This type of enforcement, grounded on the technological capabilities of service providers to regulate information flows (*lex informatica*)[6], helps circumvent infringement in cyberspace, but poses democratic problems, specifically the risk of undermining freedom of expression in a society in which citizens massively rely on online platforms to communicate.

These activities, generally referred to as content moderation, have received increasing attention from academics in multiple fields as well as regulators. Platforms have been conceived as a new discourse police, mediating between that content that users share and what ultimately becomes available to the public[7]. Nevertheless, content moderation activities are difficult to undertake, mainly because of the high volume of content to be reviewed. As Gillespie notes "The immense amount of the data, the relentlessness of the violations, the need to make judgments without demanding that human

1. M. Castells, *Comunicación y poder*, Barcelona, Alianza Editorial, 2016.
2. J. Clought, *Principles of cybercime*, Cambridge, Cambridge University Press, 2010.
3. ECHR, Delfi As v. Estonia, (Application no. 64569/09).
4. F. Miró Llinares, S.D. Johnson, *Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace*, in Gerben J.N. Bruinsma, Shane D. Johnson (eds.), *The Oxford Handbook of Environmental Criminology*, Oxford Handbooks, 2018.
5. M. Husovec, ¿*(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement*, 2021, available online en: *http://dx.doi.org/10.2139/ssrn.3784149*.
6. J. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, *Tex. L. Rev,* Vol, 76, 1997.
7. D. Kaye, *Speech Police. The global struggle to govern the Internet*, Columbia global reports, 2019.

moderators make them, all become the reason why AI approaches sound so desirable, inevitable, unavoidable to platform managers"[8]. The industry, on its own initiative, or in anticipation of possible regulation, has invested and implemented different filtering technologies to deal with harmful content. They enable the reduction of content moderation activities cost, as well as their "emotional" cost, in the sense of the havoc that human moderators face when confronted with illicit content[9].

With the shift to "algorithmic enforcement"[10]platforms have introduced architectural changes that pose a threat to fundamental rights. To put in the words of Husovec these technologies are "technically sophisticated but legally blind"[11]. Due to different shortcomings in its functioning, the quality of the data sets that they are trained on[12], or the lack of capabilities to understand the context of the content, they are likely to detect false positives and affect lawful speech. Moreover, the enable a shift on the processes of online curation, adopting a proactive approach in which filters curate users' speech before content is available[13].

The hazards that automated filtering poses to democratic freedoms have been addressed by European Union's statutes since the enactment of the Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce (ECD). Nevertheless, some new laws and shifts in the jurisprudence present new aspects on the regulation of these systems that must be addressed. This chapter analyzes the legal challenges that algorithmic enforcement poses, focusing on the response of the European Union`s legal framework. Firstly, it references the Regulation (EU) 2022/2065 of 19 October 2022 on Single Market for Digital

8. T. Gillespie, *Content moderation, AI, and the question of scale*, in *Big Data & Society*, 2020.
9. S. Udupa, A. Maronikolakis, H. Schütze, A. Wisiorek, *Ethical Scaling for Content Moderation: Extreme Speech and the (In)Significance of Artificial Intelligence*, 2022, available online at: *https://shorensteincenter.org/ethical-scaling-content-moderation-extreme-speech-insignificance-artificial-intelligence/*.
10. G. Frosio, *Algorithmic enforcement online*, in *Centre for International Intellectual Property Studies Research Paper,* 2020.
11. M. Husovec, *Mandatory Filtering Does Not Always Violate Freedom of Expression: Important Lessons from Poland v Council and European Parliament* (C-401/19), in *Common Market Law Review*, 2023, 173-198.
12. C. Shenkman, D. Thakur, E.J. Llansó, *Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis*, in *Centre for democracy and law*, available at: *https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/*.
13. E.J. Llansó, *No amount of "AI" in content moderation will solve filtering's prior-restraint problem*, in *Big Data & Society*, 2020.

Services (DSA), that limits the deployment of algorithmic tools establishing rules for public and private actors. Secondly, addresses the algorithmization of private enforcement in the field of copyright. Finally, some reflections are made on the new due diligence obligations on the DSA and its links with the principle of no monitorization.

II. THE GENERAL FRAMEWORK ON ALGORITHMIC CONTENT MODERATION: THE PRINCIPLE OF NO MONITORIZATION AND SAFEGUARDS AGAINST ALGORITHMIC CURATION ON THE DSA

The ECD was passed with the aim to foster electronic commerce in the internal market and provide legal certainty to business and consumers. In the view of European Union legislators, the directive did not only strengthen the exercise of economic freedoms but one of the cornerstones of European societies legal frameworks: freedom of expression[14]. This was achieved by introducing liability exceptions of service providers, forbidding Member States to hold intermediaries liable of content provided by the users of their services if they complied with some standards known as safe harbors (article 12 to 14 of the ECD). Alongside these liability exemptions the ECD enshrined the principle of no general monitoring, which prevented States to force intermediaries to monitor the information which intermediaries transmit or store to detect infringements. Both aspects of the framework configure the liability regime of the ECD as negligence-based system in which intermediaries have to act ex post, once the illegal content is notified, and not ex ante, preventing them to screen their services looking for infringements and deploying algorithmic systems to that end[15]. The key principles of the

14. The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.

15. G. Frosio, C. Geiger, *Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime*, in *Eur Law J*, 2023.

ECD have been maintained in the DSA (art. 4 to 8)[16], and the jurisprudence of The Court of Justice of the European Union is still applicable to them[17].

The Court has ruled on article 15 of the ECD (now article 8 of the DSA) on several occasions, highlighting its connection with article 11 of the Charter of Fundamental Rights of the European Union, that protects freedom of expression and information[18]. The first case that is worthy of mentioning is SABAM v. Scarlet (Case C-70/10). The Court analyzed the legality of a Member State court ruling that forced an Internet Service Provider to introduce a filtering system to prevent copyright infringement. In this case, the court found that the injunction not only violated article 15 of the ECD but posed a limitation to other fundamental rights like freedom of information and data protection that was not balanced. The court came to a similar conclusion in Tobias Mc Fadden (Case C-484/14), ruling that an order imposed on a mere conduit service provider that would force to examine all communications passing through an internet connection would not comply with the prohibition of imposing general monitoring obligations.

In Glawischnig-Piesczek (Case C-360/10) made a relevant distinction between a general and a specific duty of monitorization. In this case the CJEU

16. Indeed, the European Parliament in a recommendation directed to the Commission before the Digital Service Act proposal was presented Stressed the need of "maintaining safeguards from the legal liability regime for online intermediaries set out in Articles 12, 13, 14 of the E-Commerce Directive and the general monitoring prohibition set out in Article 15 of the E-Commerce Directive are pivotal for facilitating the free movement of digital services, for ensuring the availability of content online and for protecting the fundamental rights of users and need to be preserved; in this context, underlines that the legal liability regime and ban on general monitoring should not be weakened via a possible new piece of legislation or the amendment of other sections of the E-commerce Directive": *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020IP0272*.
17. Indeed, there was a rejected amendment to article 8 of the DSA proposal that limited the monitorization duties of service providers. The European Parliament wanted to guarantee that "Providers of intermediary services shall not be obliged to use automated tools for content moderation or for monitoring the behavior of natural persons" and that "No general obligation to monitor, neither de jure, nor de facto, through automated or non-automated means" (amendment 139). This amendment was rejected and the DSA sticks with the wording of article 15 of the ECD, maintaining Glawischnig-Piesczeks principles and thus allowing specific monitorization duties that entail algorithmic filtering (recital 30)
18. For a more detailed analyzes see M. Senftleben, C. Angelopoulos, *The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market*, 2020.

analyzed an injunction towards Facebook to remove defamatory comments directed to the defendant. The particularity of this case is that the order did impose a duty to cease any content that was identical to the one which was previously declared to be defamatory. The Court acknowledged that the functioning of social media services posed a "genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user of that network" (n. 36). Taking this into account, attempted to strike a fair balance between both the right to self-reputation and freedom to conduct business[19]. The Court found, that in light of recital 47 of the ECD, the prohibition of imposing general monitoring obligations "does not concern the monitoring obligations in a specific case" (n. 34). Thus, it was held that an injunction that forced it to act against duplicate content stored on the website of the services provider was not precluded by the prohibition of imposing general monitoring obligations. According to the Court, in this case "the monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies" (n. 46)[20].

Regardless of the duties imposed by current statutes on the European Union, platforms monitor users' behavior relaying on automated tools. A quick look to the DSA transparency database or the very large online platforms transparency reports suggests that most moderation activities are automated. These proactivity through automatization is a way of platforms protecting themselves from lawsuits or an anticipation to the movements of

19. As M. Senftleben, M. Angelopoulos outline "The CJEU's approach appears to be based on an interpretation of the prohibition on general monitoring obligations as a reasonableness rule (…) In this way, instead of accepting that the right balance was achieved in Article 15, the Court relies on the need for balance to mitigate the consequences of adopting a definition of 'general monitoring' that is driven (contrary to previous case law), not by the generality of what is being monitored, but by the reasonableness of the monitoring": M. Senftleben, M. Angelopoulos, *op. cit., 14.*

20. "Providers of intermediary services should not be, neither de jure, nor de facto, subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation, in compliance with Union law, as interpreted by the Court of Justice of the European Union, and in accordance with the conditions established in this Regulation. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or a general active fact-finding obligation, or as a general obligation for providers to take proactive measures in relation to illegal content".

legislators[21]. However, it can materially affect the exercise of user's freedoms by over removal of lawful content. With a shift in the philosophy of how to tackle hazards on speech, the DSA establishes procedural freedoms to ensure users rights against content moderation[22], affecting voluntary measures deployed by private actors. This encompasses remedies against algorithmic filtering.

Users that are affected by content restrictions shall be notified about some circumstances that informed the decision. Article 17 of the DSA forces this way to provide for a statement of reasons for the receipt of the service, which must include "the use made of automated means in taking the decision, including information on whether the decision was taken in respect of content detected or identified using automated means". Article 17 forces platforms as well to include the reference to the contractual ground used to justify the restriction and "explanations as to why the information is considered to be incompatible with that ground"[23].

Secondly, users have the right to access an internal complaint-handling system in which they can appeal the automated decision (article 20). Platforms must handle complaints in a non-discriminatory, diligent and non-arbitrary manner, with the possibility of reversing the decision when no infringement of Member states legal frameworks and terms and conditions of the provider is found. It has to be noticed that article 20 pushes platforms to resolve the appeals with "supervision of appropriately qualified staff, and not solely on the basis of automated means". In my view, the DSA shall have prohibited the use of AI to resolve user appeals; given the over-reliance on AI platforms to moderate, internal appeal management systems shall be the place to introduce human review.

Finally, the DSA establishes different transparency mechanisms that affect algorithmic moderation. Intermediaries must publish reports covering any content moderation activities they have undertaken (art. 15). This covers

21. G. Frosio, M. Sunimal, *Monitoring and Filtering: European Reform or Global Trend*?, in G. FROSIO, (ed.), *Oxford Handbook of Online Intermediary Liability*, 2020.
22. P. Ortolani, *If You Build it, They Will Come. The DSA "Procedure Before Substance" Approach*, in J. Van Hoboken et al. (eds.), *Putting the DSA into Practice*, Verfassungsbooks, 2022.
23. This of course is something that does not match well with automated decisions, in which it is not possible to give reasons to support decisions, and only is conceivable a broad explanation on how algorithm logic works. In any case, a quick look at the DSA transparency database, which stores statements of reasons by digital platforms, shows how platforms provide little explanations to support their decisions, only referring to the terms of service with no specific statements regarding the affected content.

"any use made of automated means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes". Regarding large online platforms and search engines the DSA expands this obligation, requiring these intermediaries to publish "the indicators of accuracy and related information referred to in Article 15(1), point (e), broken down by each official language of the Member States" (article 42). Additionally, it is worthy of considering other transparency mechanisms like the mentioned DSA transparency database, which can offer a good picture of the use of automated tools on moderation and data access to allowed researchers under article 40.

Nonetheless, the DSA does not include an obligation to maintain risk management systems or other data governance practices like the Proposal for a Regulation laying down harmonized rules on artificial intelligence by the European Commission. It is true, thought, that the risk mitigation measures contemplated to face system risks (article 34 and 35) could entail some of the safeguards of the AI proposal[24].

In this sense, the work of the Digital Services Board on providing specific guidelines will be crucial in this aspect considering that the proposed regulation on Artificial Intelligence does not characterize algorithmic filtering tools as a "high risk system". Accordingly, services providers that introduce algorithmic filtering do not have to comply with the requirements contemplated on Chapter 2 of the AI regulation[25]. Additionally, there are other gray areas on the DSA that the jurisprudence might help to clear, like the relationship between AI moderation and the structure of intermediaries' liability, that poses some challenges considering the new article 7 and recital 22[26].

24. Linked to this Frosio and Sunimal defend that "the DSA should adhere to the 'human-in-command' principle, ensuring that all decision-making processes fall under human oversight. This principle mandates not just the ability to monitor the AI system's overall activities and impacts, but also the discretion to determine the circumstances and manner in which the system is employed": G. Frosio, M. Sunimal, *op. cit., 40.*
25. In other words, this entails that platforms that deploy automated filtering must not carry out risk management systems, data governance practices, provide technical documentation of the system, program their systems in a way that is transparent to users to cite a few requirements to high risk systems.
26. See M. Barral Martínez, *Platform regulation, content moderation, and AI-based filtering tools. Some reflections from the European Union*, in *JIPITEC,* 2023.

III. AUTOMATED MODERATION UNDER THE DIRECTIVE ON COPYRIGHT IN THE DIGITAL SINGLE MARKET AND ITS COMPATIBILITY WITH THE PRINCIPLE OF NO GENERAL MONITORING

The DSA is a horizontal regulation that rules content moderation, and AI moderation, regardless of the nature of the illegal content that is addressed by courts or other public authorities. If this regulation hinders the development of Member State laws that govern platforms curation duties, the law acknowledges the existence of other sectoral regulations on the EU level relevant to moderation activities that act as lex specialis.

This is the case of the Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights ("DSM-directive"), that attempted to close the value gap on the online digital economy by fostering the proactivity of platforms[27]. The Directive has triggered a heated debate that has gone beyond the legislative process and questions the way that automated moderation shall be regulated[28]. Summarizing a lot[29], the Directive clarifies that online content-sharing service providers (for example, YouTube) perform an act of communication to the public when they give access to the public to copyright-protected works that are uploaded by users (art. 17.1)[30]. This is a departure

27. G. Frosio, *Algorithmic enforcement online*, *op. cit.*, 24.
28. M. Husovec, *Mandatory Filtering Does Not Always Violate Freedom of Expression*, cit., 173-198.
29. To have a better look to article 17 implications on the field of copyright M. Husovec, J.P. Quintais, *How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms under the Copyright in the Digital Single Market Directive*, in *GRUR International*, 2021.
30. Prior to article 17 of the DSM directive the CJUE stressed that "the operator of a video-sharing platform or a file-hosting and -sharing platform, on which users can illegally make protected content available to the public, does not make a 'communication to the public' of that content, within the meaning of that provision, unless it contributes, beyond merely making that platform available, to giving access to such content to the public in breach of copyright. That is the case, inter alia, where that operator has specific knowledge that protected content is available illegally on its platform and refrains from expeditiously deleting it or blocking access to it, or where that operator, despite the fact that it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform, refrains from putting in place the appropriate technological measures that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform, or where that operator participates in selecting protected content illegally communicated to the public, provides tools on its platform specifically intended for the illegal sharing of such content or knowingly promotes such sharing, which may be attested by the fact

from the way the CJEU understood the notion act of public communication, making platforms directly liable for copyright infringements "that are materially committed by users who upload unauthorized content to online services provided by them"[31]. In order to avoid liability, they must seek an authorization from the rightsholders by concluding a licensing agreement. If no authorization is granted, a very likely scenario taking into account that rightsholders are not forced to engage in negotiations with platforms, service providers still can avoid liability if they prove that they have fulfill three requirements:

> (a) made best efforts to obtain an authorizations, and
>
> (b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightsholders have provided the service providers with the relevant and necessary information; and in any event
>
> (c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightsholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b).

The requirement of "high industry standards of professional diligence" has been understood by academia[32] and by the CJEU as an obligation to introduce private filtering to circumvent infringements. The industry before the regulation did indeed introduce filtering tools to counterfeit the availability of copyrighted works on social media. The most well-known example is Google's Content ID system, used for the protection of intellectual property rights on YouTube. Content ID users store their works (consisting of audio, video, or both) in a database, with that database being matched against each new piece of content that is stored on the platform. Once a match is detected, the rightsholders receive a notification and are given the opportunity either to remove the content, obtain revenue from the advertising generated by the respective video or take no action. Google notes that "Content ID can now catch efforts to evade detection like changing a video's aspect ratio, flipping images horizontally, and speeding up or

---

that that operator has adopted a financial model that encourages users of its platform illegally to communicate protected content to the public via that platform" (Joined cases C-682/18 and C-683/18, n. 102).

31. G. Frosio, M. Sunimal, *Monitoring and Filtering*, cit.
32. C. Geiger, B. Jütte, *Platform Liability Under Art. 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match*, in *GRUR International*, 2021.

slowing down the audio. With advancements in machine learning, Content ID can now detect copyrighted melodies, video, and audio, helping identify cover performances, remixes, or reuploads they may want to claim, track, or remove from YouTube"[33].

These systems pose a threat to freedom of expression for several reasons. To put in simple words, if AI tools can detect copyrighted works, they cannot assert whether the use of the work is protected by an exception provided in the legislation. Rightsholders exploit these vulnerabilities on Content ID and flag licit uses of copyrighted works to obtain the income of the videos or delete them[34].

With this in mind, legislators introduced several safeguards to limit the hazardous effects of the statute on users' speech. It claims that the obligations shall be seen "in light of the principle of proportionality", specifically considering "the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service; and the availability of suitable and effective means and their cost for service providers" (article 17.5). Moreover, online content-sharing service providers must put in place an effective and expeditious complaint and redress mechanism to users (article 17.9). The statute claims that "the application of this Article shall not lead to any general monitoring obligation", something apparently contradictory with the regime established on article 17.4 b).

The Regulation was challenged to the CJEU, which had to rule on its compatibility with freedom of expression, enshrined on article 11 of the Charter of fundamental rights of the European Union (Poland v. Parliament and Council, case C-401/19). In line with academia and the Advocate General the CJEU described Article 17 as a *de facto* obligation to introduce filtering tools (n. 54). Considering that the introduction of prior filtering is likely to restrict an important means of disseminating online content, concluded that constituted a limitation to freedom of information and expression (n. 55).

Nevertheless, the interference on freedom of information was found proportional, and subsequently allowed. The CJEU gave different reasons to support the decision (up to six[35]), mainly arguing that the Directive had

33. Google, *How google fights piracy*, 2018, available online at: *https://www.blog.google/documents/27/How_Google_Fights_Piracy_2018.pdf/*.
34. T. Bartholomew, *The Death of Fair Use in Cyberspace: YouTube and the Problem With Content ID*, in *Duke Law & Technology Review*, 2015, 66-88.
35. See for more detail W. Kornelius, *Prior filtering obligations after Case C-401/19: balancing the content moderation triangle*, in *JIPITEC*, 2023, 123.

introduced several safeguards to limit the over removal of legal content such as content protected by copyright exceptions. The Court interpreted the safeguards as an obligation that must achieve a specific result: that the filtering does not prevent the availability of works or other subject matter uploaded by users that do not infringe copyright and related rights. Linked to that, reminds that "the Court has already held that a filtering system which might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications, would be incompatible with the right to freedom of expression and information, guaranteed in Article 11 of the Charter, and would not respect the fair balance between that right and the right to intellectual property" (n. 86).

Nevertheless, it is unclear how a statute like Article 17 can be compatible with the prohibition of imposing general monitoring obligations. From the ruling of the CJUE it can be inferred that the prohibition of general monitoring obligation implies that "the providers of those services cannot be required to prevent the uploading and making available to the public of content which, in order to be found unlawful, would require an independent assessment of the content by them in the light of the information provided by the rightsholders and of any exceptions and limitations to copyright" (n. 90). Interpreting the ruling and trying not to make the principle superfluous, Husovec stresses that what the principle adds is a compulsory way to protect freedom of expression against automatic filtering. In his view, the principle implies that legislators and court cannot impose the introduction of automated filters that cannot autonomously judge the legality of content, making the reliance on other safeguards to avoid over removal not a possibility for compliance[36].

I find more appealing the Advocate General opinion, that links Article 17 to a specific monitoring obligation. In his mind Article 17 only forces to filter content which is "identical or equivalent to works and other protected subject matter identified by rightsholders", precluding the provider to assess the legality of content[37]. Indeed, this is indeed how YouTubes Content ID works: is a system that searches for duplicates of protected works and then relies on the collaboration of rightsholders to identify infringing content once a match is detected. I believe that this is more in line with Glawischnig-Piesczeks ruling, maintaining a reactive model and limiting the filtering

36. M. Husovec, *Mandatory Filtering Does Not Always Violate Freedom of Expression*, cit., 173-198.

37. Opinion of Advocate General Saugmandsgaard Øe delivered on 15 July 2021, Case C-401/19 (n. 201).

to works and content previously identified by rightsholders. The problem is that the mere identification of the protected work is not enough for the filter to work properly since copyright infringement has many nuances and depends on the context of a specific upload[38].

IV. THE PRINCIPLE OF NO GENERAL MONITORING AND THE DSA DUE DILIGENCE OBLIGATIONS

As previously stated, the DSA maintains some of the principles that did characterize the ECD, between them the ban of general monitoring obligations. Nevertheless, the DSA is an example of a second generation of rules for digital services[39], and faces old internet challenges in a novel way. The main contribution of the DSA is establishing a new set of rules that are known as due diligence obligations and that go beyond the issue of liability of platforms for user generated content. Using an "asymmetric system", the DSA establishes risk management obligations to service providers that fall under the category of very large online platforms and online search engines. In this framework, intermediaries must assess the existence of systemic risks that arise for the functioning of their services: the dissemination of illegal content, negative effects on fundamental rights and negative effects on civic discourse, to cite a few (art. 34.1). They shall assert how some factors, such as the design of their recommender systems and any other relevant algorithmic systems, influence these risks. Additionally, they must implement mitigation measures to tackle systemic risks, between them "testing and adapting their algorithmic systems, including their recommender systems" as well as "adapting content moderation processes" (art. 35).

Is clear that one of the measures that platforms will deploy to face systemic risks is to introduce algorithmic filtering to detect and rapidly act against illicit content. This, however, remains as an option, between a set of tools, something that is clear considering the wording of article 35. Thus, if the automatization of enforcement is a way to comply with the DSA is something that public authorities that deal with the act's enforcement cannot impose to platforms.

This follows the experience of the regulatory process of the Regulation 2021/784, 17 of may on addressing the dissemination of terrorist content online. If the text did initially impose filtering to act against terrorist content,

38. C. Geiger, B. Jütte, *op. cit.*, 17.
39. M. w, *Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules*, *Berkeley Technology Law Journal*, 2023.

at least this was the vision of several commentators that criticize the act, the final text approved by the Council and the European Parliament did not include this obligation. Instead, the statute holds that hosting platforms must apply provisions to address the misuse of its services for the dissemination to the public of terrorist content, being the hosting service provider the one that shall choose the type of specific measures to take. Furthermore, the Regulation stresses "that any requirement to take specific measures shall be without prejudice to Article 15(1) of Directive 2000/31/EC and shall entail neither a general obligation for hosting services providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity" and that "Any requirement to take specific measures shall not include an obligation to use automated tools by the hosting service provider" (article 5.7 and 8).

Both the DSA and this regulation take a cautious approach to enforcing the use of this technology. They leave a margin of appreciation in implementing automated tools. I think we should welcome this approach. Platforms are the ones that know better about the suitability of conducting automated enforcement and when these tools are ready to undertake content moderation tasks. Nevertheless, and as we have previously addressed, the DSA, introduces some limitations (procedural guarantees), in the view that this choice of private entities on introducing filters shall be monitored by authorities with the aim to protect fundamental rights.

Nevertheless, the discussions on automated enforcement are far from over in the European Union. Civil society organizations are trying to force a ruling of the Court of Justice of the European Union on the lawfulness of Regulation 2021/784, according to the EU fundamental rights framework and principle of no monitorization of article 8 of the DSA[40]. Additionally, the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse is triggering a heated debate on the use of filtering to detect child sexual abuse material, posing "serious concerns regarding the necessity and proportionality" of the limitations to data protection and privacy rights[41].

40. *https://www.article19.org/resources/france-civil-society-takes-eus-dangerous-terrorist-content-regulation-to-court/*.

41. EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, Adopted on 28 July 2022.

REFERENCES

Barral Martínez, M., "Platform regulation, content moderation, and AI-based filtering tools. Some reflections from the European Union", *JIPITEC*, Vol. 14, 2023.

Bartholomew, T., "The Death of Fair Use in Cyberspace: YouTube and the Problem With Content ID", *Duke Law & Technology Review*, Vol. 13, 2015, pp. 66-88.

Castells, M., *Comunicación y poder,* Alianza Editorial, Barcelona, 2016.

Clought, J., *Principles of cybercime*, Cambridge University Press, Cambridge, 2010.

Frosio, G., and Sunimal, M., "Monitoring and Filtering: European Reform or Global Trend?", in FROSIO, G., (ed.), *Oxford Handbook of Online Intermediary Liability*, 2020.

Frosio, G., "Algorithmic enforcement online", Centre for International Intellectual Property Studies Research Paper, No. 2020-04.

Frosio, G and Geiger, C., "Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime", *Eur Law* J, 2023.

Gillespie, T., "Content moderation, AI, and the question of scale", *Big Data & Society*, 7(2), 2020.

Geiger, C and Jütte, B., "Platform Liability Under Art. 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match", *GRUR International*, Volume 70, Issue 6, 2021.

Google, "How google fights piracy", 2018, Available online at: https://www.blog.google/documents/27/How_Google_Fights_Piracy_2018.pdf/

Husovec, M., "¿(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement", 2021, Available online en: http://dx.doi.org/10.2139/ssrn.3784149

Husovec, M., "Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules", *Berkeley Technology Law Journal*, Vol. 38, No. 3, 2023.

Husovec, M., & Quintais, J. P., "How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms under the Copyright in the Digital Single Market Directive", GRUR International, 70(4), 2021.

Kaye, D., *Speech Police. The global struggle to govern the Internet*, Columbia global reports, 2019.

Kornelius, W., "Prior filtering obligations after Case C-401/19: balancing the content moderation triangle", *JIPITEC*, Vol. 14, 2023. 123.

Llansó, E. J., "No amount of 'AI' in content moderation will solve filtering's prior-restraint problem", *Big Data & Society*, 7(1), 2020.

Miró Llinares, F., & johnson, S. D., "Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace", in Gerben J.N. Bruinsma, and Shane D. Johnson (eds), *The Oxford Handbook of Environmental Criminology,* Oxford Handbooks, 2018.

Ortolani, P., "If You Build it, They Will Come. The DSA 'Procedure Before Substance' Approach" in Van Hoboken, J et al, (eds), *Putting the DSA into Practice*, Verfassungsbooks, 2022.

Reidenberg, J., "Lex Informatica: The Formulation of Information Policy Rules through Technology", Tex. L. Rev, Vol, 76, 1997.

Senftleben, M. and Angelopoulos, C, "The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market", 2020, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717022

Udupa, S., Maronikolakis, A., Schütze, H., & Wisiorek, A., "Ethical Scaling for Content Moderation: Extreme Speech and the (In)Significance of Artificial Intelligence", 2022 Available online at: https://shorensteincenter.org/ethical-scaling-content-moderation-extreme-speech-insignificance-artificial-intelligence/

Local government law

Digitisation of public administration in small municipalities: administrative simplification and equal opportunities

1Elsa Marina Álvarez González*

ABSTRACT: The depopulation of small rural municipalities, under different perspective, represents a relevant problem in Spain as in many other countries, that could be faced with different solution provided by administrative law. The digitalization, also using Artificial Intelligence tools, and a special administrative legal regime based on administrative simplification could represent a very effective institutional response for local administrations facing that kind of problem, beyond the administrative capacity that individual entities can express with their own strength, in the current regulatory framework.

KEYWORDS: Local Government; Depopulation, Artificial Intelligence, Administrative simplification.

I. INTRODUCTION

Depopulation is an extremely complex phenomenon which is linked above all

* Associate Professor in Administrative Law, University of Malaga.

to territorial imbalances and their impact on the organisation and management of land and, above all, on the economy and society. There are various legal options to mitigate the negative effects of depopulation, but we wish to focus here on the impact it has on the people living in these small communities. One aspect we are particularly concerned about is the social inequality that results from living in a particular place. The consequences of this social inequality range from a lack of basic infrastructure, local businesses and employment opportunities, to limited access to information and public services, all of which are accompanied by a significant gender gap. We believe that technological advances can be used to minimise these effects and reduce social inequalities by focusing on digitising the administrations of depopulated municipalities. This process should be seen as disruptive in comparison to previous digitisation policies. It is not simply a matter of digitising access to public services and administrative procedures and investing money to bring the internet and 5G to the smallest communities; it is about truly transforming government and using artificial intelligence (hereafter AI) to ensure access to local public services for all citizens.

II. DIGITAL TRANSFORMATION AND AI IN DEPOPULATED MUNICIPALITIES

Before examining the challenges and benefits of digitising government and using AI to address depopulation, it is worth briefly analysing the current situation regarding digital transformation and the impact of AI on public administration in general.

II.1. DIGITAL TRANSFORMATION AND AI IN PUBLIC ADMINISTRATION: THE CURRENT SITUATION

The digital transformation of public administrations is still a work in progress. This is sometimes due to a lack of technical and economic resources, but more often to the complexity of the project and, above all, to the constant development of new technologies. We had not yet completed the digitisation of the administrative process and the creation and management of documents—so that we could claim to have a proper and effective electronic administration throughout the country—when new technologies and the use of algorithms and AI in the public sector emerged, forcing us to rethink many of the classic approaches of administrative law. It is therefore clear that the digital transformation of public administrations still has a long way to go[1].

1. See in this respect the work of Professor E. Gamero Casado, *La transformación digital de la administración autonómica andaluza*, in F. Castillo Blanco (ed.), *Las políticas de*

However, we must also remember that the implementation of AI in public administrations improves their performance and allows them to open up new channels of interaction with citizens and businesses in order to achieve better results and greater openness and accountability[2]. The use of data by public administrations through algorithms enables public decision-making and allows them to assess the effectiveness of regulations, the impact of public policies and the efficiency of public services. In short, this is smart governance[3] and with artificial intelligence already being used widely in public administration, we can safely say such governance is well underway.

The digital transformation of public administrations and the use of AI in them pose many challenges. Nevertheless, we need to make a firm commitment to their implementation in order to address the social problems caused by the depopulation of our country, Spain. At present, digital transformation and AI are inseparable in the field of public administration and must go hand in hand. AI can only work in the context of digital or electronic administration. Moreover, the impetus given by public authorities to the implementation of AI and the digital transformation of public administrations can be seen in the actions and initiatives launched in recent years.

For example, at EU level, we can highlight, among others, the European AI Strategy 2018, adopted by the European Commission in its White Paper on AI in 2020. The strategy puts people at the centre of AI development and promotes the use of this powerful technology to help solve the world's biggest challenges: from treating diseases, fighting climate change and predicting natural disasters to making transport safer, fighting crime and improving cybersecurity. Meanwhile, the White Paper aims to lay the foundations for Europe's technological leadership, with a high-quality digital infrastructure and a regulatory framework based on its core values, to become a world leader in innovation in the data economy and its applications.

---

buen gobierno en Andalucía, Ed. Instituto Andaluz de Administración Pública, 2022, 23-42.

2. A. Cerrillo I Martinez, *Datos masivos y datos abiertos para una gobernanza inteligente*, in *El profesional de la información*, n. 27/2018.

3. A. Cerrillo I Martinez, defines smart governance in the introduction to the book he coordinated, *La transformación digital de la administración local*, Fundación Democracia y Gobierno local, 2021, 20, as a new management model based on the intensive use of data and greater collaboration between public administrations, citizens and companies through the use of ICTs.

This regulatory framework is set out in the proposal for a Regulation presented by the European Commission in April 2021, which lays down harmonised rules for AI and, subject to adoption, is expected to enter into force in 2023. The proposal regulates AI systems to maximise the benefits they can bring, while preventing and minimising their risks, in a way that is consistent with the EU's values and principles. It sets out certain preventive control measures for AI systems and promotes their use in a safe and ethical manner by establishing a set of rules aimed at mitigating certain risks and negative consequences. A normative model has been chosen to regulate AI, which includes various techniques of administrative intervention. It combines the total or partial prohibition of certain activities in order to avoid risks (in accordance with the precautionary principle) with a system of authorisation (preventive control) and a posteriori control (civil and, where appropriate, criminal liability of those who cause damage using this risk-creating technique). This is accompanied by a system of inspections, normally carried out at the request of victims, to help them and the courts detect and prove illegal behaviour[4].

We will have to wait for its adoption to see what the final text will look like. Once approved, there will be a harmonised regulation of AI systems across the EU. However, we believe that a regulatory model based on risk and certification to ensure transparency does not in itself protect the digital rights of European citizens, which we believe are significantly weakened in the European regulation. More needs to be done to regulate AI and its impact in order to achieve the technological leadership that Europe aspires to.

At the national level, several measures have been implemented, although we still do not have a regulatory standard on AI. We would like to highlight, for example, the approval in 2019 of the Spanish R&D&I Strategy on Artificial Intelligence as a key element for the development of the Coordinated Plan on Artificial Intelligence, which was approved by the European Commission at the end of 2018. This strategy is included in the framework of the SDGs, as set out in the Action Plan for the implementation of the 2030 Agenda in Spain. Its main objective is to make the instruments for promoting R&D&I more effective, and to identify how and where different technologies can contribute to Spain's growth. Among the issues it addresses are personalised medicine, the digitalisation of tourism services, the challenges of cybersecurity and an interoperable and digital public administration.

4. This was pointed out by Professor A. Huergo Lora, *El proyecto de Reglamento sobre la Inteligencia Artificial*, published in the blog *El Almacén de Derecho*, 17 April 2021 (*https://almacendederecho.org/el-proyecto-de-reglamento-sobre-la-inteligencia-artificial*).

In addition, and as a result of the above strategy, the National Strategy for Artificial Intelligence (hereafter ENIA for its Spanish acronym) was approved in December 2020 to coordinate and align state investments and policies. This will improve synergies and facilitate public and private investment to promote the use of these technologies in our society and economy. In line with the Digital Spain 2025 Agenda, it addresses four major social challenges for AI that we wish to highlight: closing the gender gap; promoting the transition to a greener future and reducing our carbon footprint; promoting the territorial structuring of the country to achieve regional governance and ensuring that all levels of government, from national to local, benefit from digitisation and the development of artificial intelligence; and finally, reducing the digital divide.

The ENIA is undoubtedly an important step forward in the development and implementation of AI in our country. It is a much-needed and ambitious commitment that requires a profound economic and social transformation. In the field of public administration, a preliminary step still needs to be taken: its complete digital transformation. In this regard, it is worth highlighting the entry into force of Spanish Royal Decree 203/2021 of 30 March, which approves the regulation on the operation and functioning of the public sector by electronic means. This regulation, which is included in the Digital Spain 2025 Agenda as part of the "digital transformation of the public sector" strategic axis, has four main objectives: a) to improve administrative efficiency; b) to increase transparency and participation; c) to ensure user-friendly digital services; and d) to improve legal certainty.

Other important instruments are the Spanish Digitisation Plan for the General State Administration (2021-2025) and the National Digital Skills Plan. The former aims to promote digitisation so that 50% of digital public services can be delivered via mobile phones. It also aims to integrate the Spanish national identity card on these devices, improve the user experience of digital administration by simplifying identification systems with biometric technologies, promote common platforms for automated processing and allocate funds to a cybersecurity operations centre. The National Digital Skills Plan aims to achieve a high level of digital literacy across society.

Together with the ENIA, these two plans are coordinated through the Recovery, Transformation and Resilience Plan (hereafter PRTR for its Spanish acronym), the Next Generation European Funds, and Royal Decree-Law 36/2020, of 30 December, which sets out urgent measures to modernise public administration and implement the PRTR. Adopted in June 2021, the PRTR is

based on four strategic pillars: ecological transition, digital transformation, social and territorial cohesion and gender equality. For us, it is noteworthy that the PRTR has allocated 20 billion euros to digital transformation up to 2023, which represents more than 30% of its investments.

The interest of public authorities in digital transformation and AI in public administration is undeniable. However, the implementation of the measures set out in these instruments and whether the financial support allocated to them is sufficient to achieve the objectives set is another matter. In any case, what is important is that these plans and strategies indicate that digital transformation will bring about a profound change in public administration. This involves building a new model of administration based on a new and extensive use of electronic media and new technologies[5]. Such a model must be based on two premises: firstly, the internal transformation of the administrative organisation itself and, secondly, putting the citizen at the centre of administrative action, which means simplifying procedures and designing personalised and proactive public services.

Finally, we would also like to highlight the Charter of Digital Rights as a tool to achieve equal opportunities in depopulated communities, and which is, therefore, of interest for the purpose of our work. The Charter recognises the challenges of adapting existing rights to the virtual environment. It contains a set of principles and rights to guide future regulatory projects and public policies to ensure the protection of individual and collective rights in the new digital environment. It is a policy document that provides a roadmap to address the challenge of adapting existing rights to the virtual environment. The Charter does not create new rights, but protects existing rights in the context of digital competencies. Its lack of normative value means that the rights recognised in the Charter are not binding. However, this is not the purpose of the Charter; rather, it is intended to reflect the trends and circumstances of our society. In fact, it is a step forward in the digital transformation of public administration, in which citizens must be at the centre, and a guide for the adaptation and development of regulations in the coming years[6].

5. This was also pointed out by A. Cerrillo I Martinez, in the introduction to the book he coordinated, *La transformación digital de la administración local*, cit., 15.
6. In this regard, see the collective work L. Cotino Hueso, *La Carta de Derechos Digitales*, Ed. Tirant Lo Blanch, 2022.

II.2. THE NEED FOR THE DIGITAL TRANSFORMATION OF ADMINISTRATIONS IN RURAL OR DEPOPULATED AREAS

In the process of digitising public administrations, local authorities are often the ones lagging furthest behind. In terms of e-government implementation, given that there are still many municipalities that do not have basic e-government services, such as notification platforms or payment gateways, or that do not really use them when they do have them (especially in the case of notifications)[7], it is reasonable to assume that the extent to which AI tools have been implemented is considerably lower. If we analyse the data on digital transformation in rural or depopulated communities, the implementation of e-government and the use of AI is still at a very early stage[8].

However, as we have seen in the previous section, public authorities have identified the actions needed to reverse this situation. These range from ensuring infrastructures and digital environments, to providing broadband, interoperability, data security and cybersecurity. For citizens, this includes ensuring access through digital identification systems and reducing gender and digital divides through digital literacy training. In this regard, the application of Spanish Royal Decree 203/2021 of 30 March, which approves the Regulation on the Performance and Functioning of the Public Sector by Electronic Means, is key, as it aims to create a fully electronic and interconnected administration by specifying and implementing the use of electronic means established in Laws 39/2015 of 1 October (hereafter LPAC for its Spanish acronym) and 40/2015 of 1 October (hereafter LRJSP for its Spanish acronym).

It is clear that implementing these measures will not be quick or easy. At this point, however, we would like to go further and consider the impact that AI can have on small communities. There are already a number of interesting applications of AI, especially in public services such as transport, security, health, social services and education. It is also being

7. E. Gamero Casado, *La transformación digital de la administración autonómica andaluza*, cit., 28.

8. See in this respect the report *Informe IRIA sobre las Tecnologías de la Información y las Comunicaciones en las Administraciones locales de 2021* published in the Observatorio de Administración Electrónica: (*https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/pae_Informes/pae_InformeIRIA/pae_InfDescripcion.html?urlMagnolia=/pae_Home/pae_OBSAE/pae_Informes/pae_InformeIRIA.html#.YywipS8lNhA*) and the report of the Court of Auditors on the state of implementation of e-government in municipalities of February 2022.
(*https://www.tcu.es/repositorio/72fc660c-bb74-4606-bac5-3ae27b81b2db/I1466.pdf*).

used in traffic management and to personalise public services by analysing citizens' personal data and the behaviour of other users through profiling. Implementing these tools in depopulated communities would, we believe, contribute to ensuring equal opportunities and citizens' access to public services.

This is a complex and costly process that requires the full digitisation of rural or depopulated administrations. However, we believe that in order to combat depopulation, we need to develop a medium-term action plan in this area. We are also convinced that in municipalities with such a small number of inhabitants, the introduction of computer systems and the development of the algorithms needed to personalise public services will be less costly and more feasible than in large municipalities.

The aim would be to apply the idea of a smart city or smart territory to small municipalities on a smaller scale[9]. There is no clear definition of the term, but all proposed definitions agree that it refers to the use of new technologies to create a more agile, modern and citizen-friendly administration[10]. Smart towns or smart rural areas would be communities that use new technologies to collect and analyse data from the community in order to provide inclusive, efficient, resilient, sustainable and people-centred services[11]. This is essentially another way of describing the digital governance that we have been calling for in these depopulated areas or areas at risk of depopulation.

In order to achieve this, of course, a strategy needs to be drawn up in which the model is designed and planned on the basis of the characteristics of the municipality. Local urban agendas (or, in our case, rural agendas, of which there are already a number) currently provide a good opportunity for

9. See S. De La Sierra, *Los procesos de transformación digital, ¿las brechas y la lucha contra la despoblación ¿Hacia una procura existencial digital?*, in C. Navarro, *Despoblación, Territorio y Gobierno Locales*, Ed. Marcial Pons, 2023.
10. Another interesting proposal is that of 'smart communities', which focuses attention not on the territory (where the term 'city' is used, or 'territory' if it is a supra-municipal space or one that aggregates several population centres) but on the means (use of ICTs) to achieve this efficient and sustainable management of cities. See in this regard M. Almeida Cerreda, D. Santiago Iglesias, Las smart communities: un instrumento para alcanzar, de forma planificada y concertada, el equilibrio en la distribución espacial de la población, in *Revista Cuadernos de Derecho Local*, n. 56/2021.
11. Adapting the definition of smart city provided by A. Cerrillo I Martinez, in *La transformación digital de la administración local*, cit., 143.

this)[12] [13]. Furthermore, provincial councils have an important role to play in the digitisation process of rural administrations, as they need to compensate for the lack of resources, capabilities and skills to undertake the digitisation of depopulated municipalities by supporting and cooperating with small municipalities, as they have done in the past[14].

In this planning process, which is crucial for the design of the smart small municipality model, the difficulties of integrating AI into administrative activities (no different from those faced by other public administrations) will have to be addressed. The main challenge is how to provide legal certainty for the application and use of AI in rural public administrations. Various ways of providing legal certainty through regulation for the use of AI in public administration have been suggested. These include self-regulation by the designers of the IT processes themselves, the adoption of an entirely new regulatory framework, or the adaptation of existing regulations. We are aware that with the current development of AI in our country, the application of current regulations could raise some issues, as they are not adapted to the new technologies. However, by adapting their provisions to this new situation, we believe that the principles governing the actions of public administrations would be fully applicable and would guarantee the use of AI in compliance with the legal system and with full respect for fundamental rights.

To this end, there are several key issues that need to be highlighted, as we have already mentioned in another paper[15]. First, we need to distinguish between the role of each application or use of artificial intelligence, i.e. the algorithm, in administrative action. In this respect, we can distinguish between predictive and non-predictive algorithms[16]. Secondly, it is

12. This is the case of the Sustainable Rural Agenda of the province of Segovia or the Urban and Rural Agenda of Gea de Albarracín, a Spanish municipality with 400 inhabitants.
13. Similarly, C. Campos Acuña, *La digitalización de los procedimientos en los gobiernos locales: una tarea pendiente*, in *Cuadernos de Derecho Local*, n. 58, 108.
14. In the same vein, A. Cerrillo I Martinez, *La digitalización en los gobiernos locales intermedios y la contribución al Plan de Recuperación, Transformación y Resilencia*, in *Cuadernos de Derecho Local*, n. 58, 109.
15. E.M. Álvarez González, *La función normativa y la técnica legislativa en España. A new tool: artificial intelligence,* Ed. Tirant Lo Blanch, 2021.
16. There are algorithms that translate a legal regime to facilitate administrative decision-making and administrative action, but do not influence its content (e.g. programmes that help to pay a tax, calculate a subsidy or a pension). There are also those that are used to mechanise or automate regulated processes without changing the legal framework, but where the process is so complex that it cannot be replicated without the algorithm, so that it cannot be disregarded when it comes to controlling the administrative action

important to avoid bias in both data and algorithms, so that decisions do not discriminate against any person or group of people. To avoid this, it is necessary to improve the quality of data, to design algorithms in a way that takes into account possible discrimination, and to encourage the participation of interested parties and the public at large in the design of algorithms[17]. It is important to emphasise that the doctrine has argued for the need to set up expert committees or other interdisciplinary collegiate bodies, in which society is also represented, to monitor the development of algorithms and, more generally, to assess the impact of artificial intelligence on society or to carry out risk analyses[18]. It is also important to create a register of AI algorithms and systems used by public administrations, together with a system for certifying that the systems comply with the rules and codes in force, and to carry out regular inspections or audits to test the performance of the algorithms[19].

Thirdly, the principle of transparency in the use of AI in public administrations must be guaranteed[20]. This requires removing the opacity that characterises algorithms, to the extent that they are even referred to as

---

and verification of how it has worked is necessary. Other algorithms, however, help to steer administrative action in a certain direction and, unlike the previous ones, provide their own decision-making elements. These are predictive and represent artificial intelligence in the strict sense of the word. At present, this type of model is used (without regulatory approval) to support decisions to initiate procedures. The danger of using these algorithmic models is limited to the extent that, in the absence of an algorithm, these decisions would, in practice, not be subject to legal control (they are not administrative discretionary acts, but informal acts or procedural acts). A. Huergo Lora, *Una aproximación a los algoritmos desde el Derecho administrativo*, in A. Huergo Lora, G.M. Diaz Gonzalez, (eds.), *La regulación de los algoritmos*, Ed. Aranzadi, 2020, 68 ff.

17. A. Cerrillo I Martinez, *El impacto de la inteligencia artificial en el Derecho Administrativo, ¿nuevos conceptos para nuevas realidades técnicas?*, in *Revista General de Derecho Administrativo*, n. 50/2019, 16.
18. See in this regard D. Canals Ametlller, *Incidencia del avance tecnológico en el derecho público (elaboración, práctica, docencia e investigación)*, in B. Puentes Cociña (ed.), *El derecho ante la transformación digital: oportunidades, riesgos y garantías*, 2019, 31-50.
19. This is reported in O. Cortes, *Algoritmos y algunos retos jurídico-institucionales para su aplicación en la Administración pública*, in *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, n. 18/2020, 59.
20. In this regard, Merchán Murillo points out that the use of AI by public administrations will require reconciling the principle of transparency and publication of administrative documents with the protection of personal data and the right of individuals to privacy, under a clear and explicit regulatory framework: A. Merchán Murillo, *Artificial intelligence and blockchain: legal challenges in parallel*, in *Revista Española de Derecho Administrativo*, n. 50/2019, 25.

'black boxes'. Because algorithms are technically complex, they are difficult for ordinary people to understand and therefore difficult to access. We believe that administrations should provide access to the content of algorithms, formalise and register the decision to use artificial intelligence (purposes, resources, results, etc.) and, above all, explain how the algorithms work and give reasons for the results obtained. Transparency would be guaranteed if, in addition to the above-mentioned audits, there were also audits showing how the algorithms actually work. Although AI is complex, the principle of transparency means that it must always be possible to justify any decision taken with the help of artificial intelligence that could have a significant impact on people[21].

Fourthly, interoperability between different public administrations is needed, as AI does not understand national, regional or local government. Finally, respect for data protection and privacy rights is essential, and the use of AI must therefore be compatible with the protection of these rights under European and national law.

Having considered all the difficulties and challenges of implementing AI in depopulated communities, we would like to highlight the benefits it would bring to mitigating the effects of depopulation[22]. Firstly, we believe that some AI tools can make a significant contribution to simplifying administrative procedures. Although this issue will be analysed in the following section, we would like to point out here that while it seems clear that AI can facilitate the exercise of regulated powers, its use in the exercise of discretionary powers is less clear. In these cases, the administration assesses

21. In the same vein, A. Merchán Murillo, *Inteligencia artificial y blockchain: retos jurídicos en paralelo*, in *Revista Española de Derecho Administrativo*, n. 50/2019, 12, and G. Vestri, *La inteligencia artificial ante el desafío de la transparencia algorítmica. Una aproximación desde la perspectiva jurídico-administrativa*, in *Revista Aragonesa de Administración Pública*, n. 56/2021, 382. The author argues that the transparency of algorithms should be considered in two ways. On the one hand, there is a clear need to verify that the public administration's choice of algorithm is transparent. Secondly, it is necessary to verify the transparency of the algorithm when it is in operation in the public administration, ensuring that stakeholders can find out how the algorithm makes the decision. The aim is thus to achieve a double level of transparency, which is essential for such an intangible tool as the algorithm. A distinction is therefore made between ex-ante transparency (at the contracting or supply stage of the artificial intelligence system) and ex-post transparency (once the artificial intelligence system has been implemented and is operating).

22. This has been analysed in more detail in our work *El régimen jurídico de la despoblación en España. Reforma territorial, transformación digital y valorización del patrimonio natural y cultural*, Aranzadi, 2023.

or considers different rights, properties or interests that should be excluded from the AI, so that they cannot be replaced by an algorithm, even if it is technologically possible to do so. However, this is an issue that needs to be reviewed soon, as it seems that such a strict application of the precautionary principle in automated administrative actions may conflict with the principle of effectiveness.

Meanwhile, there are many regulated procedures that could be simplified through AI, at least in depopulated municipalities, which would significantly reduce the difficulties and obstacles that citizens face in their electronic relations with public administrations in these areas. In addition, we believe that it would facilitate the relationship between citizens and public administrations and, above all, benefit the delivery of public services, as we will see in the following sections.

III. ADMINISTRATIVE SIMPLIFICATION AND BURDEN REDUCTION IN DEPOPULATED MUNICIPALITIES

A second factor directly related to digital transformation as a means of combating depopulation is the need to urgently introduce effective administrative simplification in small municipalities. This will lead to a reduction in the number of administrative procedures, using AI tools as mentioned above.

Regulatory and administrative simplification for small municipalities is a cross-cutting objective included in the general guidelines of the *Estrategia Nacional frente al Retorno Demográfico* (National Strategy to Confront the Demographic Challenge) (approved in 2019) and the *Plan de Medidas Ante el Retorno Demográfico* (2021- 2023) (Plan of Measures to Address the Demographic Challenge), approved in March 2021. We believe that small local authorities should be granted a special administrative regime based on administrative simplification. By administrative simplification in small municipalities, we mean the actions of public administrations aimed at lessening the administrative burdens that reduce or hinder the exercise of rights by citizens.

III.1. PROPOSALS FOR THE SIMPLIFICATION OF PROCEDURES

The introduction of e-government is undoubtedly the key instrument for administrative simplification, since its proper implementation implies significant cost savings. The LPAC and the LRJSP contain numerous measures

aimed at simplifying and generalising e-government, as they constitute the two pillars on which its main innovations are based. In addition, in recent years the devolved regions have adopted regulations aimed at simplifying administration and reducing administrative burdens.

In any case, we believe that, despite the efforts made by the public administrations, we have not managed to achieve real administrative simplification, which is essential in order to combat depopulation. A thorough analysis of the administrative procedures in force is needed, and efforts must be made to simplify those procedures that involve the recognition of citizens' rights, as this is the way to avoid the digital divide and guarantee equal opportunities. The exercise of rights cannot depend on whether or not citizens initiate a (mostly electronic) procedure, which can often be very complex for people living in a sparsely populated municipality. Moreover, this presupposes that people have access to the information and are aware that they can apply for recognition of this right.

Admittedly, this is an enormously complex task, especially with regard to the administrative process, given the role it plays in guaranteeing citizens' interests and rights. It is therefore important to strike a balance between the principles underlying the need to simplify administrative procedures and the functions they perform[23].

The simplification of administrative procedures for small municipalities should be approached in a structural way, by selecting the procedures that can be simplified and planning how this can be done. It is important to emphasise that the focus should be on those regulated procedures that are most common in these municipalities and that the simplification process should follow some general criteria. Among these, we wish to highlight:

a) The unification or elimination of procedures.

b) Reducing terms and deadlines as much as possible, while maintaining all the necessary guarantees.

c) The elimination or simplification of formalities that do not add value or delay the procedure, provided that they do not affect the guarantees of the interested parties.

d) Proactivity on the part of the body responsible for the procedure.

23. See C. Cierco Seira, *La simplificación de los procedimientos administrativos en Italia*, RAP, 2000, 387.

e) The creation of models for declarations, reports or compliance tests that facilitate the drafting of mandatory reports.

f) The extension and improvement of procedures for immediate response or automated resolution for the initial recognition of a right or a power and for its renewal or continued exercise; this criterion will be applied in particular to procedures and services in which citizens' claims and demands are resolved after a single contact with the administration or in within a very short time span.

g) The speeding up of communication.

h) Providing guidance to the public.

The aim of simplifying procedures is to reduce the burden on citizens, provided of course that these are not essential for the resolution of the procedure, by eliminating requirements that are not imposed by existing legislation. Documentary simplification is essential to achieve this. We need to eliminate or reduce the documentation required from interested parties and replace them with data transmission or the submission of statements of responsibility. One very helpful approach is to standardise application forms, certificates and similar documents, and to design models that are easier and quicker to fill in, with the minimum data necessary to identify the interested party and, where possible, facilitate pre-completion.

It is possible to imagine a small municipality where people interact extensively with the administration through communications and statements of responsibility; where documents are standardised (forms, declaration models, reports or compliance tests that allow for the drafting of mandatory reports); and where there are immediate response or automated resolution procedures for the initial recognition of a right or power, or for a renewal or continued exercise of the right or power. This would undoubtedly be a major step forward. It could, however, involve some risks, as we believe that the standardisation of documents should never lead to the non-acceptance of an application in a different format, as this would mean undermining the anti-formalist nature of the administrative procedure. Furthermore, the introduction of compliance tests to speed up the delivery of mandatory reports could call into question the reasons that must be given for administrative acts when these reports are binding, since they determine the final content of the administrative act. However, these are risks that need to be addressed in order to minimise their impact.

The work carried out on simplifying procedures should be catalogued and inventoried in a kind of register of simplified procedures for depopulated municipalities. It would include not only the procedure but also the forms established for carrying out the procedures, which would be published on the transparency portal of each municipality. It would have a clear and simple interface, where the search for procedures would be intuitive and all the information and documents (forms, etc.) necessary for each procedure would be provided. This would greatly facilitate the relationship between citizens and the administration.

Nevertheless, the simplification of administrative procedures in small municipalities requires a thorough and obligatory study to ensure that the common principles and criteria we have mentioned can be applied to a fully electronic operation, without prejudice, of course, to respect for the rights of those who are not obliged to interact with the administration by electronic means. Article 67 of Spanish Law 4/2019, of 17 July, on the Digital Administration of Galicia illustrates this, as it establishes the following key principles that the digital procedures and services implemented must respect:

The 'once-only principle': ensuring that citizens provide the same information only once.

Homogenisation: simplify administrative procedures and digital public services through a homogeneous interface, making it easier for people to learn how to use the services and understand the information required of them.

Interoperability: ensuring compliance with technical interoperability standards that allow data and documents to flow between public administrations.

Personalisation: providing customisable digital solutions that are best suited to the needs and characteristics of specific groups.

Security and data protection: compliance with the legal framework on the protection of personal data, privacy and information security and the integration of these elements in the design phase.

Automation: promoting automated administrative actions for acts or actions that can be configured as such in the context of an administrative procedure.

Inclusion and accessibility: designing digital public services to be inclusive and responsive to the needs of groups such as the elderly and the disabled.

Transparency and open government: sharing information and data between public administrations and allowing the public to access, control and modify their own data, as well as allowing stakeholders to monitor administrative procedures that affect them.

Technological adaptation: changing technologies and computer systems so that they are always up to date with technological trends and the technological environment.

Electronic payment: it should be possible to pay electronically for procedures requiring the payment of autonomous community fees.

AI plays an important role in the simplification process. With AI, we will have instant response procedures or automated solutions for recognising a right or power, or for renewing or extending the exercise of a right or power. Citizens' claims will be resolved easily, quickly and with only one direct contact with the administration. Consider, for example, the financial aid available to the inhabitants of a small municipality (aid for the agricultural sector, renewable energies or small local businesses), which could be processed by an algorithm that identifies those who meet the requirements of the regulation and who are then notified of the positive resolution. Of course, this means that the administration must have a set of data on each resident (which it already does in many cases), who will have given prior consent for their data to be accessed. This data must be matched so that the algorithm can identify who meets the requirements. Simplifying procedures in this way would be a radical change to the way things are currently done, and while it could reduce the burden on citizens, it could also increase the burden on public administrations, which in small municipalities have limited staff. In this case, however, local authorities could contract a private company to carry out these tasks.

Another way of simplifying administration, which should be more widespread when dealing with the public administration in a sparsely populated municipality, is self-declaration or self-certification. This takes the form of self-declarations or self-certifications by individuals to confirm certain situations and have been in use in Italy for some time. The instrument replaces the administrative certification of facts or situations with a declaration by the interested party. This significantly reduces the documentary burden of administrative procedures, as individuals are responsible for what they declare and are criminally liable in the event of a false declaration.

Citizen participation in the digital age. A focus on the local level

[1]Manuel Moreno Linde*

SUMMARY: I. TOWARDS A MORE PARTICIPATORY DEMOCRACY - II. CITIZEN PARTICIPATION AND THE COMMUNICATIONS REVOLUTION - III. FOCUSING ON PARTICIPATION AND DIGITISATION AT THE MUNICIPAL LEVEL - IV. CONCLUDING REMARKS

ABSTRACT: The citizen participation is a fundamental element for a more democratic governance, also for local government. Local authorities are particularly open to development and innovation in participation, also using ICTs. In Spain currently there is a broad regulatory framework that allows local governments to use of a variety of instruments to involve citizens in the decisions making process, but in most cases the use of citizen participation instruments is still limited.

KEYWORDS: Citizen participation; Local Government; Digital Transformation; Participatory Democracy.

I. TOWARDS A MORE PARTICIPATORY DEMOCRACY[2]

Citizen participation can be defined as «a process whereby politically and socially empowered individuals work together, within or outside institutional frameworks, to influence decisions that affect their communities»[1]. This concept is linked to that of 'citizenship', in which the individual is entitled

* Contract Professor in Administrative Law, University of Malaga.

1. J. De Lucio Fernández, *La gobernanza inteligente de las metrópolis y la participación ciudadana*, in *Información comercial española. Revista de Economía,* Monographic issue *Metrópolis, el futuro es ya presente*, 2021, 98.

to a number of rights, including the right to participate as enshrined in the UN Charter of Human Rights[2]. This right is underpinned by popular sovereignty, the pillar on which democratic institutions are based and which must wield sufficient strength to ensure that the consent of all citizens is a determining factor in state actions[3].

In terms of their involvement in public affairs, the profile of today's citizens has changed from that of twenty years ago. Citizens are often seen as unmotivated and disjointed, but they are by no means indifferent to social and economic developments. Despite having disengaged themselves from traditional forums, they are organised, active on social networks, express opinions and demand that public authorities respond to their needs and aspirations[4].

It should also be remembered that the management of public affairs has become more complex as a result of the dramatic increase in the amount of channels through which people have access to information, and the increase in opportunities people have to express their opinions. As a result, the views of governments alone are no longer sufficient to address global problems; the views of citizens must also be taken into account when deciding on solutions.

---

2. Article 21 of the Universal Declaration of Human Rights, adopted by Resolution of the United Nations General Assembly in Paris on 10 December 1948, states the following: «1. Everyone has the right to take part in the government of his country, directly or through freely chosen representatives.
2. Everyone has the right of equal access to public service in his country.
3. The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures».
Similarly, Article 25 of the International Covenant on Civil and Political Rights, also adopted by the United Nations General Assembly by resolution of 16 December 1966 (in force since 23 March 1976), states that:
«Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in Article 2 and without unreasonable restrictions:
(a) To take part in the conduct of public affairs, directly or through freely chosen representatives;
(b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors;
(c) To have access, on general terms of equality, to public service in their country».
3. In this respect, see. A. Naser, A. Williner, C. Sandoval, *Participación ciudadana en los asuntos públicos: un elemento estratégico para la Agenda 2030 y el gobierno abierto*, *Documentos de Proyectos* (LC/TS.2020/184), Comisión Económica para América Latina y el Caribe (CEPAL), 2021, 28.
4. *Ivi*, 26-27.

This is particularly evident in issues such as climate change where in recent years citizens' demands have been channelled through the recently created citizens' climate assemblies, to which we will return later[5].

This situation seems to suggest that we are moving from a representative democracy towards a more participatory one. Participatory democracy can be seen as an evolution of representative democracy, involving greater citizen involvement in public decision-making processes and in monitoring the activities of representatives and those in power. It is a democratic model in which the level of participation is higher than in representative democracy, but lower than in direct democracy[6]. In this respect, the Spanish Constitutional Court has pointed out that the different channels of citizen participation instituted by the ordinary legislator within the framework of its powers, are not strictly speaking expressions of either representative democracy or direct democracy, but instead «belong to a third category known as participatory democracy» (STC 31/2015, 25 February). Moreover, with regard to these mechanisms, the Court has pointed out that «they are not channels designed to ascertain the general will of citizens – in the various areas of the territorial structure of the State – [...] but rather, in most cases, to hear the opinions of sectoral interests of an economic, professional, etc. nature» (STC 119/1995, of 17 July).

Participatory democracy is not a substitute for representative democracy. Indeed, they are mechanisms that must coexist, and public authorities should promote participatory instruments to reinvigorate a democracy that is clearly showing signs of fatigue[7].

In principle, the adoption of a more participatory model of democracy is to be welcomed, since the empowerment of citizens as a whole—which is what popular sovereignty is all about—gives greater legitimacy to the decisions taken by public authorities. However, this benevolent view of participatory democracy conflicts with the liberal model, which is concerned about the negative consequences of a more spontaneous and emotion-driven mass participation[8].

Furthermore, it has been argued that involvement in initiatives to promote citizen participation tends to be limited and unequal. This seems to indicate

5. *Ivi*, 29.
6. J. De Lucio Fernández, *op. cit.*, 99.
7. See S. Fernández Ramos, J.M. Pérez Monguió, *Vox Populi: Consultas populares y procesos participativos*, Thomson Reuters, Aranzadi, 2018, 244-245.
8. C. Rico Motos, *op. cit.*, 29

that the underlying cause of demands for such initiatives is not so much a genuine desire to participate as an expression of dissatisfaction with the performance of representatives. It is also argued that individuals' attitudes towards participation and the democratic model are strongly conditioned by educational, socio-demographic and ideological factors. This argument runs the risk of overestimating the views of those who participate to the detriment of those who do not. There are also concerns about the ability of participatory instruments to produce good decisions in terms of technical efficiency[9].

In addition to these potential problems of participatory democracy from the perspective of representative democracy, there is another: the risk of over-exploitation of the benefits of participatory mechanisms by lobby groups. From a negative perspective, these groups can be seen as catalysts for the specific interests of one group which seeks to influence public bodies in order to advance their own interests, even at the expense of the general interests.

The intervention of such groups in the process of adopting norms or public policies constitutes a deterioration of democracy if it undermines the capacity for genuine citizen participation as a whole[10]. As such, when these groups—whose influence on the functioning of power within the model of representative democracy is unquestionable—impose their interests on the general interest, even when the instruments of participatory democracy are used, the result will be nothing other than frustration and growing dissatisfaction with democratic institutions[11].

9. *Ivi*, 31-32.
10. In this respect, J. De Lucio Fernández argues that «participation is often limited, leading to activist groups monopolising the decisions and interests that are the focus of participatory processes. Frameworks for local participation are often dominated and used by powerful groups to further their own interests, regardless of collective interests. Hence, a small organised group can control the governance process by deliberately excluding other groups»: J. De Lucio Fernández, *op. cit.*, 101.
11. In this regard, Castellanos Claramunt states that «if people think that it is the strong economic powers, with the organisational capacity and influence, that are going to manage the inner workings and intricacies of democracy in the drafting of regulations and the shaping of public policies, then obviously there will be a progressive distancing of citizens from democratic institutions»: J. Castellanos Claramunt, *Lobbies y calidad democrática. La difícil integración de la participación ciudadana en un contexto de presiones e intereses*, in *Participación y calidad democrática*, Tirant lo Blanch, 2022, 240.

II. CITIZEN PARTICIPATION AND THE COMMUNICATIONS REVOLUTION

When discussing participatory democracy, new technologies also need to be considered.

Used properly, new ICTs can undoubtedly contribute to the strengthening of participatory democracy, since by fostering interaction between governments and citizens they promote greater involvement of the latter in decision-making processes, thus enabling more open government. In this respect, when governments use ICTs not only to improve public administration in general (electronic government or e-government), but also with the aim of encouraging citizen participation, they are in effect promoting the transformation to a digital democracy (e-democracy)[12].

The specific benefits of using ICT in the area of citizen participation include:

– Increased access to the public sphere for more sectors of society and thus the fostering of different discourses in decision-making processes. In this way, it is possible to overcome the discriminatory bias of assigning the leading role in such processes to 'professional participation groups', thus alleviating one of the problems mentioned above that can be associated with the use of participatory tools.

– Increased effectiveness and efficiency. The use of ICTs allows for lower costs in terms of time, economics and organisation. With regard to the latter, we have already pointed out that the use of new communication technologies leads to the replacement of traditional organisations (political parties or secondary organisations) which were previously essential for channelling citizen participation. On the positive side, it can be said that ICTs simplify the organisation

12. On the concepts of e-government and digital democracy, see E. García Guitián, *Democracia digital. Discursos sobre participación ciudadana y TIC*, *Revista de Estudios Políticos*, n. 173/2016, 173-174 and L. Cotino Hueso, *Derecho y "Gobierno Abierto". La regulación de la transparencia y la participación y su ejercicio a través del uso de las nuevas tecnologías y las redes sociales por las Administraciones Públicas. Propuestas concretas*, *Monografías de la Revista aragonesa de Administración Pública* no. XIV (on transparency, citizen participation and public administration in the 21st century), 2013, 52-53. The author refers to e-democracy as «the granting of an important role to information and communication technologies in the democratic and participatory processes of liberal democratic systems».

of citizen participation by removing the need for such organisations and replacing them with others created by new technologies.

– Supporting advocacy and voter mobilisation. ICTs enable the transmission of information from advocacy groups (other than lobbies or pressure groups) to potential participants in various participatory processes. This increases citizens' trust in such groups and encourages participation.

– Nevertheless, although participation is the cornerstone of open government and is closely linked to ICTs, government openness should not be based solely on this resource. Rather, it should be seen as a privileged complement to other procedural channels of participation, where the deliberative principle can be more effective, especially at the levels of government closest to the citizen[13].

However, it is important to bear in mind that the use of ICT as a tool to promote civic participation can also have its drawbacks. Some authors have suggested that the use of new technologies does not lead to a significant increase in participation. The fact is that ICTs are only a tool and do not in themselves promote citizen participation. Indeed, their introduction as a tool for citizen participation must be accompanied by active measures to promote their use. In addition, it has been pointed out that the digital divide implies unequal access to participation, which in turn can lead to questions about the legitimacy of participatory processes and a lower quality of participation compared to face-to-face deliberation[14].

The digital divide is the subject of special attention in the Spanish Recovery, Transformation and Resilience Plan[15], of which one of the main axes is the digital transformation of the economy and society. Accordingly,

13. S. Castel Gayán, *Marco normativo e institucional del nuevo derecho de participación y las TIC: análisis desde las experiencias autonómicas*, *Revista de internet, derecho y política*, n. 19/2014, 50-51. In the same vein, De Lucio Fernández states that «technology is a suitable instrument for increasing participation, but it is not enough. To enable citizen participation, it is not just a question of incorporating new technologies and promoting digital governments, but also of providing physical and virtual spaces for citizens to participate in the whole process of proposal, execution and evaluation, preferably through the use of new technologies, but also allowing for other channels»: J. De Lucio Fernández, *op. cit.*, 103.
14. On the effects, advantages and disadvantages of the introduction of ICTs in the field of citizen participation, see. E. García Guitián, *op. cit.*,180-181 and S. Castel Gayán, *op. cit.*, 58.
15. The Plan was approved by Agreement of the Council of Ministers on 27 April 2021.

the Plan is based on the premise that a resilient society must be able to cope with the challenges and opportunities of the future, including, as we have said, digital transformation. In this context, the implementation of a National Digital Skills Plan, through component 19 of the Recovery Plan, aims to strengthen the digital skills of the population as a whole and ensure digital inclusion, so that everyone can use digital technologies correctly and independently.

The problem of the digital divide is also addressed by the Charter of Digital Rights, an instrument of a non-regulatory and indicative nature, approved by the Spanish government in 2021 within the framework of the Recovery, Transformation and Resilience Plan. Article XII of this document provides public authorities with guidelines aimed at avoiding gaps in access to digital environments. This is achieved through public policies that address possible discriminatory biases in accessing these environments based on existing differences in age groups, levels of autonomy, levels of digital literacy or other personal and social circumstances. The aim of these policies is, therefore, to ensure full digital citizenship and participation in public affairs for all groups at greater risk of social exclusion and above all for the elderly.

Of particular interest for this paper is the fact that the Charter of Digital Rights dedicates Article XVI specifically to the right of citizen participation through digital means. In summary, the provision states that:

- Governments must promote digital environments that allow effective access to public information, transparency, accountability, as well as the proposal of initiatives and the participation of citizens in their actions.

- Any process of political participation carried out by electronic means must guarantee: access to information on the process in question; full transparency and accountability of the actors involved, be they administrations or other types of public or private entities; conditions of equality and non-discrimination in participation, as well as institutional loyalty and accessibility of digital systems for public participation.

- Digital environments for citizen participation must meet high security standards. When procedures involving voting in processes regulated by electoral legislation are carried out in digital environments, security, reliability, accessibility, usability, effectiveness and efficiency must be ensured.

It is worth mentioning the use of social networks as a means of participation in the activities of public administrations.

Social networks are virtual spaces that have emerged as a result of digital transformation. They allow a large number of users to interact and thus they contain a huge amount of information on which public institutions can base their decisions[16]. The presence and behaviour of public administrations in social networks has not yet been regulated by administrative law, so their role in this area is still uncertain[17]. In this regard, Cotino Hueso has suggested various aspects of government intervention in social platforms and networks that should be regulated: the identification of the administrative bodies or units responsible for managing them; the possibility of controlling and moderating the content posted by third parties; the possibility of 'following' or 'friending' individuals in certain networks; and the guarantees for citizens regarding the exercise of these powers[18].

Whatever the case, social networks are a valuable resource for promoting effective citizen participation. To take full advantage of this tool, public administrations must participate in them, not only as mere receivers and selectors of information, occasionally responding to users' queries, but by actively intervening to generate discussions that are truly enriching and enable informed public decisions to be taken that meet citizens' needs and expectations.

However, beyond this institutional use of social networks, and looking at it from a broader perspective, we should point out that the massive use of this technological resource by citizens as a tool for participating in public debates could be detrimental to our democratic system.

At first glance, one might think that because we can easily access information through social networks, they can help create freer, more informed citizens who are able to express well-founded, independent

16. D. Canals Ametller, *Transparencia y nuevos cauces de participación de la sociedad civil en el proceso normativo*, in *Información comercial española (ICE). Revista de* Economía, n. 907/2019, 100.

17. *Ibidem*. However, public administrations have provided staff with several guidelines which, although of a merely advisory nature, give detailed advice on how to act on the networks. For example, it is worth highlighting the *Guía para la comunicación digital para la Administración General del Estado* [*Guide for digital communication for the General State Administration*], which was adopted by a resolution of 21 March 2013, by the Secretariat of State for Public Administrations, and updated by a resolution of 15 June 2022, by the Secretariat of State for the Civil Service.

18. L. Cotino Hueso, *op. cit.*, 83-84.

opinions in online debates, and moreover opinions that are not dictated by large corporate media groups. This concept is far from the truth, as it is based on the false premise that citizens are active seekers of accurate information, wise judges and careful evaluators of the information they receive (and transmit) via the networks, and that they express their opinions after serious consideration of the content. In fact, as Porras Nadales stated «the new 'cybernetic citizen' seems to act more like a spontaneous, heated and passionate egoist or an irreverent and unthinking replicant»[19].

The reality is that social networks have become a huge repository and disseminator of disinformation, much of which is user-generated. Fake news (content masquerading as information that is self-servingly fabricated or falsified to harm a particular political figure or social group) is on the rise, and appeals to emotion are more likely to shape public opinion than objective facts – a phenomenon known as post-truth[20]. As a result, the debates in these forums are far removed from the calm exchanges in which participants enrich each other, and instead become highly fragmented, impassioned and often partisan discussions. The implication is that the quality of democracy in our society is not improved by using this technological resource as a tool for discussion.

The next stage in the process of using technology for citizen participation will be the application of artificial intelligence in this area. It is not our aim to explain in detail what this technology consists of here, nor what its ethical and legal implications are, other than to say that, broadly speaking, the term artificial intelligence is applied to those systems that, through the use of algorithms and data, can perform actions that we would consider intelligent if they were performed by humans, in order to achieve a specific goal[21]. The use of AI in the field of citizen participation involves creating a system capable not only of collecting, but also of processing and evaluating

19. A.J. Porras Nadales, *La democracia en el dedo del ratón*, in *La participación ciudadana como pilar del Estado democrático*", Aranzadi, 2019, 105.
20. On the concepts of fake news and post-truth, see. C. Rico Motos, *op. cit.*, 35-36.
21. See A. Cerrillo I Martínez, *El impacto de la inteligencia artificial en el derecho administrativo. ¿Nuevos conceptos para nuevas realidades técnicas?*, in *Análisis monográfico. Derecho público, derechos y transparencia ante el uso de algoritmos, inteligencia artificial y big data. Revista General de Derecho Administrativo*, n. 50/2019; J. Ponce Solé, *Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico*, *ivi*; European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, titled "Artificial Intelligence for Europe", COM (2018) 237 final.

the contributions made by citizens during a participatory process, and even of making decisions based on the data obtained.

The use of artificial intelligence to manage citizen participation is not a pipe dream. Studies in the US have shown that using computer analysis to process and evaluate citizens' comments and suggestions in regulatory rule-making procedures can help improve government decision-making. This technology is particularly useful in cases where there is mass participation in these processes and the officials responsible for processing them cannot feasibly read and evaluate all the comments posted on social media platforms and networks.

A situation such as this may seem strange to us. However, we cannot rule out the possibility that artificial intelligence could be introduced in Spain, and elsewhere, as a tool for managing the information provided by citizens in public participation processes[22].

III. FOCUSING ON PARTICIPATION AND DIGITISATION AT THE MUNICIPAL LEVEL

Local entities, and especially municipalities, are favourable environments for the application of participatory processes. This is reflected in Article 1.1 of Law 7/1985, of 2 April, on the Regulation of Local Government (Spanish: Ley Reguladora de las Bases del Régimen Local) (hereafter LRBRL), which defines municipalities as «basic entities of the regional organisation of the State and *direct channels for citizen participation* in public affairs, which institutionalise and independently manage the interests of the corresponding communities».

The law itself sets out a number of instruments for citizen participation at the municipal level. Thus, the second paragraph of Article 70 bis[23] regulates the so-called "popular initiative". This provision stipulates that those residents who have the right to vote in municipal elections may exercise their right of popular initiative by submitting proposals for agreements or measures or draft regulations on other matters within the municipal

22. D. Canals Ametller, *El proceso normativo ante el avance tecnológico y la transformación digital (inteligencia artificial, redes sociales y datos masivos)*, in *Análisis monográfico. Derecho público, derechos y transparencia ante el uso de algoritmos, inteligencia artificial y big data. Revista General de Derecho Administrativo*, n. 50/2019 , 16-17. On this issue, see also E.M. Álvarez González, *La función normativa y la técnica legislativa en España. Una nueva herramienta: la inteligencia artificial*, Tirant lo Blanch, 2022, 244-253.

23. Incorporated into the LRBRL by virtue of Law 57/2003, of 16 December, on measures for the modernisation of local government.

jurisdiction. Popular initiative proposals must be signed by a certain percentage of the population of the municipality, which varies according to its size. As such, in municipalities with a population of up to 5,000, 20 percent must back the initiative; in municipalities with a population of between 5,001 and 20,000, 15 percent; and in municipalities with a population of more than 20,001, 10 percent.

These initiatives are debated and voted on by the municipal assembly, without prejudice to the decision taken by the body competent in the matter. In all cases, a preliminary report on the legality of the initiative is required from the secretary of the town council and, if the initiative affects the financial rights and obligations of the town council, a report from the financial controller is required.

It should be emphasised that the provisions set out in this Article of the LRBRL are «without prejudice to the legislation of the autonomous communities in this matter». In fact, the autonomous communities have been enacting laws on citizen participation for some time under the protection of certain second-generation Statutes of Autonomy, which have given new impetus to this issue[24]. In the same way, the municipalities themselves adopt their own regulations on participation, based on the provisions of Article 70.bis LRBRL, the first paragraph of which states that «town councils shall establish and regulate in their organic rules the appropriate procedures and bodies for the effective participation of the inhabitants in matters of local public life, both at the level of the municipality as a whole and at the level of the districts, if such territorial divisions exist in the municipality».

Municipalities now have at their disposal a variety of tools for involving residents in local public affairs, including participatory budgeting (which is already a relatively widespread tool for local citizen participation) and popular consultations. Also worth mentioning among the participatory processes are the so-called deliberative processes, which create a public space for debate in order to identify citizens' opinions and interests and to hear their proposals.

The initiative to develop participatory processes can come either from local government or from citizens (as in the case of popular initiatives

24. See Articles 4.2 and 43 of the Statute of Autonomy of Catalonia; Articles 15.3 and 20.a) of the Statute of Autonomy of Aragon; Articles 1.3 and 9.4 of the Statute of Autonomy of the Valencian Community; Articles 10.1 and 10.3.19 of the Statute of Autonomy of Andalusia; Article 8.2 of the Statute of Autonomy of Castile and Leon and Article 15 of the Statute of Autonomy of the Balearic Islands.

regulated by the LRBRL). In the latter case, regional laws and municipal regulations on citizen participation often lay down various procedural requirements that need to be met in order for the initiative to be validated, such as obtaining a certain number of backing signatures or a justification of the proposal, in addition to the approval of the initiative by a municipal body. Once these formalities have been completed, it would seem reasonable for the local body to implement the participatory process. However, the rules on citizen participation do not always make this clear, which means that the implementation of the citizen-initiated participatory process ultimately depends on the discretionary decision of the competent body[25].

In order to develop these processes, the rules on citizen participation provide for a number of participatory instruments: public hearings, which are set up to hear the proposals of those affected by a particular issue; surveys; participation forums, which allow for discussion, cooperation and drafting proposals for action; citizens' panels, where citizens can respond to consultations presented by the administration; and citizens' juries, which are created as a space for citizens to assess a particular public activity[26].

Among the tools used for citizen participation, there has been a great deal of interest in popular, citizen or participatory consultations. Their aim is to find out through a voting system, what a particular sector or group of people thinks about a specific decision or public policy or, more broadly, about matters of public interest that concern them. Consultation is an ideal mechanism for involving citizens in decisions that affect them.

It should be pointed out that popular consultations can refer to two different instruments of participation: popular consultations with a referendum and consultations without a referendum. The former are regulated by Article 71 of the LRBRL [27] and, in development of this

25. In this respect, see S. Fernández Ramos, J.M. Pérez Monguió, *op. cit.*, 304 and S.E. Castillo Ramos-Bossini, *La ciudad como espacio político: las iniciativas ciudadanas*, in *La ciudad del siglo XXI: transformaciones y retos*, Madrid, Instituto Nacional de Administración Pública, 2020, 137-142.

26. A full and comprehensive study of participatory processes and instruments based on regional regulations, can be found in S. Fernández Ramos, J.M. Pérez Monguió, *op. cit.*, 277-335.

27. This provision states the following: «In accordance with the legislation of the State and the Autonomous Community, when the latter is statutorily empowered to do so, mayors, following agreement by an absolute majority of the plenary and authorisation of the national government, may submit those matters of municipal competence and of a local nature that are particularly important for the interests of the residents to popular consultation, with the exception of those relating to the local Treasury».

provision, by the laws of the autonomous communities approved in this matter. Referendum consultations are a more formal type of consultation in that they require the participation of an electoral body (in this case, that of the territorial scope of the municipality), and the holding of such consultations therefore must comply with the guarantees governing electoral events. As such, they require the authorisation of the Council of Ministers.

Popular consultations without a referendum (participatory consultations in Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations) are a more informal, flexible and faster type of consultation, and therefore better suited to the objective of ensuring dynamic and effective citizen participation.

In any event, as explained in the previous section, the use of ICTs can help to promote participation and for this reason all local participatory processes can (and should) be supported by these technologies[28].

The LRBRL itself refers to this issue in several of its provisions. Article 25.ñ) empowers municipalities to «promote citizen participation through the efficient and sustainable use of information and communication technologies in their municipalities». In addition, the aforementioned Article 70 bis states that «local entities, and in particular municipalities, shall promote the interactive use of information and communication technologies to encourage participation and communication with residents, to submit documents, to carry out administrative procedures, to conduct surveys and, where appropriate, to hold citizen consultations».

The implementation of these technologies is also provided for in regional laws on citizen participation and local regulations.

With regard to regional laws, an example is Law 7/2017 of 27 December on citizen participation of Andalusia, which includes provisions to promote the use of ICT in participatory processes. The obligations the law imposes on Andalusian administrations (including municipalities) in these processes include: establishing «the appropriate means to promote the effective exercise of the right to citizen participation through ICTs, especially by creating interactive spaces in their electronic offices, portals or websites, as well as through the use of electronic voting and polling systems» (Article 9.c); promoting «the use of information and communication technologies

28. In this regard, Cotino Hueso states that «information and communication are the essence of any participatory process and ICTs are ideal for this»: L. Cotino Hueso, *op. cit.*, 54.

(ICTs) among those social groups that find it most difficult to use them»; and providing «alternative channels that guarantee the exercise of their right to participate» (Article 9.d).

With regard to local regulations on citizen participation, we can take as a reference the model organic regulation approved in 2018 by the Spanish Federation of Municipalities and Provinces, which provides a model for the drafting of these regulations by local councils. The model regulation includes a provision on the use of electronic media in participation processes. Thus, Article 6 states that the local council must promote the interactive use of information and communication technologies to facilitate the participation of residents, and that measures will be adopted to guarantee the right of citizens and citizens' organisations to use electronic media to ensure their participation in any of the bodies, means and rights covered by the regulations, with an emphasis on promoting remote participation.

In the specific case of popular or citizens' consultations, the local authorities should enable online voting. In this regard, we have noted above that the Andalusian Law on Citizen Participation requires the administrations of the autonomous community to promote electronic voting and voting systems. Similarly, other regional laws on citizen participation also provide for online voting. These include the Regional Law 12/2019, of 22 March, on Democratic Participation in Navarre (Article 26.3, regarding non-referendum consultations[29]); Law 2/2016, of 7 April, on Local Institutions in the Basque Country (Article 81. 8, on sectoral or limited territorial consultations [30] and Article 82.3, on local open citizen consultations on public policies or decisions[31]); Law 10/2014, of 26 September, on non-referendum popular consultations and other forms of citizen participation (Article 28)[32] and Law

29. The provision states that voting «shall be carried out in person or online, as provided for in the electoral notice».
30. The precept establishes that «the decision regarding the voting system in these processes (paper or electronic system) will correspond to the local entity, which will decide on this according to the characteristics of its population and area, and ensure that all persons with the right to participate can do so with due guarantees».
31. The article states that «the convening local authority, taking into account the characteristics of its population and territory, may arrange for voting to be carried out on paper or online, or both, and shall use all the resources at its disposal to ensure that any person entitled to participate can express their point of view with due guarantees».
32. According to this provision, «participation in non-referenda popular consultations may be carried out by electronic means […]».

12/2019, of 12 March, on popular consultations and participatory processes of the Balearic Islands (Articles 75 et seq.)[33].

In addition, as Fernández Ramos e Peréz Monguió point out, electronic voting methods must guarantee the identification of participants, the non-duplication or multiplication of participation by the same person, secret ballots, the security of electronic voting to prevent the alteration of the number of votes cast and sufficient transparency to allow interested parties to carry out independent monitoring and control[34].

IV. CONCLUDING REMARKS

Given the current trend towards the digital transformation of all types of human activity (economic, cultural, social, etc.), the transition from a purely representative democracy to a more participatory one – with all the problems that this entails, as pointed out in the first section of this chapter – must undoubtedly be based on the resources offered by ICT. The use of these technologies can certainly contribute to improving our democracy by providing more open governments that allow greater citizen participation in public decision-making processes. However, the increased opportunities for participation in the public sphere brought about by these technologies can also have negative sides, including those resulting from the so-called digital divide, as mentioned in the second section.

From a socio-political perspective, we have also noted the paradoxical effect of communication technologies: although citizens now have access to vast amounts of information that would have been unimaginable a decade ago, the fact is that they are no more knowledgeable or willing to participate in public debate. This is because they are not looking for accurate information, but for arguments to support their preconceived opinions, which in many cases they find in sources spreading disinformation. This leads to heated and fragmented debates which do not contribute to the creation of a society that is better in terms of the quality of its democracy, and in fact have the opposite effect.

On a strictly legal-institutional level, we have pointed out that local authorities are the most appropriate bodies for developing participatory processes. We have seen that there is currently a broad legal framework that

33. Article 75.1 of the Law establishes that «participation in citizen consultations can be carried out through electronic or face-to-face voting».
34. S. Fernández Ramos, J.M. Pérez Monguió, *op. cit.*, 229.

allows local governments to use a variety of instruments to involve citizens in the decisions they take; instruments that can and should be supported by the resources of the digital age, as defined by the rules on the legal regime of local entities and on citizen participation.

However, in spite of this comprehensive legal framework, the reality is that since the implementation of participatory processes is left to the will of the local authorities, in most cases the instruments of citizen participation continue to be used in an aesthetic or superficial way. In order to also make progress in the legal field, it is necessary to strengthen the culture of participation, so that the use of these instruments becomes a matter of course and does not depend almost entirely on the commitment of local authorities to citizen participation; in short, to ensure the real and effective participation of citizens in public decision-making processes on issues that concern them.

Tax law

Automated decision making by tax authorities and the protection of taxpayers' rights in a comparative perspective

1Chiara Francioso*

SUMMARY: I. RISKS AND OPPORTUNITIES ASSOCIATED WITH AUTOMATED DECISION MAKING BY TAX AUTHORITIES - II. A COMPARATIVE OVERVIEW OF AUTOMATED DECISION MAKING IN TAX PROCEDURES… - *II.1. …For guidance and early-certainty purposes - II.2. …In taxpayers' selection and tax auditing* - III. REGULATORY CHALLENGES IN THE PROTECTION OF TAXPAYERS' RIGHTS

ABSTRACT: After comparing a sample of artificial intelligence (AI) applications used by the different Countries' revenue bodies, this paper questions the adequacy of the existing and proposed regulatory frameworks. While AI enhances efficiency by identifying abnormal behavior and reducing repetitive tasks, it also raises issues related to legality, transparency and fairness. Automating tax audits with the most up-to-date machine learning tools may yield accurate results that are however difficult to interpret and validate, thereby undermining the administrative duty to state reasons and taxpayers' right to defense. Moreover, since self-learning algorithms learn from the past, AI can perpetuate historical patterns of discrimination due to biased data or training. Regarding the early-compliance phase of tax procedures, AI-powered virtual assistants can advise taxpayers on countless doubts, without stating clear boundaries and rights: therefore, the users might not be aware of the non-binding nature of advice and be audited contrary to favorable responses. With the approaching of the approval of the EU Regulation on AI, challenging its current wording, this study advocates for a robust regulatory framework to strike a fair balance between administrative efficiency and taxpayers' rights.

* Research Fellow, University of Milano-Bicocca.

KEYWORDS: Tax administration; artificial intelligence; legal principles; taxpayers' rights.

I. RISKS AND OPPORTUNITIES ASSOCIATED WITH AUTOMATED DECISION MAKING BY TAX AUTHORITIES

A recent survey on the digital transformation of tax administrations[1] shows that most EU member States use artificial intelligence (AI) applications in tax procedures, mainly to assist taxpayers at an early stage or for risk management purposes.

These technologies are starting to play a pivotal role in taxation, due to the massive collection of data by the administrations, coupled with the apparent mechanical applicability of many provisions. Algorithmic applications, especially those based on machine learning (ML), have proven effective in the cross-checking of vast amounts of data. By promptly detecting anomalies and taxpayers' mistakes, advance analytics relieves tax officers from repetitive and time-consuming tasks, enabling administrations to focus on subtler forms of tax avoidance or evasion. This can also benefit taxpayers in several ways. For instance, they can correct errors in a timely manner with little or no penalty or they can use interoperability to easily access all their data held by public authorities.

As administrations become acquainted with such applications, challenges and risks for taxpayers' rights begin to emerge. Apart from privacy and cybersecurity concerns, the use of AI by tax authorities raises issues of legality and fairness of their decisions.

In terms of legality, if machine learning is involved, the reasoning may not always be straightforward. To borrow a popular metaphor, the most advanced AI applications (particularly "deep learning" models) appear as black boxes that connect input and output data without revealing their inner workings[2]. Statisticians and AI experts have warned about the trade-

1. OECD et al., *Inventory of Tax Technology Initiatives*, 2022, Table TRM3.
2. While the developers of supervised self-learning systems are aware of both input and output, the users – such as civil servants – may be denied access to both the inner workings (which are inherently opaque even to the developers) and the input data. The lack of transparency hampers the ability of public officials to exercise substantial oversight over the system and the ability of the recipient of the decision to understand its rationale. *See*, Amnesty International, *Xenophobic Machines. Discrimination Through*

off between prediction accuracy and model interpretability[3], meaning that accuracy tends to increase at the expense of interpretability. In other words, groundbreaking self-learning tools (e.g., neural networks), easier to train and much more accurate than traditional decision trees, produce results that are difficult to interpret and validate. Thus, their use by tax authorities without sufficient human oversight may conflict with the rule of law, namely by undermining the duty to state reasons and, ultimately, the taxpayer's right to defense.

When it comes to fairness, AI is often endorsed for its neutrality: it is perceived as an asset to any organization because it seems to be able to circumvent human bias and avoid discrimination or preferential treatment based on an individual's or group's characteristics. However, it has been repeatedly pointed out that AI can indeed lead to discrimination based on biased data or training, with a potentially massive reach when compared to human bias[4]. The risk of using AI in criminal investigations and proceedings, in recruitment and in creditworthiness activities is starting to be adequately acknowledged[5]. Yet, the same is not happening with the use of AI by tax administrations[6]. In some cases, biased fraud-detection ML applications have discriminated against thousands of families of certain backgrounds (based on ethnicity or nationality), who have been targeted with false fraud allegations, causing them financial and personal hardship[7].

Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal, London, Amnesty International Ltd, 2021, 26.

3. G. James et al., *An Introduction to Statistical Learning*, New York-Heidelberg-Dordrecht-London, Springer, 2013, 24.
4. See the Italian case law on the algorithms used to assign a school to qualified teachers (Consiglio di Stato, VI sec., December 13, 2019, no. 8472-8473-8474; *Idem*, VI sec., February 4, 2020, n. 881) and the Dutch leading case "*SyRI*" (Rechtbank Den Haag, February 5, 2020, ECLI:NL:RBDHA:2020:865). See also R. de la Feria, M.A. Grau Ruiz, *The Robotisation of Tax Administration*, in M.A. Grau Ruiz (ed.), *Interactive Robotics: Legal, Ethical, Social and Economic Aspects*, Cham, Springer, 2022, § III.
5. Draft Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), position of the European Parliament adopted at first reading on March 13, 2024, rec. 57-59.
6. *Ivi*, rec. 59, according to which "AI systems specifically intended to be used for administrative proceedings by tax and customs authorities as well as by financial intelligence units carrying out administrative tasks analysing information pursuant to Union anti-money laundering law should not be classified as high-risk AI systems used by law enforcement authorities for the purpose of prevention, detection, investigation and prosecution of criminal offences".
7. D. Hadwick, S. Lan, *Lessons to Be Learned from the Dutch Childcare Allowance Scandal: a Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany*, in *World Tax J.*, 2021, 609 ff.

This essay reviews and compares a sample of AI techniques employed by some revenue bodies at different stages of tax procedures with a view to questioning the adequacy of the existing and proposed regulatory frameworks. Challenging the EU current approach[8], it contends that rights and principles at stake in the interaction of taxpayers and administrations are no less important than those affected using AI in other domains such as recruitment and credit scoring. With the approaching of the approval of the world's first comprehensive Regulation on AI ("EU AI Act"), this study stresses the need to strike a fair balance between administrative efficiency and taxpayers' rights.

II. A COMPARATIVE OVERVIEW OF AUTOMATED DECISION MAKING IN TAX PROCEDURES…

Before discussing the current experiences with AI in tax procedures, a few historical notes on the development of AI show how it has always interacted with taxation.

Due to the complexity and apparent mechanical applicability of many fiscal provisions, back in the seventies, one of the first ever developed AI applications was specifically designed for tax purposes. It was an "expert system", called "Taxman", able to classify under the relevant fiscal provision the facts of a given corporate restructuring, so as to detect the right tax treatment[9]. It relied on the translation of fiscal provisions into a complete set of "if-then rules" (knowledge base) and an inference engine using logical inference rules for deduction[10]. Expert systems could solve complex queries efficiently, thereby supporting users in the identification of the relevant rules and automating the more mundane aspects of their job. However, these systems never took off: unable to learn from data, they were limited by the knowledge explicitly programmed into them and often required manual updates to stay relevant[11]. Moreover, the "if-then" logic was nonsuited to represent the often multifaceted reality[12].

8. "EU AI Act" draft, rec. 59.
9. L.T. McCarty, *Reflections on "Taxman": an Experiment in Artificial Intelligence and Legal Reasoning*, in *Harvard L. Rev.*, 1977, 837.
10. E. Alpaydin, *Machine Learning*, Cambridge-London, The MIT Press, 2016, 50.
11. *Ivi*, 51.
12. *Ibidem*.

Building upon Alan Turing's insights into "learning machines"[13], the research on AI has since shifted its focus from the detailed programming of the knowledge bases to the power of data. In other words, instead of providing the machine with a full system of logical inference, developers began to design machines that were "as simple as possible consistently with the general principles"[14] but capable of extracting knowledge from data (e.g., through pattern recognition).

At the core of both approaches lie algorithms. An algorithm is "a finite set of rules that gives a sequence of operations for solving a specific type of problem"[15]. While the first mentioned approach, often referred to as "symbolic", uses a set of fixed rules manually programmed into the machine, the second approach ("non symbolic") learns the rules or improves their performance based on data. The latter is based on "learning algorithms", that is the process of learning or adjusting a function from input data ("unsupervised learning"), input and output data ("supervised learning") or reward signals ("reinforcement leaning"). This paper focuses on unsupervised and supervised learning algorithms that are often employed by revenue agencies.

Given a set of raw input data ("unlabeled"), unsupervised learning is a process that seeks to learn structure in the absence of an identified output[16]. Over the years, revenue agencies have widely used an unsupervised method, called "clustering", to scan businesses and segment them into homogeneous groups, in order to single out comparable taxpayers who – despite having similar features – are far less profitable than average[17]. This technique can be used for taxpayers' selection as well as for automated tax audits and assessments.

In the age of big data, unlabeled data are much easier and cheaper to find than labelled data, making unsupervised methods an asset to any organization[18]. Besides, there may be clusters that no expert could have

13. A.M. Turing, *Computing machinery and intelligence*, in *Mind*, 1950, 433 ff.
14. *Ivi*, 457.
15. D.E. Knuth, *The Art of Computer Programming: Fundamental Algorithms*, I, Reading, Addison Wesley Longman, 1997, 4.
16. *Unsupervised Learning*, in C. Sammut, G.I. Webb (eds.), *Encyclopedia of Machine Learning*, Boston, Springer, 2011, 1009.
17. For some examples, see V. Thuronyi, *Presumptive Taxation*, in V. Thuronyi (ed.), *Tax Law Design and Drafting*, I, Washington, International Monetary Fund, 1996, ch. 12, and P. Pistone, *General Report*, in P. Pistone (ed.), *Tax Procedures: 2019 EATLP Congress*, Amsterdam, IBFD, 2020, 51 ff.
18. E. Alpaydin, *cit.*, 117.

foreseen[19] and those findings may then serve the purpose of labeling data to feed supervised applications for more accurate analyses.

However, there are pitfalls to consider. Firstly, machine learning does gain insights from data, but it only identifies correlations, not causal relationships. Sometimes correlations may be random or based on irrelevant characteristics. Secondly, unsupervised techniques avoid biased results due to biased training (as there is no supervisor involved), but do not prevent biased results due to biased data.

Supervised learning refers to "any machine learning process that learns a function from an input type to an output type using data comprising examples that have both input and output values"[20]. Basically, the machine is trained to find or adapt a function to new data by feeding it pairs of labelled input-output data.

Revenue bodies can employ several different supervised learning methods, ranging from the traditional ones such as "decision trees" to the most advanced such as "neural networks".

A decision tree is a tree-structured supervised model that is easy to understand even by nonexpert users[21]. This model could be used by tax administrations for risk-management purposes (*i.e.* to predict non-compliant behaviors). The system may be trained with a dataset of past audit notices labeled according to selected attributes of taxpayers and their behaviors suggesting a risk of non-compliance (e.g., residents for fiscal purposes vs non-residents; real economic activity vs no economic activity; passive-to-active-income ratio, etc.). Basically, the algorithm divides data into smaller and smaller subsets, based on the attributes of the audit notices that statistically provide the highest categorizing ability. The resulting tree structure embodies the decision rules inferred from the audit notices that can be used to make predictions for other taxpayers having the same input attributes. Thus, once trained, the model will be able, based on those features, to classify taxpayers that have not yet been audited, expressing the probability of their non-compliance, and enabling tax administrations to prioritize them for tax audit purposes. This method handles high-dimensional data well and its reasoning remains easy to interpret[22] because each step can be described

19. *Ivi*, 115.
20. *Supervised Learning*, in C. Sammut, G.I. Webb (eds.), *cit.*, 941.
21. J. Fürnkranz, *Decision Tree*, in C. Sammut, G.I. Webb (eds.), *cit.*, 263.
22. I.H. Sarker, *Machine Learning: Algorithms, Real-World Applications and Research Directions*, in *SN Computer Science*, 2021, 7.

with an "if-then" rule. Its main weaknesses are the long training process and the high exposure to biases.

However, further research showed that, due to the "accuracy vs interpretability trade-off", tree-based methods are not competitive with the best supervised learning approaches in terms of prediction accuracy. Experts developed techniques such as "bagging", "random forests" and "boosting", that involve "producing multiple trees which are then combined to yield a single consensus prediction"[23], because "combining a large number of trees can often result in dramatic improvements in prediction accuracy, at the expense of some loss in interpretation"[24].

Tax authorities are known to use neural network models as well[25]. Neural networks are (supervised or unsupervised) learning algorithms based on a loose analogy of how the human brain functions: "learning is achieved by adjusting the weights on the connections between nodes, which are analogous to synapses and neurons"[26]. They result from the interaction between computer engineering and neuroscience and are composed of multiple interconnected processing units with a fast computation power. Neural networks can learn online, by doing small updates on the connection weights based on new data, without the need to collect a whole database to train the model all at once[27]. Deep learning, *i.e.* neural networks with many layers, has been proving to have a high prediction performance, while requiring less manual interference[28]. However, neural networks, especially when deep learning is involved, tend to learn black boxes[29]: in other words, it is not possible to identify a rule or a set of rules linking the output rendered by the outer layer to the input.

A few attempts are being made to increase the interpretability of neural networks[30], but, given the current state of technology, tax authorities should

23. G. James et al., *cit.*, 303.
24. *Ibidem*. See also I.H. Sarker, *cit.*, 2021, 7.
25. P. Castellón González, J.D. Velásquez, *Characterization and detection of taxpayers with false invoices using data mining techniques*, in *Expert Systems with Applications*, 2013, 1429, according to which neural networks methods were already being applied by the revenue bodies of Canada, US, UK, Bulgaria, Puru and Chile in 2013.
26. *Neural Networks*, in C. Sammut, G.I. Webb (eds.), *cit.*, 716.
27. E. Alpaydin, *cit.*, 90.
28. *Ivi*, 107.
29. *Ivi*, 155, and Z.H. Zhou, *Machine Learning*, Singapore, Springer, 2021, 124.
30. A. Barredo Arrieta et al., *Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI*, in *Information Fusion*, 2020, 82 ff.; B. Kuźniacki et. al., *Towards eXplainable Artificial Intelligence (XAI) in Tax Law: The Need for*

carefully assess the performance of each AI method without losing sight of its interpretability.

II.1. …FOR GUIDANCE AND EARLY-CERTAINTY PURPOSES

Tax administrations employ AI in risk management not only to select taxpayers and prioritize their returns for audit purposes, but also to prevent non-compliance.

This may be done in several ways, which raise different legal issues.

The OECD "Tax Administration" Series highlighted repeatedly that a growing number of administrations have been setting up virtual or digital assistants, such as "chatbots", to help respond to taxpayer enquiries and support self-service[31]. Compared to general rulings published on the administrations' websites, these tools, especially if fueled by machine learning, provide automated yet tailored solutions that enhance guidance services. Besides, they are available all the time, regardless of opening office hours, and proved useful during the pandemic[32].

A recent survey shows that in 2020, among fifty-eight national tax administrations, 72% of them – including those of twenty European countries – were using (60%) or implementing (12%) virtual assistants (e.g., chatbots or voice bots)[33]. The newly established "Inventory of Tax Technology Initiatives" reports that roughly one third of them is rule-based, meaning that interactions with taxpayers follow a set of pre-programmed rules; thus, their answers are easy to interpret but not too accurate. A little less than a third of them uses machine learning, that presumably gives more accurate replies. The remaining part integrates both approaches[34].

The US Internal Revenue Service (IRS) set up voice and chatbots that simulate human conversation and use an AI-powered software to respond to natural language prompts. They are currently unauthenticated, meaning

---

a Minimum Legal Standard, in *World Tax J.*, 2022, 573 ff. See also European Commission, *White paper on artificial intelligence. A European approach to excellence and trust*, February 19, 2020, COM(2020) 65.

31. OECD, *Tax Administration 2022: Comparative Information on OECD and other Advanced and Emerging Economies*, 2022, Paris, OECD Publishing, 79.
32. *Ibidem*.
33. OECD, *Tax Administration 2022*, cit., 79-80.
34. OECD et al., *Inventory of Tax Technology Initiatives*, 2022, Table TT5; OECD, *Tax Administration 2022*, cit., 80.

they cannot answer questions about a specific taxpayer account, but the IRS planned to launch more advanced authenticated bots that would allow access to taxpayers' IRS accounts and be able to set up taxpayer-specific instalment agreements[35]. Currently the IRS "Interactive Tax Assistant" contains a disclaimer warning taxpayers about the fact that they cannot rely on the reply as if it was a private ruling. Therefore, the IRS retains the power to collect additional tax and penalties if taxpayers act in accordance with incorrect answers[36].

Another example is that of Spain, that resorted to a rule-based virtual VAT Assistant when implementing the e-invoicing reform. The virtual assistant is trained on decision trees drafted by IT and legal experts based on frequently asked questions about the e-invoicing system. Like the US bots, the VAT Assistant simulates human conversation thanks to natural language processing algorithms. At the end of the conversation, the taxpayer can rate the answer and send suggestions for improvements[37]. If the rating is negative, taxpayers have the possibility to submit their questions by email to a tax official. The conversations are then audited, and the trees are manually updated and corrected when necessary. Managing taxpayers' expectations is a challenge also for the Spanish tax administration: currently, the automatic replies do not bind the tax administrations, but, if taxpayers act in line with them, they cannot be punished[38].

The same is going to happen in Italy, where a new database is being established to provide automated advice, based on previous guidance, to individuals and partnerships ("*consultazione semplificata*")[39]. These taxpayers will be allowed to submit advance ruling requests only when the new tool will not reach a "univocal answer". Even if a "univocal answer" is obtained, their expectations will not be fully protected: they may be audited in contrast with a favorable solution, but not be subject to penalties[40].

The binding or non-binding nature of automated advice is indeed the most relevant legal issue raised by AI tools at the initial stage of tax

35. *Ivi*, 83.
36. The disclaimer mentioning the exclusion from the protection afforded by sec. 6404(f) of the Internal Revenue Code can be found at *www.irs.gov/help/ita*.
37. OECD, *Tax Administration 2019: Comparative Information on OECD and other Advanced and Emerging Economies*, 2019, Paris, OECD Publishing, 176.
38. *Ivi*, 178.
39. Article 10-*nonies* of the Taxpayer Bill of Rights, as amended by *Decreto legislativo* December 30, 2023, no. 219.
40. Article 10-*nonies*(3) of the Taxpayer Bill of Rights.

procedures[41]. So far, tax administrations have been using disclaimers to warn users of the automatic nature of the response[42] and its non-binding effect[43], in the absence of a statutory solution.

Developers should set up clear boundaries: while stating, as it is often the case, that virtual assistants are intended for easier or routine doubts, they should prevent the systems from replying to more complex questions and refer the case to a tax official. Lawmakers, on their part, should seek the right balance between legality and legal certainty, just like they do when setting up advance ruling systems.

Basically, it should be established whether the user may or may not be audited contrary to the favorable response provided by the AI tool, in order to recover higher taxes based on a different solution. If it was established that taxpayers may be audited, it should also be cleared whether they may be punished, despite being misled by the automated assistant.

A few aspects should be considered.

First of all, the learning method adopted by the AI tool. If the system is run by deterministic algorithms and its reasoning can be expressed by a set of "if-then" rules, it seems proportionate to establish the binding nature of the replies for the administration. However, for the same reasons why expert systems failed, it seems unlikely that purely rule-based virtual assistants will take off.

On the other hand, tools based on cutting-edge technology like neural networks should be prevented from giving binding legal advice. After all, with the sudden growth of popular generative deep learning systems (like "ChatGPT"), everyone has had the chance to witness their "hallucinations", despite realistic results.

Another thing to consider is the "simplexity" paradox, that occurs "when the government presents clear and simple explanations of the law without

41. See G. Ragucci, *Gli istituti della collaborazione fiscale*, Torino, Giappichelli, 2023, 103; F. Farri, *L'attività d'indirizzo*, in L. del Federico, F. Paparella (eds.), *Diritto tributario digitale*, Pisa, Pacini, 2023, 183.
42. OECD, *Tax Administration 2019*, cit., 178.
43. In addition to the IRS and the Spanish tax administration's disclaimers, also the "*Steuerchatbot*" of the Ministry of Finance of Baden-Württemberg warns taxpayers that the tool "is currently still in the pilot stage. It is constantly learning, but it cannot and must not provide you with tax advice" (*https://steuerchatbot.digital-bw.de/steuerbw.html*).

highlighting its underlying complexity or reducing this complexity through formal legal changes"[44]. Rather than achieving simplicity – a perennial goal of policymakers – through legislative reform, research has shown that administrations such as the IRS present disputed tax laws as clear rules and fail to fully explain them, including possible exceptions, often to maximize the revenue[45]. This drawback may be amplified by interactive interfaces such as chatbots. While the efforts to make tax law understandable to the public should be encouraged, it must also be acknowledged that certain simplified interpretations may be detrimental to the principle of legality in taxation.

Even if taxpayers were to be allowed to rely on virtual assistants, they should bear in mind that, as in any advance ruling system, guidance is provided "*rebus sic stantibus*". Therefore, they could still be audited to check whether the facts described are true. Moreover, the assistants' replies may lose their validity because of factual or legal changes, according to the rules on legitimate expectation of each jurisdiction.

To conclude, it should not be overlooked that these automated systems might reshape early compliance in a way that affects taxpayers' rights. For instance, the scope of the Italian provision on advance rulings was recently restricted to questions that may not be addressed through quick response services, including AI-based technologies[46].

There is no doubt that virtual assistants provide basic guidance without the need to wait (weeks or months) for the issuance of a private ruling or for tacit approval. However, the scopes of virtual assistants and private rulings do not overlap. While the first are meant to address easier or routine doubts, advance ruling applications under the Italian legislation must meet the "objective uncertainty" requirement[47]. Otherwise, Italian revenue bodies already have the power to quickly reject those applications[48]. Virtual assistants should rather be seen as replacing more informal communication channels such as calling, emailing or visiting the office.

44. J.D. Blank, L. Osofsky, *Simplexity: Plain Language and the Tax Law*, in *Emory L. J.*, 2017, 263.
45. *Ivi*, 236-237.
46. Articles 10-*nonies* and 11 of the Taxpayer Bill of Rights, as amended by *Decreto legislativo* December 30, 2023, no. 219, based on article 4(1), c), of the Enabling Law for the reform of the tax system, August 9, 2023, no. 111. See in detail V. Mastroiacovo, *Procedimenti accertativi e nuovo rapporto tra fisco e contribuente nella legge delega di riforma tributaria*, in *Rass. trib.*, 2023, 497-498.
47. Article 11(1), a), of the Taxpayer Bill of Right ("*Statuto dei diritti del contribuente*"), Law July 27, 2000, no. 212.
48. Art. 11(4), Law no. 212/2000.

More worryingly, this restriction will only affect individuals and small businesses, while larger businesses' ruling applications benefit from full and direct human intervention, without being filtered by AI tools. It should not go unnoticed that it is individuals and small businesses that are most exposed to the risks of personal data breaches and algorithmic discrimination.

Despite the conclusion that virtual assistants cannot replace advance rulings, on the positive side, AI does not need to be completely ruled out from the assessment of ruling applications.

The responses to past rulings requests retain a high degree of predictive power, especially if dealing with regimes that show recurring factual patterns (e.g., ruling procedures for high net worth individuals). Such predictive potential has been known for decades and sparked a debate in the US that led the IRS to publish its tailored determinations that were once kept secret[49]. Therefore, tax authorities might use smart databases of past responses to address similar new applications and avoid inconsistencies.

II.2. …IN TAXPAYERS' SELECTION AND TAX AUDITING

Unable to audit all taxpayers, tax administrations are constantly seeking effective methods of monitoring non-compliance and selecting taxpayers for audit. Moving away from random audits, they have been testing annual selections of specific categories of taxpayers, parameters and statistics to identify unusual positions and, more recently, AI-based risk-management methods[50].

AI is also being used to gather evidence of tax evasion and to automate – partially or fully – tax assessments.

According to the already mentioned "Inventory of Tax Technology Initiatives", the revenue bodies of sixteen Countries in Europe use artificial intelligence in their risk assessment analyses or to detect tax evasion and fraud[51]. The tax administrations of eleven European Countries report using AI to assist tax officials in making administrative decisions or to make

49. Large law and accounting firms were believed to have developed substantial libraries of written determinations issued to their clients, while ordinary practitioners were disadvantaged because they did not have access to what was perceived as a "body of secret law" (J.P. Holden, M.S. Novey, *Legitimate Uses of Letter Rulings Issued to Other Taxpayers - A Reply to Gerald Portney*, in *The Tax Lawyer*, 1984, 343).
50. See P. Pistone, *General Report*, in P. Pistone (ed.), *cit.*, 50 ff.
51. OECD et al., *Inventory of Tax Technology Initiatives*, 2022, Table TRM3.

recommendations for actions, but only one of them employs AI to make final administrative decisions (Albania). For these purposes, only one of them (United Kingdom) reports having an ethical framework in place for the application of AI[52], while ten of them report having limitations in place, such as the prohibition to use AI to make final administrative decisions.

AI-based risk-assessment methods are widely used in France, Italy and Germany.

France gained a significant experience with the use of data mining algorithms to tackle VAT and personal income tax frauds. After creating a data warehouse that collects all the relevant data from multiple sources that used to be compartmentalized (e.g., tax returns, bank account files, social security data, etc.), algorithms cross-check them, uncovering inconsistencies, and compare them to models of fraudulent behavior[53]. The system does not merely select taxpayers for subsequent audit, but it may send them automatic requests for information when detecting mistakes. They can escape a more in-depth audit by timely correcting those mistakes. Moreover, to counter certain tax violations, a law was passed in 2019 to allow tax authorities, on a trial basis, to collect and use taxpayers' freely accessible content (e.g., on social media or online marketplaces) by means of "computerized and automated processing" (except for any facial recognition system)[54].

52. *Ibidem*. See the guidance on the ethical use of artificial intelligence in the public sector: "*Ethics, Transparency and Accountability Framework for Automated Decision-Making*", May 13, 2021, *https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making/ethics-transparency-and-accountability-framework-for-automated-decision-making*.

53. M. Serrat Romaní, *Big data, artificial intelligence and machine learning in European countries: a compared and practical analysis*, in Á. Antón Antón, C. García-Herrera Blanco (eds.), *Digital transformation of tax administrations in the European Union*, Madrid, IEF, 2023, 99-100; V. Dussart, *L'intelligence artificielle et le data mining au service du contrôle fiscal des entreprises*, in A. Mendoza, Caminade (ed.), *L'entreprise et l'intelligence artificielle. Les réponses du droit*, Toulouse, Presses de l'Université Toulouse Capitole, 2023, 167 ff.; F. Perrotin, *Contrôle fiscal et intelligence artificielle: des résultats prometteurs*, in *www.actu-juridique.fr*, January 20, 2021.

54. Article 154, *Loi n° 1479 de finances pour 2020*, December 28, 2019. Even though this system is based on publicly available data, the *Conseil constitutionnel* (*Décision n° 2019-796 DC*, December 28, 2019) stated that it may entail a restriction of the rights to privacy and freedom of expression. Therefore, its use must remain within limits that are strictly necessary for pursuing its lawful purpose of combating fraud (§ 83). The Council ruled that the provision allowing the use of the web scraping software even when the French administration is aware of the non-submission of the tax return is in breach of the principle of proportionality (§ 94). Proposals to use web scraping tools on social media for tax audit purposes have been made in Italy too (see Ministry of Economy

Italy has recently set up a similar scheme, by making administrative databases interoperable and scanning them with AI algorithms looking for abnormal behavior[55]. Basically, AI traces and extracts models of tax evasion or avoidance from a database of past audits. Data from tax returns, bank accounts and other public databases are then cross-checked and compared to those models[56]. For instance, models may be based on incoherent expenses, compared to income, savings and property. Taxpayers are automatically notified of any errors and can correct their tax returns with only minor penalties. Otherwise, they will undergo a more in-depth audit[57].

Especially when it comes to ML algorithms, one may wonder whether these findings are interpretable enough for taxpayers to accept error correction and for tax officials to conduct a deeper audit without fear of contradicting AI[58]. Previous Italian attempts to use parameters and statistics to directly assess taxes have been rejected for failing to comply with the obligation to state reasons ("*studi di settore*"[59]). Their scope has then been

and Finance, "*Relazione per orientare le azioni del Governo volte a ridurre l'evasione fiscale derivante da omessa fatturazione*", attached to the proposed Council implementing Decision on the approval of the assessment of the Recovery and resilience plan for Italy, December 20, 2021, 34-37; "*Relazione sull'economia non osservata e sull'evasione fiscale e contributiva*" submitted by an expert group to the Ministry for 2022, 127).

55. Article 2-*ter*(2) of the domestic Data protection code (*Decreto legislativo* June 30, 2003, no. 196), as amended by *Decreto legge* October 8, 2021, no. 139, article 9. See also article 2 of *Decreto legislativo* February 12, 2024, no. 13, defining the notions relevant for the automated tax risk analyses.

56. Law December 27, 2019, no. 160, article 1(682-686) and Ministerial Decree of June 28, 2022. See G. Ragucci, *L'analisi del rischio di evasione in base ai dati dell'archivio dei rapporti con gli intermediari finanziari: prove generali dell'accertamento "algoritmico"?*, in *Riv. tel. dir. trib.*, September 4, 2019; A. Santoro, *Nuove frontiere per l'efficienza dell'amministrazione fiscale: tra analisi del rischio e problemi di privacy*, in G. Arachi, M. Baldini (eds.), *La finanza pubblica italiana. Rapporto 2019*, Bologna, il Mulino, 2019, 66 ff.; C. Francioso, *Intelligenza artificiale nell'istruttoria tributaria e nuove esigenze di tutela*, in *Rass. trib.*, 2023, 47 ff.; M. Fasola, *Le analisi del rischio di evasione tra selezione dei contribuenti da sottoporre a controllo e accertamento "algoritmico"*, in G. Ragucci (ed.), *Fisco digitale*, Torino, Giappichelli, 2023, 84 ff.

57. Law December 27, 2019, no. 160, article 1(682).

58. In this respect, the Italian data protection Authority (opinion no. 276, July 30, 2022) expressed serious concerns in relation to the Italian Revenue Agency's Privacy Impact Assessment.

59. The Italian Supreme Court has on several occasions rejected the view that sectoral studies amount to (rebuttable) presumptions of law and could thus automatically justify tax assessments based on mere inconsistencies. A reliable tax assessment that reflects the effective ability to pay may stem from these inconsistencies, but it must be pursued by granting taxpayers the right to be heard (Grand chamber, December 18, 2009, no. 26635-26638). Before and after these judgments, see respectively M.

limited to identifying unusual positions, so as to encourage voluntary compliance or conduct further audit ("*indici sintetici di affidabilità fiscale*"[60]). These techniques are regaining momentum with the recent approval of a new advance compliance program designed to automatically assess direct taxes for the following two years, disregarding actual income ("*concordato preventivo biennale*")[61].

In Germany, following the enactment of the "Taxation modernization act" of 2017[62], tax assessments have been fully automated. Income taxation in Germany is not entirely self-assessed: taxpayers submit, along with the tax return, a "tax assessment proposal", but it is up to the administration to issue the final assessment notice[63]. To manage the great number of tax cases, tax authorities use an algorithmic risk assessment-management system to select those that should be verified by tax officials[64]. This occurs, for instance, in case of implausible relationship between certain variables, past violations or alerts deriving from the international exchange of information or other

---

Versiglioni, *Prova e studi di settore*, Milano, Giuffrè, 2007, 234 ff., A. Marcheselli, *Natura giuridica degli accertamenti mediante studi di settore e "giusto procedimento" tributario: quattro sentenze capitali delle Sezioni unite della Corte di cassazione*, in *Giur. it.*, 2010, 711 ff., and F. Montanari, *Un importante contributo delle Sezioni Unite verso la lenta affermazione del "contraddittorio difensivo" nel procedimento di accertamento tributario*, in *Riv. dir. fin.*, 2010, II, 33 ff. While sectoral studies applied to small and medium-sized enterprises and to professionals, the income of natural persons could be assessed with another presumptive method based on statistics and multiple public databases, "*redditometro*", that is no longer in use [Article 38(5), Presidential Decree September 29, 1973, no. 600; see N. Sartori, *Accertamento sintetico del reddito*, in *Digesto comm.*, agg., VIII, Milano, Utet, 2017, 15 ff.; F. Tesauro, *Istituzioni di diritto tributario. Parte generale*, XIV ed., updated by M.C. Fregni, N. Sartori, A. Turchi, Milano, Utet, 2020, 227].

60. Article 9-*bis*, *Decreto legge* April 24, 2017, no. 50.

61. Articles 6-39, *Decreto legislativo* February 12, 2024, no. 13. The new tool overlaps with the sectoral studies and the tax compliance index in terms of subjective scope (self-employed taxpayers and SMEs), data and techniques. The novelty lies in the voluntary participation of the taxpayer. Nevertheless, this does not dispel doubts on the compliance with the principle of legality. The final provisions do not grant the right be heard before the agreement, disregarding the case law on sectoral studies (in footnote 59) and one of the requirements set out in the Enabling Law August 9, 2023, no. 111 (article 17, "*previo contraddittorio con modalità semplificate*").

62. *Gesetz zur Modernisierung des Besteuerungsverfahrens*, July 18, 2016 (BGBl. I S. 1679). See R. Seer, *Modernisierung des Besteuerungsverfahrens. Gedanken zum Referentenentwurf zur Modernisierungdes Besteuerungsverfahrens*, in *StuW*, 2015, 315 ff.

63. M. Krumm, *Germany*, in P. Pistone (ed.), *cit.*, 526-527.

64. *Abgabenordnung*, sec. 88(5).

authorities[65]. Hence, the vast majority of cases is processed without human intervention, based on data declared by taxpayers or transmitted by third parties.

Despite the lack of transparency regarding the type of algorithms used (deterministic or self-learning), certain German tax authorities have reportedly incorporated neural networks in their risk-management systems since 2011, to detect VAT carousel fraud[66]. French tax authorities are believed to be using neural networks as well[67]. The Italian tax administration, following the Data protection Authority's recommendations, announced that it has been testing both supervised and unsupervised learning algorithms, in addition to deterministic algorithms, without further details[68].

The selection phase is usually secret, to avoid the risk of reverse engineering of tax audits[69], and it is discretionary, to leave a certain margin of appreciation to peripheral offices that have a deeper knowledge of the local economy. Therefore, choices regarding the prioritization of tax audits are hardly transparent and questionable[70], whether made by humans or by

65. Moreover, taxpayers can opt for the manual verification of their tax returns. M. Krumm, *Germany*, in P. Pistone (ed.), *cit.*, 527.

66. N. Braun Binder, *Artificial Intelligence and Taxation: Risk Management in Fully Automated Taxation Procedures*, in T. Wischmeyer, T. Rademacher, *Regulating Artificial Intellihgence*, Cham, Springer, 2020, 301; Landtag von Baden-Württemberg, Mitteilung der Landesregierung, December 14, 2011, no. 15/1047, 19. For the same purpose, Bulgaria too gained a significant experience in identifying missing traders by combining a rule-based system risk score for all VAT-registered taxpayers with machine learning techniques to identify abnormal VAT transactions through the production chain. The result is a predictive model, more flexible compared to a solely rule-based system, that reduced by 15% the time needed to identify a missing trader since the beginning of its fraudulent activities (OECD, *Tax Administration 2022*, cit., 105).

67. V. Dussart, *L'intelligence artificielle et le data mining au service du contrôle fiscal des entreprises*, in A. Mendoza-Caminade (ed.), cit., 167 ff.

68. The Revenue agency recently published an extract from its privacy impact assessment and a notice on the logic behind its new algorithmic tools (*https://www.agenziaentrate.gov.it/portale/web/guest/analisi-basate-sui-dati-archivio-dei-rapporti-finanziari*). The literature shows that the Italian Revenue agency has been testing advanced supervised models, such as "bagging", that, by combining multiple trees, significantly improve prediction accuracy, at the expense of interpretation (see footnote 25 and M. Barone, S. Pisani, A. Spingola, *Data Mining Application Issues in the Taxpayer Selection Process*, in Y. Dimotikalis et al. (eds.), *Applied Modeling Techniques and Data Analysis 2*, Hoboken, Wiley, 2021, 12).

69. E.g., in Germany, *Abgabenordnung*, sec. 88(5).

70. M. Krumm, *Germany*, in P. Pistone (ed.), *cit.*, 533; R. Cordeiro Guerra, *L'intelligenza artificiale nel prisma del diritto tributario*, in S. Dorigo (ed.), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, Pacini, 2020, 98; F. Gallo, *Discrezionalità nell'accertamento*

means of software. While a detailed disclosure on the algorithm's features may facilitate reverse engineering dynamics, there appears to be no reason to stop taxpayers from accessing their data held by tax authorities to timely rectify inaccurate information.

The automation of tax assessment, with little or no human judgment, can lead to decisions that are difficult to interpret or biased.

Under the obligation to state reasons, tax audit notices resulting from automated decision-making techniques should only be upheld if the reasoning is interpretable and coherent with the relevant tax provisions. Moreover, taxpayers should always be granted the right to be heard[71].

Tax authorities may resort to presumptions to justify their assessments. Presumptions have been traditionally allowed due to the authorities' limited powers in fact-finding. However, *de iure condendo*, the large availability of personal and business data, often disclosed in real time thanks to taxpayers' and third parties' reporting obligations, may decrease the need to resort to presumptions[72]. At the same time, the ability of self-learning algorithms to extract knowledge from data can suggest new assumptions. Their rationale deserves careful evaluation before accepting them for tax assessment purposes[73].

The ability of AI to make decisions in an instant can amplify the impact of biased data and training, leading to thousands of incorrect decisions. Not only would this adversely affect the rights of those concerned, but it would also undermine, rather than enhance, the performance of the legal system as a whole.

This was the case in the Netherlands, where the government resigned in 2021 over the "childcare allowance scandal", due to false claims of fraud

e sindacabilità delle scelte d'ufficio, in *Riv. dir. fin. sc. fin.*, 1992, I, 661 ff.; G. Vanz, *I poteri conoscitivi e di controllo dell'amministrazione finanziaria*, Padova, Cedam, 2012, 232 ff.

71. Italian Data protection Authority, opinion, March 14, 2019, no. 58; S. Dorigo, *Intelligenza artificiale e norme antiabuso: il ruolo dei sistemi "intelligenti" tra funzione amministrativa e attività giurisdizionale*, in S. Dorigo (ed.), *cit.*, 137; A. Guidara, *Accertamento dei tributi e intelligenza artificiale: prime riflessioni per una visione di sistema*, in *Dir. prat. trib.*, 2023, 414.

72. S. Muleo, *Riflessioni sull'onere della prova nel processo tributario*, in *Riv. trim. dir. trib.*, 2021, 616, footnote 43; J.A. Rozas, *Tax assumptions in the digital era*, in Á. Antón Antón, C. García-Herrera Blanco (eds.), *cit.*, 229. Big data availability and analysis may also decrease the need for onsite inspections at the taxpayers' premises (P. Pistone, *General Report*, in P. Pistone (ed.), *cit.*, 52).

73. N. Sartori, *I limiti probatori nel processo tributario*, Torino, Giappichelli, 2023, 74.

uncovered by biased ML applications employed by the social security unit of the Dutch tax administration.

In summary, according to a parliamentary inquiry[74], the algorithmic system wrongly classified foreign parents as ineligible recipients, presumably because the system was trained on previous assessments of fraud involving foreign individuals. However, as Dutch nationality was not required to receive the childcare allowance, the analysis should have excluded this characteristic from the training data. Instead, thousands of erroneous recovery orders were issued, causing financial and personal hardship to the families concerned, due to poor training of the risk-management system and minimal human oversight.

This case, which was uncovered following an investigation by the Dutch Data Protection Authority, offers several key takeaways[75]. Not only does it show that AI is not neutral, but it also highlights the risks of automation without effective human supervision.

III. REGULATORY CHALLENGES IN THE PROTECTION OF TAXPAYERS' RIGHTS

From a policy perspective, the above mentioned "childcare allowance scandal" reveals the lack of a regulatory framework to address the challenges posed by AI. The framework on data protection does provide some principles that might be invoked to counter such risks, but their scope is limited to the treatment of natural persons' data. Besides, national data protection authorities are supposed to counter countless issues (e.g., the safety of minors' online activities, the use of sensitive data etc.) with limited resources, while AI is starting to become ubiquitous.

According to case law in different European countries[76], three main rights should be granted when public administrations rely on automated decision-making tools: the right to algorithmic transparency, the right to human intervention and the right to protection against discrimination.

These rights are mainly inferred from the right to private life enshrined in the European convention on human rights and in the EU Charter of

74. Tweede Kamer der Staten-Generaal, *Unprecedented injustice*, December 17, 2020, The Hague.
75. D. Hadwick, S. Lan, *cit.*, 2021, 609 ff.
76. Mentioned *supra*, in footnote 4.

fundamental rights[77]. The right to private life is further developed in the General data protection regulation (no. 2016/679, "GDPR"), according to which individuals have the right to be informed about the existence of automated decision making[78], including profiling, and the right not to be subject to a decision based solely on these techniques[79].

For multiple reasons, this framework does not appear to offer taxpayers a minimum level of protection.

First of all, the GDPR allows EU member States to restrict the scope of those rights to ensure other important objectives of general public interest, including taxation matters[80].

Furthermore, the principle of tax secrecy, preventing reverse-engineering of tax audits, is difficult to reconcile with the principle of algorithmic transparency.

While such a limitation is reasonable, other restrictions should be avoided or reconsidered, if currently in place. That is the case of limitations to the rights to access and rectify personal data held by tax authorities and to the right to refuse fully automated fiscal decisions, advance rulings included.

Not even the draft Regulation on AI appears to properly address these issues. The "EU AI Act" proposal, following a risk-based approach, imposes regulatory burdens only when AI systems are likely to threaten fundamental rights and safety. That is the case, for instance, with systems used by law enforcement authorities in relation to criminal offences. Other high-risk applications include those related to employment, as they may appreciably impact future career prospects, livelihoods and workers' rights[81], and the systems impacting on the access to certain essential private and public services and benefits necessary for people to fully participate in society or to

77. Article 8 ECHR and articles 7-8 CFREU. The Council of Europe's Committee on Artificial Intelligence recently proposed to negotiate a "Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law" (draft of January 6, 2023, revised on March 20, 2024).
78. *I.e.* the right to receive from the data controller "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing" [GDPR, article 15(1) h)].
79. GDPR, article 22(1).
80. GDPR, article 23(1) e).
81. "EU AI Act" draft, *corrigendum* of April 19, 2024, rec. 57.

improve one's standard of living[82]. Among the latter, explicit consideration is given to AI systems used to evaluate the credit score or creditworthiness of natural persons, since they determine the access to financial resources or essential services and may perpetuate historical patterns of discrimination.

While minimal transparency requirements (e.g., the obligation to flag the use of an AI system when interacting with users) are imposed for limited-risk systems, for the high-risk ones the draft Regulation sets "requirements of high quality data, documentation and traceability, transparency, human oversight, accuracy and robustness"[83]. However, according to its current wording, AI systems intended to be used for administrative proceedings by tax and customs authorities should not be classified as high-risk AI systems used by law enforcement authorities in relation to criminal offences[84].

The underlying assumption seems to be that the rights at stake in tax procedures are less significant than those involved in credit-scoring, in employment and in the enjoyment of essential services. That is not always the case, because we are witnessing the use of the income tax system, by multiple tax authorities, also to provide social benefits and address poverty (e.g., during the Covid-19 pandemic)[85]. When taxpayers are dependent on those benefits or in a vulnerable position, they should not be excluded from the protection afforded by the "EU AI Act". In addition, while tax provisions are formally unbiased, recent studies show that, despite the overall decline of tax audits in the United States due to budget cuts, low-income taxpayers (who often come from counties where most of the population is non-

82. Nonetheless, the proposed Regulation should not hamper the development of innovative approaches in the public administration, as long as that those systems do not entail a high risk to legal and natural persons (*ivi*, rec. 58).

83. "EU AI Act" proposal, explanatory memorandum, § 2.3. At opposite ends of this risk spectrum are AI systems with unacceptable risk and those with minimal risk: the former will be banned from the EU market (e.g., systems that exploit specific vulnerable groups or used by public authorities for social scoring purposes etc.); the latter will not be subject to any legal obligation under the draft Regulation.

84. "EU AI Act" draft, *corrigendum* of April 19, 2024, rec. 59.

85. D. Shaviro, *Tax law, inequality, and redistribution: recent and possible future developments*, in L. Parada (ed.), *A Research Agenda for Tax Law*, Cheltenham-Northampton, Elgar, 2022, 90 ff. See also the Policy forum hosted by the *Canadian Tax Journal*, issue no. 1/2021, on "*The Canada Revenue Agency as a Benefits Administrator*", 83 ff. The Italian Revenue Agency too has been designated to provide a range of non-repayable grants to businesses and freelancers experiencing economic hardship during the pandemic (see *www.agenziaentrate.gov.it/portale/web/guest/contributi-a-fondo-perduto-at*).

white) are far more likely to be audited than wealthier taxpayers[86]. As self-learning algorithms learn from the past, AI-driven selection of taxpayers for audit can only worsen these outcomes, perpetuating historical patterns of discrimination.

In conclusion, automated decision making has great potential to reshape tax procedures, but its implementation should be inspired by democratic values[87], not just efficiency. The comparative review of administrative practices reveals two opposing approaches: blind confidence in these tools[88], leading to fully automated decisions in the early-compliance and assessment phases, and a more careful approach, seeking the right balance between efficiency and the protection of taxpayers' rights, such as the rights to be heard, to human intervention and to the protection of legitimate expectations.

The former approach requires frequent exceptions to the rights enshrined in the charters of fundamental rights, the GDPR and the proposed "EU AI Act". For tax assessment purposes, it allows new assumptions to be inferred from big data. Regarding early compliance, AI-powered chatbots are starting to partially replace private rulings, but these automatic responses do not formally bind the authorities.

---

86. K.M. Bloomquist, *Regional Bias in IRS Audit Selection*, in *Tax Notes*, March 4, 2019. A.A. Abreu, *Racial issues in tax law: identification, redress, and a new vision of horizontal equity*, in L. Parada (ed.), *A Research Agenda for Tax Law*, cit., 110. Bloomquist compared the audit rates of regular tax returns with those claiming the "earned income tax credit", a widespread tax break for moderate-income households in the US. He explained that the IRS regional bias reveals a class bias on low-wage taxpayers that is not intentional on the IRS's part and is most likely due to the fact that audits on this tax allowance are fairly low cost to conduct, because they can be done by low-graded personnel (W. Hoffman, K.M. Bloomquist, *A Closer Look At IRS Tax Audit Selection Bias*, in *Forbes*, January 19, 2021).

87. See A. Giovannini, *Note controvento su interesse fiscale e "giustizia nell'imposizione" come diritto fondamentale (muovendo dall'intelligenza artificiale)*, in *Riv. dir. trib.*, 2023, I, 249 ff., conducting a principle-based analysis that revolves around the principle of personality, recognized as having an axiological precedence over the others, as well as around individual rights of justice.

88. S. Salardi, *Intelligenza artificiale e semantica del cambiamento: una lettura critica*, Torino, Giappichelli, 2023, 53, warning that "[s]e si lascia troppo margine operativo alla valenza persuasiva delle nozioni come fiducia si rischia di svuotare il ruolo dello stesso diritto nell'orientare lo sviluppo tecnologico. Chi si fida non controlla e chi non è controllato non ha nemmeno bisogno di regole entro cui operare". Similarly, regarding the digitalization of the tax administration, see F. Paparella, *L'ausilio delle tecnologie digitali nella fase di attuazione dei tributi*, in *Riv. dir. trib.*, I, 2022, 651.

Pursuant to the latter approach, the use of big data and AI could support taxpayers and tax officials at different stages of tax procedures for routine doubts and tasks, without excluding human judgment. The benefits would be less intrusive tax audits, a reduced need to rely on presumptions and faster decisions (yet compliant with the principle of legality). An acceptable level of taxpayers' protection could be negotiated as part of the amendments to the "EU AI Act". A more comprehensive approach to the digitalization of tax authorities could be pursued through amendments to the existing "Taxpayer Bills of Rights" or through the approval of "Digital Government Taxpayer's Charters"[89].

89. F. Montanari, S. Giorgi, *Digital Government Taxpayer's Charter*, in Á. Antón Antón, C. García-Herrera Blanco (eds.), *cit.*, 279 ff.; 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, I, 124.

Criminal law

Modern crimes. The case of digital identity protection

Francesco Diamanti*

SUMMARY: I. INTRODUCTION - II. THE "DIGITAL" IDENTITY - III. THE LEGAL GOOD "DESERVES" THE INTEREST OF CRIMINAL LAW - IV. DIGITAL IDENTITY CAN BE STOLEN (AND MORE) - V. IDENTITY THEFT. CAN IT BE PUNISHED? - VI. ARTICLE 640-TER (3) OF THE CRIMINAL CODE - VII. CONCLUSIONS

ABSTRACT: Can digital identity be stolen? Can this theft be punished in the italian legal system? How? The paper aims to answer these and other questions by exploring the topic of criminal protection of digital identity.

KEYWORDS: Criminal law, digital identity.

I. INTRODUCTION

Although it might not be so obvious at first glance, the evolution of the *Internet*, as a veritable place *(topos*) where human relationships are created, intertwined and exhausted (in its own way a community, a *polis*), has disproportionately broadened the tools with which to study, read, phone, meet, inform, do business, etc.[1]

* Associate professor in Criminal Law, University of Modena and Reggio Emilia.

1. It is no coincidence that today we speak of a "constitutional right to access the internet", for all see S. Rodotà, *Una costituzione per internet?*, in *Politica del diritto*, n. 3/2010, 337 ff. See also the (rightly) proposed constitutional law on the initiative of MP Madia, presented on 13 October 2022: *http://documenti.camera.it/leg19/pdl/pdf/leg.19.pdl.camera.327.19PDL0008910.pdf*; T.E. Frosini, *Il diritto costituzionale di accesso a internet*, in *Rivista AIC*, n. 1/2011, 1 ff., available *online* at *https://www.rivistaaic.it/images/rivista/pdf/Frosini_001.pdf*.

The network, influenced by all other technologies, is always on the move: from Web 1.0 to Web 2.0, for example, everything has changed.

It is one thing to live in an era characterised by static websites, almost like digital shop windows; quite another to move into a century characterised by a highly interactive web, marked by the development of extremely high-performance media such as social-networks (YouTube, Myspace, Twitter, Facebook, Instagram, TikTok, etc.), or in which institutions dialogue and exchange information, even there, with citizens. Here, mankind's communicative approach has undoubtedly changed with the development of these new platforms of "human contact", and with it have changed professions, ways of conceiving and doing business, of studying, of informing oneself, of relating to others, of dealing with the public administration, of spending time, of acting, and so on.

Just one example among many.

We live in a world in which with any camera, even a typical smartphone camera, and a good video editing programme, it is possible to show (almost) anyone what we can do or what we like to do, in the hope that someone will view them, that the content will interest them, and that they will later become followers.

You can do (or say) almost anything.

The limit, besides the normal rules of decency and illicit content, is really the imagination. There are those who wear clothes for promotional purposes, there are those who discuss international politics, there are those who dance, those who play an instrument, those who play games, those who teach, those who act, those who sing, those who inform, those who travel, those who cook, those who eat, those who test mattresses, those who review restaurants, those who whisper, those who do nothing, and so on. In short, if the content is liked, it is possible to hope, in the short to medium term, to create a public image or to start a real business or, in most cases, to enhance an existing one.

To do all this, however, you need a digital identity.

II. THE "DIGITAL" IDENTITY

According to the best known and most widespread definitions, "personal identity" is to be understood as the representation of an individual in relation

to the social context in which he develops his personality. A real "... right to be oneself, understood as respect for the image of participating in associated life, with the acquisitions of ideas and experiences, with the ideological, religious, moral and social convictions that differentiate, and at the same time qualify, the individual"[2].

Digital identity, on the other hand, what is it?

Defining it is not an easy task[3].

However, this is an unavoidable step for those who wish to discuss the criminal protection it has, or should have in the future: this locution, in a nutshell, can indicate both an explicit reference of the citizen or entity on the web, and the set of information connected to that same citizen and enabling his or her online identification[4].

More can be done.

At least at an introductory level, one can observe its (recent) terminological evolution. Well, the idea of "digital identity" spread in Italy in the early years of the new millennium, initially indicating "... any digital interface of a natural person, such as a profile on a social network or a blog"[5]. It is only since 2009 that the term "digital identity" begins to be transformed into the synthesis of the citizen's identity for administrative purposes: to see it mentioned in a legal text, however, it will be necessary to wait until Law No. 69 of 2013, which will associate it with the SPID (Sistema Pubblico di Identità Digitale – Public Digital Identity System) that many people are now familiar with and use regularly in their dealings with the public administration or other institutions (e.g. the Revenue Agency)[6]. In 2014, a Prime Ministerial

2. See Corte costituzionale, sent. no. 13 of 1994. On the right to personal identity, among the first organic studies of the 20th century, A. De Cupis, *Il diritto all'identità personale. Parte prima: Il diritto al nome. I- Il nome civile*, Milan, Giuffrè, 1949.
3. On these versions of digital identity see M.F. Cocuccio, *Il diritto all'identità personale e l'identità "digitale"*, in *Dir. fam. e pers.*, n. 3/2016, 949 ff., esp. 954 (also taken up in C. Crescioli, *La tutale panale dell'identità digitale*, in *Dir. pen. cont.*, n. 5/2018, 265 ff.).
4. For all, see again C. Crescioli, *La tutela penale dell'identità digitale*, cit., 265 ff.
5. Cf. *https://accademiadellacrusca.it/it/parole-nuove/identit-digitale/21516*.
6. On one point, however, there is no need to be confused: case law, which intervened on the applicability of the aggravating circumstance set out in Article *640-ter* (3) of the Criminal Code, which we will discuss below, clarified the obvious: it specified that, despite the absence of a legislative definition of it, a digital identity, in order to be considered as such, does not necessarily require a validation procedure by the public administration. See Cass. pen., Sez. II, 27 October 2022, Sent. No. 40862; Cass. pen., Sez. II, 11 August 2020, sent. No. 23760. For all, on the subject, cf. R. Flor, *Phishing,*

Decree defined digital identity as "... the computer representation of the two-way correspondence between a user and his or her identifying attributes, verified through the set of data collected and recorded in digital form in accordance with the modalities set out in this decree and its implementing regulations"[7]. This, in fact, is also the historical moment when the phrase under analysis began to spread more widely in Italian society, following an exponential increase in its relevance for all citizens. So much so that, in 2022, the term "digital identity" entered into the European Committee of the Regions' Opinion on the creation of a European digital identity (eID), i.e. a "portfolio" containing all national digital identity data, educational qualifications, and vocational training information, in order to guarantee and implement the exchange between EU countries[8].

Digital identity is thus a rib of personal identity.

So much so that, at least for the purposes of criminal liability, it would be advisable to follow a broad definition of "digital identity", thus encompassing "... any data, information, code, programme, application or medium, even in combination with each other, that enable the identification, recognition or authentication of a natural or legal person in interaction with computer or telematic systems or for access to them or for the use of services or functions offered through them"[9].

But does it deserve criminal protection?

III. THE LEGAL GOOD "DESERVES" THE INTEREST OF CRIMINAL LAW

When discussing digital identity, as mentioned above (see § 1 above), a fact that is obvious to digital natives, but not so obvious to everyone else, must be taken into very close consideration: the web allows the real subject to enter a virtual world and remain in continuous contact with a number of people, entities or institutions, unimaginable in reality. In hypothesis, the web makes it possible to connect the individual with the entire population

identity theft and identity abuse. Le prospettive applicative del diritto penale vigente, in *Riv. it. dir. proc. pen.*, n. 2-3/2007, 899 ff.

7. DPCM 24 October 2014, Gazzetta Ufficiale No. 285, 9/12/2014, 2.
8. Cf. again *https://accademiadellacrusca.it/it/parole-nuove/identit-digitale/21516*.
9. This definition, which in our view is very comprehensive, is to be found in the reform draft available at *https://www.aipdp.it/allegato_prodotti/71_riservatezza_sicurezza_informatica_identita_digitale_Picotti.pdf*.

of the planet. This new reality, unthinkable in the world before, generates a double, and potentially immense, exposure of human beings.

The individual is ahead of everyone and everyone is ahead of him.

Here, however, you have to get it right.

Online activities are often very serious things: if we take the famous entrepreneur Chiara Ferragni as an example, we discover that her Instagram profile (to which her identity is linked) currently has 28.6 million followers. This data, if contextualised, is of great interest: in addition to the attractiveness for companies that need to market products – which with these numbers would in itself be (abundantly) sufficient for our purposes -, it is good to know that social, precisely the platforms, also remunerate individual posts according to the views achieved. In this system, a photo or video posted on Instagram by well-known entrepreneurs can reach millions of people around the world in an instant and, consequently, result in immediate earnings for the influencer (for publication alone) of tens of thousands of euros. And this happens to Chiara Ferragni as it does to millions of other people, often unknown to the younger generation: there are gamer-influencers like Nick Kolcheff who earn millions of dollars a year by being watched on YouTube or Twitch while playing video games.

Here everything becomes clearer.

By hacking into a very simple Instagram account of some well-known influencer or content creator, it is possible to generate gigantic economic damage, just as it is possible to instantly connect with tens of millions of people. In addition to the one already mentioned of Chiara Ferragni, consider that Elon Musk's Twitter account, for example, has almost 103 million followers, i.e. people all over the world who read everything he posts on that social-network in a matter of moments. Stealing their digital identity – e.g. taking possession of their social accounts – does not only mean depriving those people of an essential means of communication or of huge earnings, but it also means having the tools to carry out acts of immense gravity: from extortion[10] to very serious defamation[11], up to shifting, for

10. M. Luberto, *"Sex-torsion" via web e minaccia a mezzo ransomware: la nuova frontiera del delitto di estorsione*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, II, Turin, Giappichelli, 2023, 764 ff.

11. F.P. Lasalvia, *La diffamazione via web nell'epoca dei social-network*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, cit., 346 ff.

instance by spreading a fake news[12], a large part of Italian or European public opinion, perhaps a few hours before an important vote.

If identity deserves (criminal) protection, then so does digital identity[13].

On the one hand, there is the right not to have our opinions misrepresented; on the other hand, there is the right to the exclusive use of one's personal details on the web[14]. Having said that, however, we need to understand whether our criminal law – by which we mean the criminal code and special criminal laws – is already equipped to prevent and repress acts of such personal, economic and social significance.

IV. DIGITAL IDENTITY CAN BE STOLEN (AND MORE)

Assuming, merely by way of introduction, that criminal actions aimed at targeting digital identity are now generally brought under the category of computer crime (or cybercrime)[15], it is necessary to start the discussion with theft.

Its phenomenology is not trivial.

Partly because it is undoubtedly a prodromal offence to the commission of other offences (including criminal offences) and which develops in stages that are also very different from each other: the core of the offence consists in the theft of users' confidential data, but then there is the phase of interaction with this information (e.g. possession, sale), and the use of the data themselves to commit further offences (e.g. defamation, threats, persecution, extortion, etc.)[16]. This is partly because the ways in which the perpetrator can take possession of a digital identity are many and very complex; moreover, since they are mostly methods of injury characterised by a massive use of technology, they are refined over time. It is no longer a question of the old subtraction of the paper identity document (which, moreover, will soon be dematerialised), but, for example, of all those

12. On this topic, most recently, see P. Guercia, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, cit., 1290 ff.
13. L. Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Idem (eds.), *Il diritto penale dell'informatica nell'epoca di internet*, 2004, 125 ff.
14. C. Crescioli, *La tutela panale dell'identità digitale*, cit., 274.
15. For all, L. Picotti, *Sistematica dei reati informatici*, cit., 21 ff., esp. 29. On the subject, most recently, see A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, cit., 321 ff.
16. C. Crescioli, *La tutela panale dell'identità digitale*, cit., 265 ff.

telephone and/or computer techniques by which the victim falls into a trap. Think of the (most widespread) case of phishing, in which one receives an ad hoc e-mail created to alert the user-victim to problems with their bank's server, requesting them to update their data via a specific link[17]. This, of course, is only a "simple" example, but there would be many more and much more complex ones: think of "man-in-the-middle" phishing, in which the e-mail contains a malicious link capable of damaging or altering the computer data of the electronic device used; or smishing or vishing, i.e. those committed with the use of SMS or mobile phone; or pharming, which consists of requesting the user-victim to enter a "clone" website, which often reproduces in detail that of their banking institution, and to enter all the data.

There is a problem.

Digital identity theft does not exist as an autonomous case.

Neither in the criminal code of 1930, nor in the special criminal laws.

V. *IDENTITY THEFT*. CAN IT BE PUNISHED?

The legislative framework, as mentioned above, is daunting.

However, in the first years of the new millennium, Italian jurisprudence tried to solve the problem hermeneutically, initially attributing digital identity theft to the violation of confidentiality and of the right to express consent to the processing of personal data, with the consequence that the offence referred to in Article 167 of Legislative Decree No. 196 of 30 June 2003 ('unlawful processing of data') could be operative[18].

The sanctions were not adequate.

Subsequently, the judges followed different paths.

The best-known ways of damaging the digital identity that result in damage to the victim other than purely pecuniary damage have been more correctly brought back, albeit by means of highly extensive hermeneutical operations[19], to the case under Article 494 of the Criminal Code. ('substitution

17. R. Flor, *Phishing, identity thefte identity abuse: le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 900 ff.
18. Cass. pen., sez. III, 26 March 2004, sent. no. 28680.
19. So also C. Crescioli, *La tutela*, cit., 267.

of person')[20]. This offence, incidentally, provides for imprisonment of up to one year for anyone who, in order to procure for himself or for others an advantage or to cause damage to others, misleads someone by unlawfully substituting his own person for the person of others, or by attributing to himself or to others a false name, or a false status, or a quality to which the law attributes legal effects.

One of the cases dealt with by the jurisprudence of legitimacy concerned the creation of a fake Badoo profile (an old and well-known dating site), with the user name "Naty", the offended person's photo and a profile description "... anything but flattering". The purposes were different: on the one hand, the offender was able to gain several (non-pecuniary) advantages from the digital identity theft, concerning the possibility of having personal relationships with several girls and satisfying his vanity; on the other hand, the conduct was, according to the judges, certainly capable of seriously damaging the image and dignity of the offended person, so much so – the Court recalled – that the victim even received a verbal assault from the boyfriend of a girl harassed on Badoo by the offender[21].

The range of hermeneutic solutions is much wider than that.

20. For all of them, among the most recent, and taking up case law from at least 2007, cfr. Cass. pen., Sez. V, 5/02/2021, sent. no. 12062 (whoever uses a *social* using the photo of a different person commits the crime of person substitution). On this subject, among others, cfr. A. Crisafulli, *Sul reato di sostituzione di persona*, Messina, 1934; F. Lanzara, *Osservazioni sul delitto di sostituzione di persona*, in *Rivista di polizia*, n. 1/1970, 3 ff.; G.A. Jacovone, *Il delitto di sostituzione di persona*, Naples, 1974; R. Cappitelli, *La sostituzione di persona nel diritto penale italiano. Cass. sez. V 11 December 2003, no. 8670,* in *Cassazione penale*, n. 10/2005, 2994 ss.; C. Flick, *Falsa identità su Internet e tutela penale della fede pubblica, degli utenti e della persona. Nota a Cass. sez. V pen. 14 dicembre 2007, n. 46674*, in *Il Diritto dell'informazione e dell'informatica*, n. 4-5/2008, 526; F.G. Catullo, *Rilevanza penale dell'identità virtuale. Nota a Cass. sez. V pen. 14 dicembre 2007, n. 46674*, in *Diritto dell'Internet*, n. 3/2008, 250 ff.; M. Casellato, *Sostituzione di persona. Nota a Cass. sez. V pen. 14 dicembre 2007, n. 46674,* in *Studium iuris*, n. 6/2008, 759 ff.; P. Cipolla, *"Social network", furto di identità e reati contro il patrimonio*, in *Giurisprudenza di merito*, n. 12/2012, 2672 ff.; M. Tarsetti, *Il reato di sostituzione di persona nella identità digitale. Interpretazione estensiva o norma creativa? Nota a sent. Cass. pen. sez. V 19 luglio 2018 n. 33862*, in *La Giustizia Penale*, n. 4/2020, 230 ff.

21. Cass. pen., sez. V, 23 April 2014, sent. no. 25774, cf. F. Sansobrino, *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in *Dir. pen. cont.*, 30 September 2014, 1 ff. (the full judgment can be found at: *https://archiviodpc.dirittopenaleuomo.org/upload/1410527051Sarlo_2014_25774*.pdf).

This is because, as we have seen, digital identity theft is a criminal phenomenon that is usually highly articulated and may presuppose, contain or generate, quite other criminal hypotheses.

Some examples related to phishing[22].

Imagine that by smishing[23] someone, substituting his or her identity with another in order not to be detected, steals debit or credit card numbers, then invites the offended persons, in the name of their bank, to contact a fake telephone operator (with a recorded voice) and provide him or her with all the aforementioned card data, using them immediately afterwards to make withdrawals and purchases[24]. Well, similar cases make it possible to focus attention on the fact that the conduct of those who steal the digital identity of others is usually attributable to offences other than merely Article 494 of the criminal code.[25] Keeping the case illustrated above as a mere example, it is worth specifying how the Court of Milan found the concurrence of substitution of person (Article 494 of the Criminal Code) with the offences of fraud (Article 640 of the Criminal Code) and misuse of credit cards (Article 493 of the Criminal Code)[26]. In other cases, however, judges have recognised in phishing the concurrence of substitution of person, fraud and unauthorised access to a computer system (Article 615-ter of the Criminal

22. On the more general topic of computer frauds and *phishing*, lastly and without any claim to completeness, cfr. G. Minicucci, *Le frodi informatiche*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, cit., 893 ff. and 907 ff. with a lot of references to which we refer.
23. In a nutshell, *smishing* is a form of *phishing* that uses mobile phones as an attack platform - unfortunately much more effective than the infamous *e-mails* - to mislead recipients and carry out fraud.
24. Trib. Milan, G.I.P., 7 November 2007 in *Diritto di Internet*, n. 3/2008, 261 (for the judgment see. *http://www.intertraders.eu/pronunce/giudiziarie/TriMi_07112007.pdf*).
25. On this subject, see R. Flor, *Realizzare furti di identità tramite tecniche di phishing integra più fattispecie penali e costituisce un reato transnazionale*, in *Riv. di giurispr. ed econ. d'azienda*, n.3/2008, 136 ff. It is worth highlighting how, according to some, the perpetrator, in cases similar to the example given in the text, cannot be convicted of the offence of substitution of person, since the criminal technique used - the so-called "phishing" – is a criminal offence. *Phishing Voip Attack* – involves recorded voices, without direct human contact with the victim. Thus P. Perri, *Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia*, in *Diritto di internet*, n. 3/2008, 265 ff., esp. 267.
26. This offence can also be committed by entering credit card data in an online *form*, which sees its moment of consummation with access to withdrawal or purchase services even without the physical availability of the card itself. Thus, among others, see R. Flor, *Phishing, identity theft and identity abuse*, cit., 899 ff., esp. 914.

Code)[27]: on the other hand, as has been noted in the literature, there is no doubt that the final stage of these offences is often dedicated to abusive access to reserved computer areas or network services, which require the breaking of protective barriers such as passwords, names or user codes, and so on[28].

There is more.

VI. ARTICLE *640-TER* (3) OF THE CRIMINAL CODE

There is, for example, computer fraud aggravated by theft of digital identity (introduced into the Criminal Code by Art. 9 of Decree-Law No. 93/2013)[29] which punishes with imprisonment from two to six years and with a fine ranging from EUR 600 to EUR 3,000 anyone who, by stealing or by unduly using a digital identity to the detriment of one or more persons, alters in any way the operation of a computer or telecommunications system or intervenes without the right to do so in any way on data, information or programmes contained in a computer or telecommunications system or pertaining to it, thereby procuring for himself or others an unjust profit to the detriment of others[30].

The legislator has tried to fill the gap.

But it did so somewhat clumsily with the insertion of a special circumstance with special effect[31]which implies that the mere "theft" or the mere "misuse" of a digital identity, in itself, does not constitute an offence unless there is also an unlawful diminution of the victim's assets. Clearer: if you steal a digital identity to defame someone, this provision does not cover[32].

The case, however, presents several perplexities.

27. Trib. Milan, 7 October 2011, in *Dir. pen. proc.*, n. 1/2012, 55 ff.
28. Cfr. C. Crescioli, *La tutela*, cit., 269.
29. Although Decree-Law No. 93/2013 had also provided for the inclusion of aggravated computer fraud (Article 640-ter, paragraph 3, of the italian Criminal Code) in the list of predicate offences for the criminal liability of the entity, the conversion lost it along the way. Thus, to date, the provision only applies to the natural person. Also C. Crescioli, *La tutela*, cit., 273. highlights this missed opportunity for preventive purposes of digital identity protection.
30. The act thus described is punishable ex officio [Article *640-ter* (5) of the italian criminal code].
31. It seems cautiously inclined, however, towards the nature of an autonomous case C. Crescioli, *La tutela*, cit., 270, note 35.
32. C. Crescioli, *La tutela*, cit., 272.

Suffice it to point here to the reference to "theft" and "use", which are ill-suited to a digital identity that can neither be "physically" stolen nor (unduly) used[33]; or, to cite a much more serious matter, think of the enormous difficulties that lie behind a criminal law provision that mentions an indeterminate concept such as digital identity, which the criminal law (for now) does not define at all[34]. Of course, there are definitions: consider, by way of example, the one in Article 1(2) of legislative Decree No. 82 of 2005 (letter u quater), which defines it as "the computerised representation of the correspondence between a user and his identifying attributes, verified through the set of data collected and recorded in digital form". However, to think of using it in the criminal justice system would perhaps be to decontextualise it too much and, consequently, to restrict the scope of application of the special aggravating circumstance[35]far too much.

Having said that, however, it is necessary to get to the heart of the matter.

It is understood from the parliamentary proceedings that, pursuant to Article 640-ter (3) of the Criminal Code, digital identity theft is to be understood as "impersonation", i.e. the partial or total concealment of one's identity through the use, in a combined form, of data relating to one's person[36]. But if this is the case, then it is difficult to establish the boundaries of theft from misuse: think, for the sake of clarity on this point, of someone who legitimately uses someone else's digital identity but for unauthorised purposes. Is it not true that, in this case, he is "misusing" someone else's digital identity and, at the same time, "impersonating" another human being?[37] The undue use referred to in the provision, of course, is not unlawful processingeither, if only for the fact that the aggravating circumstance punishes the digital substitution of the person, not other unauthorised uses of the data acquired (e.g. for commercial purposes)[38].

33. C. Crescioli, *La tutela*, cit., 270.
34. For more recent jurisprudence attempting, to some extent, to define it for the purposes of criminal liability, see Cass. pen., Sez. II, 20/9/2022, sent. no. 40862, in *Cass. pen.*, 2/2023, 456 ff. (specifying that on the subject of computer fraud, the notion of "digital identity", which integrates the aggravating circumstance referred to in Article *640-ter*, paragraph 3, of the italian Criminal Code, does not presuppose a validation procedure adopted by the public administration, but also applies in the case of the use of access credentials to computer systems managed by private individuals.
35. C. Crescioli, *La tutela*, cit., 271.
36. C. Crescioli, *La tutela*, cit., 271 and footnote n.º 44.
37. C. Crescioli, *La tutela*, cit., 272.
38. G. Malgieri, *La nuova fattispecie di indebito utilizzo d'identità digitale: un problema interpretativo*, in *Dir. pen. cont.*, 2015, 143 ff., esp. 149; so also C. Crescioli, *La tutela*, cit., 272.

That being said, the offence we are talking about seems perfectly suited to repress some, albeit not very widespread, ways in which the digital identity of victims is stolen. Specifically, we refer to pharming, which, we repeat, consists in asking the user-victim to enter a website "clone" of a real one (e.g. of one's own banking institution) prepared ad hoc. Illegal conduct, this one, which, by actually requiring the alteration of the operation of a computer system, may fall within the scope of Article 640-ter (3) of the Criminal Code[39].

However, the litmus test is missing.

Does Article 640-ter (3) of the Criminal Code succeed in suppressing phishing?

This question is very important because, as has already been mentioned, this is one of the most widespread ways in which perpetrators manage to take over the digital identity of their victims. Unlike pharming, which has already been mentioned (see § 6 above), phishing does not involve the alteration of any computer system. In other words, phishing, if we really had to subsume it in a currently existing abstract case, would perhaps be more a classic fraud (Article 640 of the Criminal Code) than an aggravated computer fraud (Article 640-ter, paragraph 3 of the Criminal Code)[40].

VII. CONCLUSIONS

Concluding is not easy.

It is not because, even today, there is unfortunately little to say.

'Digital identity', as we have seen, is an expression that can mean either an explicit reference of the citizen or entity on the web, or the set of information linked to that same citizen and enabling his or her online identification. As such, it is something fundamental for (almost) everyone, on a par with classical identity: in our time, at least, it is for working, for presenting oneself to others, for playing, for sponsoring products or companies, for training and information, for volunteering, for travelling, for research, and so on. It is, moreover, a legal asset undoubtedly deserving of criminal protection (and

39. F. Cajani, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14/8/2013, n. 93 (convertito con modificazioni dalla l. 15/10/2013, n. 119)*, in *Cass. pen.*, n. 3/2014, 1094 ff., esp. 1097.

40. F. Cajani, *La tutela penale dell'identità digitale*, cit., 1097. On the relationship between fraud (Article 640 of the Criminal Code) and *phishing* see R. Flor, *Phishing, identity theft and identity abuse*, cit., 910 ff.

its protection – criminal, indeed – is not incompatible with constitutional principles).

The damage that its subtraction can generate is enormous.

Human, reputational and economic. However, not only directed at its legitimate owner, but also at society as a whole: to understand this, one only has to imagine the problems produced by someone who, a few hours before a local or national vote, takes possession of an Instagram profile with twenty-six million followers (almost all of whom are over 18); by publishing a sentence or a photo or a fake news story, he or she changes public opinion and, consequently, the election result.

However, this is not matched by serious criminal law protection.

One can hope for the legislator of the future.

The indications, in the literature, have been given[41].

First of all, Article 640-ter (3) of the Criminal Code should be repealed; then, a new autonomous offence known as "abuse of digital identity" should be introduced at the end of a (new) Section VI, dedicated to "Crimes against confidentiality and computer security" (of Chapter III of Title XII), worded as follows "Unless the act constitutes a more serious offence, any person who, without authorisation, creates or procures for himself or for others, or uses, reproduces, communicates, hands over, makes available to the public or disseminates data, information, programmes, or any other application, which enable a digital identity to be represented, shall be punished by imprisonment of from six months to two years and a fine of up to fifteen thousand euro. The offence is punishable on complaint by the offended person, unless any of the aggravating circumstances set out in the second, third and fourth paragraphs of Article 615-ter of the Criminal Code apply, or in cases where the act concerns a significant quantity or a significant number

41. For all, again, see the research for the reform of offences against the person carried out by the Italian Association of Criminal Law Professors in Group VII, which focused on "Crimes against the inviolability of the home, the protection of privacy and secrets, computer freedom and personality" (coordinated by Alessandra Rossi) and, specifically, the Subgroup that worked on "Confidentiality and computer security, digital identity"*(team*: Lorenzo Picotti, Roberto Flor, Ivan Salvadori, University of Verona. The full text is now published in DiPLaP (ed.), *La riforma dei delitti contro la persona. Proposte dei gruppi di lavoro dell'AIPDP. Atti dei seminari di discussione in collaborazione con il DiPLaP*, Milano, 2023, cfr. *https://8b257bd2-3d0e-4a3a-89f08a300a5d7f12.filesusr.com/ugd/f261dd_1c38d9b9b23843449505b7706f93bac5.pdf*.

of digital identities. For the purposes of criminal law, digital identity shall mean any data, information, code, program, application or medium, even in combination with each other, which enable the identification, recognition or authentication of a natural or legal person in the interaction with computer or telecommunications systems or for access to them or for the use of services or functions offered through them".

AI and criminal law reform: notes on the inadequacy of a criminalization model based on a substantive principle*

1Fernando Miró-Llinares**

SUMMARY: I. ¿TIME TRAVEL TO CRIMINALIZE SKYNET? A SCIENCE FICTION SCENARIO FOR TODAY'S REGULATION - II. SUBSTANTIVE REASONS FOR POTENTIAL CRIMINAL LAW REFORM IN THE FACE OF AI'S EMERGENCE - *II.1. Artificial Intelligence, new interests and/or new harms to existing ones: traditional arguments for crime reform* - II.1.1. New interests worthy of protection by criminal law and criminalization - II.1.2. New forms to harm or endanger interests worthy of criminal protection relying on AI and criminalization - III. AUTOMATION, AUTONOMY, SCALABILITY: SINGULARITIES OF AI AND THEIR RELATION TO CRIMINALIZATION - IV. ON THE INADEQUACY OF A CRIMINALIZATION MODEL BASED ON THE QUESTION "WHY CRIMINALIZE" IN THE FACE OF THE CHALLENGES OF AI

ABSTRACT: Artificial Intelligence is already widely used in many sectors of society. The advent of this technology, and the harms that may create, poses challenges relevant to criminal law. Not only the general part of criminal law could be affected but special criminal law as well. This contribution establishes the essential theoretical elements to face the challenge of the criminalization of offences related to AI. First, addresses the roots of the need of criminal intervention in this field, particularly, the emergence of new interests worthy of protection by criminal law and new harms to already protected interests that demand new offences to ade-

* Este trabajo ha sido posible en el marco del proyecto Ius_machinA, acrónimo del proyecto TED2021-129356B-100, financiado por MCIN/AEI/10130359/501100011033 y por la Unión Europea NextGenerationEU/PRTR.

** Full Professor of Criminal Law and Criminology, Miguel Hernández University of Elche.

quately respond to AI related harms and risks. Secondly, studies what makes AI a "game changer" for crime, underpinning that the automation of data-driven decision-making can have important consequences in terms of establishing criminal liability. Finally, theoretical tools to legitimise criminal law intervention are explored in the context of AI-related offences, developing a procedural approach.

KEYWORDS: Artificial Intelligence; Criminal law; criminalization and automatization.

I. ¿TIME TRAVEL TO CRIMINALIZE SKYNET? A SCIENCE FICTION SCENARIO FOR TODAY'S REGULATION

The definition of AI has become a headache for those who engage in debates about its regulation[1]. Paradoxically, this occurs even though we all have a common and intuitive understanding of what we are referring to when discussing AI. Another term, closely related to AI, that suffers a similar problem is Science Fiction. Adam Roberts expresses it very well in an interesting essay on this genre: any bookstore has a section on science fiction and it is evident that science fiction can easily identified as literature that covers worlds or realities other than those in which the reader lives, but when it comes to distinguish it from other fantastic genres and explain why, for example, "The Metamorphosis" or "One Hundred Years of Solitude" do not fall into the genre, and the difficulty begins[2]. Roberts looks for the distinctive feature of this genre and finds the key in the first noun, which functions rather as a direct object of the second one. In his view, in science fiction there is not only fantasy or unreality but a discourse of possibility, usually grounded on scientific or technological perspectives. All science fiction incorporates what Darko Suvin refers to as a novum, a point of difference between the real world and the world depicted in science fiction, which serves as a metaphor for real life[3]: Wells' time machine, Ursula K. Leguin's distinct genre, the autonomous Robot in so many works that were precursors to the very idea of AI. Hence the distinctiveness of the genre is

1. J. Zanol, A. Buchelt, S. Tjoa, P. Kieseberg, *What is "AI"? Exploring the scope of the "Artificial Intelligence Act"*, 2022, available at: *https://jusletter-it.weblaw.ch/dam/publicationsystem_leges/iris2022/zanoal_et_al_what_is_ai.pdf*.
2. A. Roberts, *Science Fiction*, Routledge, London, 2000.
3. D. Suvin, *Metamorphoses of Science Fiction: On the Poetics and History of a Literary Genre*, New Haven, Yale University Press, 1979.

that it deals with the problems and dilemmas of life through metaphors, but creating novums, ideas or new objects. Time has proven that these new features can leave fiction and reach reality. They bring problems or dilemmas that used to belong to fiction, but new ones as well, that concern reality.

A classic example of science fiction related to Artificial Intelligence technology is the Terminator film saga. It began with James Cameron 's "The Terminator" in 1984 and so far, includes five more films about the battles between the Artificial Intelligence Skynet and mankind. While there are other previous works that cover this topic (Kubrick and Clarke "2001: A space Odyssey"), it is in "Judgement Day" where the idea of an AI developed in the military field, that ends up becoming aware of itself, and tries to annihilate humanity, is developed in more detail. Beyond the relationship between humans and robots that end up acting autonomously and acquiring moral ideas, the central novum of Terminator consists in the idea of a technological company, that uses an unknown technology end up giving rise to a Superintelligence. While it is a novum that can still be considered science fiction, since Superintelligence does not exist, many already foresee its early existence. Moreover, they warn about of the risks of its development, and outline multiple risks and harms linked to the first developments of autonomous learning algorithms still under development such as autonomous driving or lethal autonomous weapons[4]. In addition, other aspects of the technological-social argument raised by these science fiction films are already present in our reality: the military use of AI, the design of open-source AI algorithms that may lead to unforeseeable future developments, and the question of how a society should deal with the development of a technology whose impacts are still unknown in a context of scientific uncertainty[5].

It is unrealistic to think that we could have a legislator of the future coming to warn us about the real risks of this technology and to tell us how and what to criminalize. Nonetheless, there are aspects of the

4. See N. Bostrom, *SUperintelligence*, Oxford, Oxford University Press, 2014. An interesting response to Bostrom's "fears" is based on the consideration that we would be facing a problem for which there would be rational expectations of a solution N. Agar, *Don't worry about superintelligence*, in *Journal of Ethics and Emerging Technologies*, 2016, 73-82

5. It is true that AI is not the first technological development in which this has problem has arisen. See in this regard the scenario of scientific uncertainty and its regulation that was brought about first by the genetic revolution and then by environmental degradation and global warming, W. Van den Daele, *Legal framework and political strategy in dealing with the risks of new technology: the two faces of the precautionary principle*, in *The regulatory challenge of biotechnology*, Edward Elgar, Cheltenham, 2007, 118-138.

aforementioned science fiction work that can help us reflect on how we should face the challenge of regulating and criminalizing behaviors related to the use of this technology. One of them has to do with the fact that almost any attempt to stop this technology is futile. It only causes a sequel of the same technological tool (in the form of a new movie), and surrenders to the the structural, almost deterministic, tendency of modern societies towards innovation and technological development, assuming any known or unknown cost that comes with it. In this vein, Van den Daele says that our societies have institutionalized a type of science that seeks to immediately transform knowledge into technology. Based on a capitalist market economy, society seeks to create needs for technological exploitation, legitimating the production and access to new technologies and crafting the legal system from that perspective[6]. This diagnosis especially suits AI technology. Not exclusively because some use of the technology has been adopted prior to its regulation (the case of militar AI), but when laws had been considered, a will of ensuring innovation and economic growth has prevailed, not imposing excessive legal burdens that might hinder these developments[7]. I don't mean that we are doomed to an unstoppable future development of AI. That said, this is more likely to occur than its complete ban by law.

Given the ongoing development of AI, and the already visible risks it poses, in this paper I will address, in a sort of a first approximation, how criminal law should address the question of criminalization in relation to its design, development and use. I will not address aspects regarding the reform of the criminal system to face (science fiction) scenarios in which AI systems can be considered autonomous and liable for their actions. Neither how current criminal liability systems respond to the damage already caused by AI. Instead, the chapter seeks to answer whether it is necessary to reform the catalog of offences in the Criminal Code with the advent of AI.

In the context of the regulatory process that we are going through in Europe and that will end with the approval of the AI Act, it is essential to start analyzing the role that criminalization can play on its regulation. However, the aim of this paper is not yet to develop a catalog of new offenses that will be passed or to specify the areas that will require the reform of the criminal

6. *Ivi*, 18-138.
7. As in the case of China. An interesting study on the different AI governance strategies in China and the European Union, H. Roberts, J. Cowls, E. Hine, J. Morley, V. Wang, M. Taddeo, L. Floridi, *Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes*, in *The Information Society*, *39*(2), 2023, 79-97.

code. The goal is establishing the essential theoretical elements to face such a challenge. What interests me in this paper is rather to make a first reflection on the weak bases that inform decisions about criminalization in complex scenarios. This seems necessary considering that accelerated technological changes surrounding AI, its social impacts and unexpected damages and risks, will more than likely force rapid reforms of the criminal justice system. In this context, it is essential to build a framework that helps us decide what to criminalize and how. My contribution, therefore, focuses on showing, considering the singularities of this technology, how the usual way used to determine what can be criminalized and what cannot, centered on reflection on substantive approaches, is insufficient in view of the challenges that AI poses.

II. SUBSTANTIVE REASONS FOR POTENTIAL CRIMINAL LAW REFORM IN THE FACE OF AI'S EMERGENCE

II.1. ARTIFICIAL INTELLIGENCE, NEW INTERESTS AND/OR NEW HARMS TO EXISTING ONES: TRADITIONAL ARGUMENTS FOR CRIME REFORM

Is assumed and hardly discussed, that AI has the potential to improve people's well-being, contribute to sustainable and positive global economic activity, increase innovation and productivity, and help respond to major global challenges such as climate change, environment and health, the public sector, finance, mobility, home affairs and agriculture.[8] . Also, that digitalization, in general, and the use of automated systems based on AI technologies, seems unstoppable in many social areas. Nonetheless, the individual and collective risks that AI poses are becoming more tangible. The Committee of Ministers of the Council of Europe has recognized the need to supervise algorithmic applications, due to the role they will play in society; the European Union has recognized that some uses of AI may jeopardize fundamental goods and rights[9], and it is likely that the future AI regulation it will ban certain uses of this technology[10]. But, as I say, the

8. Ocd, *Recommendation of the Council on Artificial Intelligence*, adopted 22 of may 2019. Available at: *https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449*.
9. European Commission, *White Paper On Artificial Intelligence – A European approach to excellence and trust*, 2020, available at: *https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en*.
10. See article 5 of the Proposal for a Regulation of the European parliament and of the Council laying down harmonised rules on Artificial intelligence (artificial intelligence act) and amending certain union legislative acts. Available at: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0206*.

observation of reality already shows us that concerns and regulations are not based on future scenarios but on present experiences. Massive amounts of data have been used to create social profiles and spread false political information, autonomous lethal weapons have caused harm not expected by their programmers, apps have been created by states to allow citizens to report incivilities, accidents have been caused by autonomous driving, apps based on generative AI that allow the creation of fake nudes of real people[11], to cite a few[12]. These are examples that are not frequent on the judicial practice, but they show that the use of AI to commit crimes is far from being just science fiction. They allow us to foresee that when the presence of these technologies in routine activities increases the probability of their criminal use will also increase.

Attending to the novelty of these harms and risks, it seems reasonable to review the penal systems and, if they do not respond adequately to them, to consider the possibility of amending the penal code, either through the creation of new offences or through the reform of existing ones. The starting point is the existence of interests that may be affected (harmed) by the irruption of this technology. This is the traditional argument to justify criminal intervention: the need to punish the conduct to prevent harm (or risk) to legal interest's worthy of protection. I will address latter whether this is sufficient. At this stage, what we need to address is the two possible reasons that could inform a reform of the special part of the penal codes. Firstly, the emergence of new social interest's worthy of protection that are not fully related to those currently protected by criminal law. Second, the impossibility of existing offences to encompass the harm or risks that the use of AI poses to already protected interests.

II.1.1. New interests worthy of protection by criminal law and criminalization

The development of AI and related technologies may raise the need to protect new interests or values. The data from which algorithms are fed, the AI systems themselves, certain conditions of their application, or even

11. In the case of Deep Fake technology See M. Santisteban Galarza, *La respuesta penal ante las ultrafalsificaciones (deep fakes). Más allá de la criminalización de la difusión de pornografía sintética no consentida*, in *Revista de Derecho Penal y Criminología*, 2024, (in press).
12. For a review of multiple cases in various countries on crimes where AI has been used for criminal purposes See F. Miró Llinares, *Penal law and criminalization in the face of the challenges of AI. General report*, in *RIDP*, 2024 (in press).

interests associated with robots, may in the near future constitute individual or collective interests worthy of protection by criminal law. Beyond the protection of AI itself as a possible distinct legal interest, we are still far from being able to guess what these interests will be and how their protection should be configured. One thing that can be anticipated is that the conception we have of privacy as an interest worthy of protection may end up being modified. It would not, therefore, be a question of the emergence of a new legal interest, but rather of the modification of the scope and significance of previous protected values. The use of data for AI may represent a paradigm shift in the understanding of this interest, and even a revision of the traditional meaning of the right to privacy as a purely individual or personal right. The collective value of data beyond the meaning they have for the individual and the implications that their control and use by institutions or individuals can have for society as a whole, makes some authors begin to wonder whether AI should not lead us to a new social understanding of the right to privacy[13].

Regarding the need to protect AI, it is clear that AI systems themselves may be subject to criminal activities, disrupting or damaging them. If they are used to carry out certain activities, as part of a critical infrastructure, their malfunctioning could cause considerable harm. From this, however, it cannot be inferred the necessity to autonomously protect AI as a new legal interest worthy of criminal protection. In this case, what is at stake is the value that the system supports, endangered by its malfunctioning (national security, public health), and the AI system can be described as the material object of the offense rather than the protected value. In those cases, the malfunction shall give rise to the criminal response in the event that the protection of that interest requires the response of criminal law. In addition, most of these systems may fall within the Budapest Convention's broad understanding of "computer system", any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. Thus, it is likely that damages caused to AI systems may already be protected by the criminal offences enacted by states on the basis of the Budapest Convention's and other laws[14] for computer-related damage.

13. In a similar vein C. Véliz, *Privacy is power,* Corgi Books, 2020.
14. Similarly, Directive 2013/40/UE on attacks against information systems defines information systems as a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.

And as regards the copying of these systems, what will be affected will be the economic and patrimonial interest of the creators, which may be protected either by the crimes related to the protection of intellectual property rights, or by those that protect industrial property rights when it can be patented or, most probably, by means of crimes against free competition.

It cannot be ruled out, in any case, that in the near future specific protection will be required in the case of robots, taking into account the different values linked to these AI technologies, especially in the event that they reach a certain degree of autonomy[15].

II.1.2. New forms to harm or endanger interests worthy of criminal protection relying on AI and criminalization

Within substantive approaches to criminalization like the principle of exclusive protection of legal interest or on the harm principle, there is another reason that may lead to the reform the catalog of criminal offenses in the face of the irruption of AI. In the case of already protected values, AI technologies may create new means of harming or endangering interests that justify a different criminal intervention. Using the indeterminate plural here is a deliberate choice. If it not disputed that due to the way in which this technology is developing, some areas, such as road safety, will be affected first, the social transformations triggered by AI systems are not limited to a few personal and social spheres, but are transversal. The new risks arising from the automation of certain processes and the need to adapt legal liability systems to them are also generic. AI is an instrumental technology that enables to carry out tasks that were already conducted by humans, although now more quickly and efficiently. As a technology applicable to many tasks and, therefore, related to multiple interests, we can intuit that soon almost all the crimes of the special part may be committed relaying on AI system.

In this way, and as happened with cybercrime, AI will allow the emergence of "replica behaviors", actions and behaviors in which the means of commission changes but end up affecting in a similar way the protected interest[16]. The reform of the criminal code should not be necessary in this scenario, unless there is an express reference on the offence to the means

15. Even separating it from her. See K. Mamak, *Should violence against robots be banned?*, in *International Journal of Social Robotics*, *14*(4), 2022, 1057-1066; K. Darling, *Extending legal protection to social robots: The effects of anthropomorphism, empathy, and violent behavior towards robotic objects*, in R. Calo, A.M. Froomkin, I. Kerr (eds.), *Robot Law*, Northampton, MA, Edward Elgar, 2016.
16. F. Miró Llinares, *El cibercrimen*, Madrid, Marcial Pons, 2011.

of commission required to carry out the prohibited conduct. This concerns, for instance, crimes of homicide or injury. The protection of life and health is carried out in practically all the known penal codes through offenses that punish the realization of a harmful result or a or a concrete risk. Criminal codes do not determine the means of commission used as a key element of the offence. It is also true, however, that all criminal codes include various types of offenses that, in relation to specific areas of risk, establish endangerment offences, establishing an advanced protection of the interest at stake. This is what happens, for example, with crimes against road safety, those related to food safety or nuclear safety. In this case the dimension of risk justifies a specific typification of the prohibited conducts, and the legislator has anticipated the criminal response to conform an adequate protection of the legal interests such as life and health of an abstract collectivity of persons.

AI, as a new means to commit the criminal offence, might alter the dimension of the harm and risk posed by the prohibited conduct, and thus, make us consider new forms of criminalization. I will devote the following section to a better analysis of this issue.

III. AUTOMATION, AUTONOMY, SCALABILITY: SINGULARITIES OF AI AND THEIR RELATION TO CRIMINALIZATION

To understand the impact of AI on the emergence of new ways of injuring and putting at risk personal and social interests that give rise to criminal liability, it is necessary to analyze the characteristics of this technology and what really makes it a "game changer". If AI promises anything, it is the automation of any data-driven decision-making process due to its high computational capacity, the high reliability of the data and the number of variables that can be analyzed. Accordingly, classical decision-making processes, based on the interaction of different human agents with different knowledge and responsibilities aimed at making the most appropriate decisions based on certain purposes, when supported or replaced by AI systems, can be affected (theoretically improved) both by the increasing speed and (allegedly) objectivity. And here comes into play another singularity of AI: the decision, or part of it, can be transferred to the machine, leaving it in the hands of an entity that, in the sense of not acting under human supervision, is autonomous. This has important consequences in terms of establishing criminal liability. First, With the use of AI systems, the key moment at which liability is triggered will generally no longer be located

close to the externalization of the harm or risk. Instead, the early stages of the AI life cycle, such as the design of the algorithm or the selection of the data that will feed the system, will be more relevant to criminal law in most scenarios. This can be explained by the fact that it is at these stages that harms or risks can be foreseen and prevented[17]. If we add to the equation the introduction of an agent other than a human, to whom we cannot transmit a duty of care and to hold liable, the key moment of liability is moving even more clearly to a place much earlier, distant to stages close to the manifestation of the harm. In other words, With AI, the selection of the purposes of algorithms, or what will form the context (and content) of their decision making, becomes decisive in the way the AI "acts". For this reason, it is logical that the normative systems that determine liability should take into account these key moments for attributing liability, although these are much "advanced" than those that are traditionally relevant for criminal law.

In addition, the automation of processes carried out with the use of AI systems will generally include the assignment of one or more of the parts of the process to an entity capable of "acting autonomously". Indeed, it has been outlined that an essential element of this technology would be the ability to learn by itself and to act autonomously, and that this would force a rethinking of liability given that there may be loopholes for the attribution of some damages caused by autonomous machines[18]. Some authors point out that the possibility of AIs acting autonomously may lead us to find ourselves with damages caused by machines for which neither the designers, developers, manufacturers or marketers could be held liable, because they were perpetrated within the framework of machine autonomy, nor the machines themselves because they are "non-moral" agents to whom liability cannot be attributed, leading to a liability gap[19]. This issue specially concerns Autonomous Lethal Weapons and has raised an interesting discussion

17. That is clearly what is happening in connection with the debate on the regulation of autonomous vehicles. As the Austrian national rapporteur points out, since damages are now caused by decision-making processes that do not originate from a human being, the debate is focused on questions of liability of human beings acting much earlier: the producer, the programmer or the user of the intelligent system. F. Salimi, *Austrian National Report* (IAPL), 1. (in press).
18. J. Danaher, *Automation and Utopia: Human Flourishing in a World without Work*, Harvard University Press, 2019.
19. J. Danaher, *Robots, law and the retribution gap*, in *Ethics and Information Technology, 18*(4), 299-309; R. Sparrow, *Killer robots*, in *Journal of Applied Philosophy, 24*(1), 2017, 62-77. König has opposed this, pointing out, adding a reflection that I find very interesting, that it is implausible to suppose that the high degree of autonomy of an autonomous system can exculpate negligent or malicious behavior on the part of its designers. P.

about how liability should be established and how these systems should be designed[20].

What are the consequences of this perspective on AI criminalization? There are several reform options. The first entails an absolute ban on certain AIs, such as autonomous lethal weapons, under the consideration that their autonomy leads to a lack of control and a liability gap, not being able to hold anyone responsible for their criminalization[21]. A second option is to anticipate criminal intervention to moments far from the materialization of the harm, but close to the responsible human action, creating new specific criminal offenses, for example, that establishes "duty of care relevant to criminal law". This option does not completely avoid the possibility of a "criminal liability gap" but limits it to those cases in which the harm was not reasonably foreseeable and human agents have fulfilled all demandable control obligations to avoid harmful results. However, the Penal Codes could sanction acts of infringement of administrative duties, or preparatory conducts that, in any of the cases, are considered to involve sufficient risk to be sanctioned in advance and autonomously, disassociated from the responsibility for the possible harmful events that could occur as a consequence of them. This comprehends conduct such as failure to maintain the necessary levels of safety standards for activities such as testing, manufacturing, updating, control, of certain high-risk AIs[22], and omissions such as the failure of manufacturers of autonomous or artificial agents to take certain precautions, or even the concealment or hindering of access to the type of programming used by the AI system[23]. Even if no damage has been caused by such behaviors, they could aspire to become not only breaches of administrative duties but, where a serious risk can be asserted, new "formal" endangerment offenses.

Another possible way to respond to this singularity of AI would be the modification of the offenses that only punish behaviors that require mens rea to encompass negligent behaviors. Nonetheless, this has some shortcomings. As Beck has rightly warned for robotics: this has several difficulties related to the slow development of standards to be used in relation to certain AI

Königs, *Artificial intelligence and responsibility gaps: what is the problem?*, in *Ethics Inf. Technol.*, 2022.

20. R.C. Arkin, *Governing lethal behavior: Embedding ethics in a hybrid deliberative/reactive robot architecture*, in *Proceedings of the 3rd ACM/IEEE international conference on Human robot interaction*, 2018, 121-128.
21. R. Sparrow, *Killer robots*, cit., 62-77.
22. J. Provaznik, *Czech national report (IDPL)*, 4 (in press).
23. N.A. Cherñavsky, M.A Riquert, *Argentine National Report (IDPL)*, 13 (in press).

systems that are still under development; to the difficulty of translating the schemes used to consider what are the appropriate risks such as general-social rationality in the case of robots, and that while the attribution of predictability of harm will not be difficult where AI is more autonomous and more potentially dangerous, it will be increasingly difficult to foresee the specific conditions and situations in which harm will manifest itself. What is evident is that the distance from the moment of agency does not play in favor of being able to consider that there will be negligence when participating in early phases of creation of tools that end up causing the harm. If, in general, when many subjects are involved in the production chain, the possibilities of determining which of them will be responsible become more difficult[24], taking into account the whole life cycle of the AI, the inquiry into the failure of the AI and what is the specific omission or action that has led to the result, will be as difficult as it is relevant in these cases.

We have seen, that, to address the singularity of AI in terms of criminalization, there are several possibilities of action and reform the criminal code. It is clear that in order for us to adopt any of these criminalization options, it would be necessary to assert its legitimacy based on a first requirement related to the endangering or harm of interests relevant to criminal law. In the case of seeking to criminalize the distribution of certain particular high risk AI systems, we would be obliged to reflect on whether there is an interest worthy of protection that could be harmed or put at stake. In order to criminalize the absence of control in the design and production of certain AIs, we should be able to affirm that the conduct endangers legal interests worthy of protection. This concerns as well the second technique, consisting of expanding the catalog of negligence-based offences, as constitutes a similar form of anticipation of criminal protection. The question if this approach is enough to completely guide the decision process regarding criminalization.

Before addressing this issue, we shall describe one more singularity of AI that should not be overlooked. The use of AI systems entails the possibility of analyzing large amounts of data, recognizing patterns and making predictions or decisions based on this information. As pointed out by Moro-Visconti, et al. in a study focused on the differences that the

24. A. Moraiti, *AI Crimes and Misdemeanors: Debating the Boundaries of Criminal Liability and Imputation*, in *RIDP*, 2021; L. Picotti, *Traditional Criminal law categories and AI: crisis or palingenesis? General report*, in *RIDP*, 2023, 11-53.

use of this technology makes in the business environment[25], AI can reduce costs by automating processes, optimize operations by reducing errors and improving decisions by taking into account knowledge that was previously ignored, and replicate and automate activities by adapting them quickly to new conditions. This implies a singularity of the use of AI systems consisting in the scalability of the operations that AI enables. What is worthy of considering on the field of criminal law, is whether this greater capacity to increase the scale, the dimension, of what is carried out when executed with AI could lead to an increase in the dimension of harm to the interests worthy of protection. In other words, will a crime against a legal interests be considered more serious just because AI is used, insofar as it entails, per se, greater potential damage to the interest worthy of protection? It is clear that AI can not only help to carry out more sophisticated attacks but can also facilitate the perpetration of such attacks on a massive scale. For example, the use of AI for the commission of crimes such as disinformation or hate speech could lead to a significant increase in the impact of these content as it is easier with these techniques to adapt the speeches to different contexts, affecting many more subjects and increasing the harmful consequences. This also happened with the Internet and the emergence of cybercrime, which, in fact, would continue to be a fundamental basis for, at least in these cases, taking for granted the greater scalability of what is perpetrated with AI.

This has been highlighted by Gullo and Flor who point out that "due to their connectivity, speed and learning of the environment, AI systems can amplify the scale of harm related to their operation or use" and that "prior to AI, the legislator addressed similar issues in relation to criminal conduct committed in cyberspace, which have the same effect of amplifying the scale of harm and affecting many more subjects"[26]. All this will lead us to consider not the possibility of creating new crimes but the adaptation of the penalties for existing crimes to the supposedly greater seriousness of the conducts perpetrated with AI. Here the question is not only one of legitimacy (due to proportionality), but of the appropriate technique to achieve it. Indeed, crimes are already typified directly allows the adaptation of the penalty to the level of the harm or, instead, that the motivation/dissuasion that seeks the prevention of these behaviors requires a generalization of the aggravation when they are used. In any case, making, per se, a total assumption that the use of this technology entails greater severity and accordingly introducing

25. R. Moro Visconti, S. Cruz Rambaud, J. López Pascual, *Artificial intelligence-driven scalability and its impact on the sustainability and valuation of traditional firms*, in *Humanities and Social Sciences Communications*, *10*(1), 2023, 1-14.

26. R. Flor, A. Gullo, *Italian National report (IDPL)*, 9 (in press).

aggravating circumstances covering the use of IA, may not be an adequate solution. This is because the use of IA as a means of commission does not pose a mayor threat to the affected interests in all cases.

IV. On the inadequacy of a criminalization model based on the question "why criminalize" in the face of the challenges of AI

So far, all the reflections made in this paper on the challenges for the criminalization of AI related offense have revolved around the same and essential question: why could we criminalize a behavior performed with the use of AI or that affects AI-related interests? Although by posing this question and arguing around it we could be implicitly turning around other issues such as what would be the maximum proportional penalty that could correspond to each conduct, the main argument is whether there is a sufficient reason that allows criminal law to punish a behavior that, previously, was not sanctioned. We are at the level of legitimacy, and working with a minimum conception of legitimacy: to criminalize a conduct, a minimum condition that legitimizes the reaction of the penal system must be fulfilled. This way we are reducing the scope of the analyzes to the reasoning behind what shall be criminalized, in this case, in relation to behaviors in which AI is used or that affect new interests related to it. Surely, the question of the legitimacy of criminal intervention is crucial when considering criminalization. Indeed, for this reason, both in common law and continental law, the issue of criminalization has been addressed from this perspective.

As Marshall and Duff have pointed out, it is not overly reductionist to state that there are two different ways of approaching the question of the construction of moral principles for the criminalization of behaviors, although one of them is clearly predominant in academia. The first of these approaches, focus on the answer to the question of "why we shall criminalize". It looks for a principle, or an alternative combination of them, to answer the question. The second is a procedural model, which the focus on political processes (attending to the formal political process required) or rational process (specifying the logical structure of the deliberations), through which the decision on criminalization should be carried out[27]. As Marshall and Duff acknowledged, a purely procedural model would be meaningless as any model of criminalization must start from some principles concerning why criminalization is possible. However, it is possible to find proposals that, without abandoning legitimacy issues, focus on the decision-

27. R.A. Duff, et al. (eds.), *Criminalization: The Political Morality of the Criminal Law*, Oxford, Oxford Academic, 2014, 41.

making procedure and are not based on a single principle. This is conducted fragmenting the substantive arguments that shall inform the process of criminalization. I will address this model later.

In the continental tradition, the pre-eminent model is a substantive approach. It is generally grounded on the protected legal interest principle or "rechtsgut"[28]. The approach is grounded in the question of whether the offence punishes a conduct that affects a legal interests worthy of protection. If the answer is affirmative, criminalization is seen as a legitim choice; other aspects are not directly introduced in the argumentation. The same is true of the common law model, based, fundamentally, on the harm principle. The criminalization of a conduct is not possible only because it is a wrongdoing, an immoral conduct. To answer the question of why it is legitimate to criminalize a conduct we must be able to affirm that it harms others[29]. The harm principle, in this sense, becomes the equivalent of the principle of exclusive protection of legal interests: we can criminalize a conduct because it is harmful (even if it is remotely so) to a legal interest worthy of protection. It is true that in the common law tradition some authors have accepted, especially in the view of the weakening of the harm principle, the introduction of other principles such as the offense principle or legal paternalism. However, these are conceived as alternative principles to the harm principle and operate under the same logic of answering why a conduct can be criminalized. In other words, in the common law tradition the answer to the question of the moral legitimacy of criminalization must be answered asserting the harmfulness or the offensive nature of the studied conduct.

What links both models, thus, is that they are configured as principles of criminalization that operate as legitimizers of criminal intervention without, at least expressly, existing any need to add any more theoretical elements to the question of criminalization. It is true that, later on, there are considerations such as the principle of minimum intervention in the continental sphere that seem to recognize that something more must be required in order to criminalize a conduct, but even when this is the case, their configuration remains on the level of legitimacy through the answer to the question "Why can we criminalize a conduct?" Applied to issue of AI criminalization both schemes offer the same approach: the answer depends

28. For a deeper look see R. Hefendehl (ed.), *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmático?*, Madrid, Marcial Pons, 2007.
29. J. Feinberg, *Harm to Others: The Moral Limits of the Criminal Law,* Oxford, Oxford University Press, 1984.

on whether we consider that a conduct is harmful or dangerous to a legal good worthy of protection.

The deficits of a criminalization model based exclusively on the idea of why we must criminalize had already been raised long before the emergence of AI. The issue, as Duff et al. point out, is not the values to which the aforementioned principles appeal (liberty, dignity), that are hugely relevant and can play a role in deliberations about criminalization. The difficulty is to develop an adequate theory of criminalization relying only on those principles[30]. The harm principle or the legal interest cannot be configured as a master principle or a silver bullet to determine the scope of criminal law. Its role is to provide a deliberative framework that brings us closer to coming to see reasons for (or against) the criminalization of certain types of conducts. In the words of Duff et al: "given the wide range of values that we can expect to figure in the public sphere of a contemporary, pluralistic polity as values requiring legal recognition and protection; given the diversity and complexity of the social and institutional formations of such a polity; given the variety of ways in which the criminal law can figure as a possible method of dealing with different types of legally defined wrongdoing: should we expect to find a diversity of motives for and paths to criminalization, a diversity that cannot be captured in any theoretical structure of coordinate principles?"[31].

As I have already pointed out, perhaps the solution is not to give up on a substantive standpoint but to integrate it into a more procedural approach to the question of criminalization. This is what is proposed, for example, by Husak, who identifies up to seven restrictions that any criminal law proposal must meet to be considered justified. Husak includes procedural considerations that a legislator must follow to decide whether or not to criminalize a type of conduct, both political, focused on the legislative process through which criminal law is developed, and rational, taking into account the logic of the appropriate legislative provisions[32]. It seems to me that the basis of this approach can be traced to the proposal of Schonscheck, who presented a filtering process to answer the question of how to decide criminalization. I cannot, in this contribution fully develop the keys of this model and its application to AI, but I am interested in directly raising some of Schonscheck's arguments, critical with the criminalization model based

30. R.A. Duff, et al. (eds.), *Criminalization*, cit., 41.
31. *Ivi*, 45.
32. D. Husak, *Overcriminalization: The limits of the criminal law*, Oxford, Oxford University Press, 2008.

on the answer to the question why criminalize. In particular, I believe that the author is right to point out at least two major problems of a model of criminalization based on a single principle. The first and the fundamental one refers to its excessive simplicity[33]. When the whole process of deciding how and when to criminalize depends on a single condition, on a single argument, the argumentation that must be made by the one who must defend criminalization is oversimplified. If, on the other hand, a step-by-step procedure is established in which the decision on whether or not to criminalize depends on overcoming a series of concrete and not generic arguments, the legislator would be forced to provide a deeper argumentation and under more complex premises. The second problem, very related, lies in the difficulty of weighing and contrasting arguments of different natures against each other and of doing so on the same level.[34]. The disadvantage of a criminalization model that aggregates all possible arguments into a single general idea of whether or not legal interests are protected against harm or risk, is that it allows different arguments, moral or deontological, consequentialist or pragmatic, to be used and prevail indistinctly, without being clear which one shall prevail.

In sum, the problem, in my opinion, remains that a procedure of this type in which the question to be answered is why we can criminalize is not adequate to account for the complexity that should be attributed to political-legislative decisions regarding criminalization. We shall look for a different approach and instead of asking "why shall we criminalize?" we focus on the question "how to decide whether to criminalize". The legitimacy of criminal intervention in the traditional way shall be taken into account in this process, but also other complements that we have always considered necessary for its rational attribution: the minimal intervention nature of criminal law, the existence of other administrative and social orders that may need to be taken into consideration, and other questions of opportunity that may justify in some cases a non-intervention. This way, we will be in a better position to deal with the complexity of these processes.

Being all of the above enough to justify abandoning a criminalization model based exclusively on the question of why we can criminalize, I believe, moreover, that there are arguments that support this decision in the context of the criminalization of AI. First of all, and starting with an argument perhaps not only applicable to AI but to many other cases of

33. J. Schonscheck, *On Criminalization: An Essay in the Philosophy of Criminal Law Cit*, Springer, 1994, 33.
34. *Ivi*, 34.

criminalization related to immediate technological changes and of great social impact, if in general the criminalization of behaviors should be taken as a complex process that requires the consideration of factors diverse in scope and nature, there are specific reasons to think that we are reflecting on a field where the complexity may be even greater. First, we are dealing with a technology that is still under development. In this vein, a single argument based on the legal interest or on the harm principle may be somewhat weak cause the dangerousness of certain AI uses has not been completely studied or described. In addition, we are still in the process of constructing the regulation of AI, which will establish permissible and impermissible risks. Thus, establishing the scope of the allowed risks only through criminal law, based on the mentioned substantive approaches and without considering extra criminal regulation, might arise inconsistencies in the legal system. There is another factor that should not be forgotten in order to discard simplistic arguments about criminalization: we are facing one of those areas, as happened with cybercrime, where national states will have a limited deterrent capacity since these tools will be mainly designed by multinationals and, in the event of an adequate response, it will be essential to coordinate and even harmonize criminal intervention.

There are other reasons why I consider clearly inadequate an approach to criminalization simply based in the concept of the legal interest legal good worthy of protection in the case of AI systems. They derive from the characteristics that make this technology a game changer and that we must take especially into consideration in any process of criminalization. Regarding the mentioned relationship between scalability and harmfulness of AI systems, a decision process simply based on whether or not there is a protected legal interest will hardly resolve the question of how and with what penalty criminalize AI related offences. Harm may be a key factor in determining proportionality, but special consideration must also be given to the role that other enforcement tools may play in terms of deterrence. And something similar happens in relation to the other singularity associated with AI, automation, and what it implies both in terms of moving away from the key moment at which liability shall be placed, and the birth of possible liability gaps when some parts of the decision-making process are ceded to entities with the supposed capacity to proceed autonomously. As we have seen in the previous point, in view of these characteristics, the possibilities that arise in terms of criminalization are multiple: banning systems that create liability gaps or create crimes of abstract endangerment that convert liability gaps into control obligations. What shall be acknowledged here

is none of this solutions can be implementing relying exclusively in a substantive approach.

Let's look at some examples. Focusing on the potential criminalization derived from the specific prohibitions of commercialization and distribution of some AI technologies that could be established by the AI Act, it is obvious that the starting point of the regulation is that they pose an unacceptable risk. But should that imply an immediate criminal translation in the sense that their design, production and commercialization should be criminalized? For those AI uses that are not prohibited but are considered high-risk, a similar problem raises. Will extra criminal obligations that are established, for example, related to the control of these technologies, also give rise to criminal liability when there is an infringement on monitoring duties? I believe that it is obvious that such approach would ignore the role that criminal law shall have, and it is grounded in the incomplete consideration that harmfulness or risk can decide criminalization on its own. Something else is missing, to cite a few key arguments: the specification that behaviors that could be considered potentially risky are those that should be effectively criminalized, and not punished by means of other systems that have a greater capacity for deterrence or that respond more adequately to the harm; the analysis of the consequences in terms of risk compared to the benefits and risks of preventing the use of technology.

The criminalization of dangerous activities related to the control over the design of some particularly risky tools suffers from a similar problem. A criminalization criterion built on the mere question of whether there is a legal interest at stake would not allow to differentiate which of the multiple key moments from the very design of the AI system can be considered really decisive and harmful. It will be essential in these cases to pay attention to the administrative regulations and the soft law that determines the permitted and impermissible risk, and to take into consideration the dissuasive capacity of the different regulatory instruments to be able to decide whether the breach of a duty of care, in itself, merits criminalization through the creation of endangerment offenses, or, instead, can only be punished when the risk materializes.

The challenges posed by the emergence of technology as AI show that excessively rigid approaches on criminalization, that are based in single principle, are dysfunctional. Instead, procedural approaches, focused on determining a logical structure of deliberation leading to criminalization decisions, would be more appropriate to guide as on the likely transformation

that our criminal codes will undergo. We cannot answer the questions relevant to determining how best to respond to the challenges of AI only by answering the question of when it is legitimate to intervene with the criminal law. It seems clear that it will be necessary to develop what the role of criminal law will be in cases of breach of risk obligations regarding the design or control of AI tools even without knowledge of the specific risk or harm that might be involved, but with knowledge that a requirement (in design, AI testing, registration, etc.) aimed at reducing the risks associated with potential uses of the tool has been violated. Although the extra criminal rules, which serve to balance risks and benefits from a general perspective, cannot be the only information taken into consideration to determine what is dangerous or not from a criminal perspective and the point of view of social morality will have to be taken into account, it seems clear that it will be necessary to take into account the developments of administrative regulations on AI control and safety in order to get closer to knowing in relation to what legal interests and at what point the anticipation of criminal law is legitimized.

Commercial law

Supervision on market infrastructures based on distributed ledger technology. The role of ESMA

Alessandro V. Guccione*

SUMMARY: I. INTRODUCTION - II. THE STRUCTURE OF SUPERVISION ON DLT MARKET INFRASTRUCTURES. THE SUPERVISORY POWERS OF THE COMPETENT AUTHORITIES - III. ESMA'S SUPERVISORY POWERS - IV. COOPERATION BETWEEN OPERATORS OF DLT MARKET INFRASTRUCTURES, COMPETENT AUTHORITIES AND ESMA - V. CONCLUSIONS: INNOVATIVE NATURE OF ESMA'S COMPETENCES ON DLT MARKET INFRASTRUCTURES

I. INTRODUCTION

With Regulation (EU) 2022/858 of 30 May 2022 relating to «a pilot regime for market infrastructures based on distributed ledger technology» (hereinafter reg.), the European Union pursues the objective of «exploring, developing and promoting the uptake of transformative technologies in the financial sector, including the uptake of distributed ledger technology (DLT)», ensuring that the «Union financial services legislation is fit for the digital age and contributes to a future-proof economy that works for citizens, including by enabling the use of innovative technologies» (Recital no. 1, reg.)[1].

* Associate Professor in Commercial Law, University of Modena and Reggio Emilia.

1. D.A. Zetzsche, J. Woxholth, *The DLT Sandbox under the EU Pilot Regulation*, University of Luxembourg Law Research Paper No. 2021-001; F. Annunziata, A.C. Chisari, P.R. Amendola, *DLT-Based Trading Venues and EU Capital Markets Legislation: State of the Art and Perspectives under the DLT Pilot Regime*, Bocconi Legal Studies Research Paper, January 2023; R. Priem, *A European DLT Pilot Regime for Market Infrastructures: Finding a Balance Between Innovation, Investor Protection, and Financial Stability*, in *SSRN*, September 2021; M. Milanesi, *Lo sviluppo delle "sandbox" regolatorie italiane tra dubbi e opportunità. "Requiem" per l'art. 223 dello "Schema definitivo di Codice dei contratti pubblici"*,

The need to intervene through a legislative act is identified in particular in the limits of applicability and in the doubts about the adequacy of the current legislation on financial markets to satisfactorily regulate the phenomenon of crypto assets, largely due to the complexity of the mechanisms underlying distributed ledger technologies which had not been considered at all at the time of the adoption of the regulatory acts on which the European regulation of financial markets had been adopted. On the other hand, European legislators considered «premature to significantly modify Union financial services legislation to enable the full deployment of such crypto-assets and their underlying technology», in consideration of the «limited experience as regards the trading of crypto-assets that qualify as financial instruments and related post-trading services and activities» (Recital no. 5, reg.), and have therefore chosen to adopt a «pilot regime», based on the *exemption* of DLT market infrastructures from some *requirements* foreseen by the rules governing the markets in financial instruments in general, on the provision of specific guarantees for investors, and which should allow supervisory authorities and legislators to acquire specific experience in such an innovative sector, also in view of future legislative interventions (Recital no. 6, reg.).

The following remarks concern the impact of the pilot regime on the structures of financial supervision within the European Union and on the sources of law relating to markets in financial instruments, as it is necessary to ask whether the relationship between the powers recognized to the different authority respects the division of competences provided by the rules establishing the European System of Financial Supervision (ESFS), and whether the measures that the different authorities can adopt in this field fall within those envisaged by the same "constitutional" sources regarding European supervision.

---

in *Federalismi.it*, n. 15/2023, 111 ff.; F. Bertelli, *Il regime pilota per le DLT tra principio di neutralità tecnologica e nuove strategie di cooperazione tra pubblico e privato*, in *Rassegna di diritto civile*, n. 1/2023, 361 ff.; P. Leocani, U. Malvagna, A. Sciarrone Alibrandi, A. Tranquillini, *Tecnologie di registro distribuito ("distributed ledger technologies") per la rappresentazione digitale di strumenti finanziari ("security token"): tra diritto cartolare e disciplina delle infrastrutture di mercato*, in *Rivista di diritto bancario*, n. 2/2022, 73 ff.; P. Cipollone, *Senato della Repubblica, 6° Commissione permanente (Finanze e tesoro). Audizione sul disegno di legge n. 605 di conversione in legge del decreto-legge 17 marzo 2023, n. 25, recante disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech*, 4 aprile 2023.

II. THE STRUCTURE OF SUPERVISION ON DLT MARKET INFRASTRUCTURES. THE SUPERVISORY POWERS OF THE *COMPETENT AUTHORITIES*

As for the structure of supervision on market infrastructures, a distinction must be made. At European level, the establishment of new authorities has not been envisaged, but only the assignment of new supervisory tasks to ESMA. At national level, European legislators have identified the competent authorities with the same authorities designated pursuant to art. 67 dir. 2014/65/EU or art. 11 of the reg. (EU) no. 909/2014 (art. 2, no. 21, letters a) and b), reg.), but having allowed the member states to indicate other competent authorities for the purpose of monitoring the application of the regulation (art. 2, no. 21 , letter c, reg. and 13, reg.), they have at the same time admitted a derogation from the structure of the supervisory system at national level.

However, there are numerous changes and additions to the powers vested in the competent authorities provided for by the general regulation of supervision on markets in financial instruments. The competent authorities are, first, the active subject of a series of information obligations placed on market infrastructures[2]. In addition to this, the competent authorities appear to have been granted with regulatory power, being able to set thresholds lower than those envisaged by the regulation in relation to both the value of individual issues of DLT financial instruments and the overall value of all financial instruments admitted to the DLT infrastructure (art. 3, par. 6, reg.). It is not clear, however, whether this power can be exercised only in the form of general provisions, valid for all market infrastructures, or for all market infrastructures of a certain type, etc., or whether it can also concern one or more market infrastructures or DLT financial instruments, assuming in this case the configuration of an individual decision in the strict sense.

The powers that the competent authorities can exercise with respect to individual market infrastructures or individual types of DLT financial

2. Market infrastructures are required to: i) notify the activation of their transition strategy and the timescale of the transition (art. 3, par. 3, reg.); ii) submit monthly reports showing compliance with the thresholds for the value of the DLT financial instruments admitted to trading or registered in the infrastructure (art. 3, par. 5, reg.); iii) allow supervisory authorities access to information relating to operations on the market infrastructure (art. 4, par. 3, reg.); iv) inform the competent authorities of certain choices relating to the management of the infrastructure (art. 5, par. 9, paragraph 2, reg.).

instruments[3], are much more complex and characterized by wide margins of technical discretion, as evident, for example, in the case of the request to market infrastructures to adopt compensatory measures that they deem necessary to achieve the objectives pursued by the rules not applicable to market infrastructures that benefit from exemptions, or for the protection of investors and market integrity or financial stability (art. 4, par. 1, reg.; art. 5, par. 1, subparagraph 2, reg.; art. 6, par. 1, subparagraph 2, and par. 2, subparagraph 2, reg.), or for protection against other risks (art. 5, par.7, last paragraph, reg.).

III. ESMA'S SUPERVISORY POWERS

As regards the supervisory tasks of ESMA, this authority, in addition to being the active subject of a series of information obligations placed on the competent authorities[4], holds the power to issue guidelines on compensatory

3. In fact, the competent authorities have the power to: i) impose on market infrastructures the adoption of compensatory measures that they deem necessary for the achievement of the objectives pursued by the rules not applicable to market infrastructures that benefit from exemptions, or for the protection of investors, market integrity or financial stability (art. 4, par. 1, reg.; art. 5, par. 1, subparagraph 2, reg.; art. 6, par. 1, subparagraph 2, and par 2, subparagraph 2, reg.), or for protection against other risks (art. 5, par.7, last paragraph, reg.); ii) authorize the operations of persons other than those who, according to the general rules, can operate on a certain market infrastructure, requiring compliance with specific measures (art. 4, par. 2, reg.; art. 5, par 5, regulation); iii) grant exemption from compliance with specific requirements established by the rules that generally regulate the activity of the various market infrastructures (art. 4, par. 3, reg.; art. 5, par. 2, 3, 4, 6, 7, 8 and 9 reg.); iv) prohibit market infrastructures from following up on decisions regarding operations (art. 5, par. 9, paragraph 2, reg.); v) require market infrastructures to verify the technological devices adopted (art. 7, par. 4, third paragraph, reg.); vi) impose the adoption of specific prudential guarantees (art. 7 par. 6, third paragraph, reg.); vii) authorize updates to the transition strategy (art. 7, par. 7, third paragraph, reg.); viii) determine the date by which the agreements relating to the transition strategy must be adopted (art. 7, par. 10, reg.); ix) authorize operations as a market infrastructure (art. 8, par. 2, reg.; art. 9 reg.; art. 10 reg.); x) withdraw a specific permission or any related exemptions (art. 8, par. 12, reg.; art. 9, par. 12, reg.; art. 10, par. 12 , reg.).
4. Since it has been established that these must: i) make the information received from market infrastructures available to ESMA (see for example art. 4, par. 3, third paragraph, regulation, but similar provisions are envisaged for all infrastructures market); ii) communicate applications for authorization as market infrastructure to ESMA (art. 8, par. 6, subparagraph 2, reg.; art. 9, par. 6, subparagraph 2, letter a, reg.; art. 10, par. 7, subparagraph 2, letter b, reg.); iii) communicate to ESMA the granting, refusal or withdrawal of the authorization to a market infrastructure (art. 8, par. 11, subparagraph 2, reg.; art. 9, par. 11, subparagraph 2, reg. ; art. 10, par. 11, reg.).

measures that the supervisory authorities must comply with when they authorize an exemption and in general to protect investors, market integrity and financial stability, and on other aspects that characterize the functioning of market infrastructures (art. 4, par. 6, reg.; art. 5, par. 12, reg.; art. 8, par. 8, reg.; art. 9, par. 8, reg.).

The regulation also contains a series of provisions on the administrative procedure aimed at obtaining authorization to operate as a DLT market infrastructure, within which ESMA is granted the power to provide the competent authority with a «non-binding» opinion on the exemptions that have been requested or «on the adequacy of the type of distributed ledger technology used», if it deems it necessary «to promote the consistency and proportionality of exemptions, or where necessary to ensure investor protection, market integrity and financial stability» (art. 8, par. 7, paragraph 1, reg.; art. 9, par. 7, paragraph 1, reg.; art. 10, par. 8, reg.). The issuing of the opinion takes place after consulting the competent authorities of the member states, whose opinion must be taken «utmost account» (art. 8, par. 7, subparagraph 2, regulation; art. 9, par. 7, subparagraph 2, reg.; art. 10, par. 8, subparagraph 2, reg.), while the competent authority must «give that opinion due consideration» and, upon request from ESMA, provide a statement regarding any deviations from the opinion itself (art. 8, par. 7, subparagraph 3, reg.; art. 9, par. 7, subparagraph 3, reg.; art. 10, par. 8, subparagraph 3, reg.).

IV. COOPERATION BETWEEN OPERATORS OF DLT MARKET INFRASTRUCTURES, COMPETENT AUTHORITIES AND ESMA

Finally, the regulation provides for cooperation between market infrastructure operators, competent authorities and ESMA (art. 11 reg.). This general duty is divided into more specific obligations, by providing for a series of information to be given by the operators of the market infrastructures to the competent authorities (art. 11, par. 1, 2 and 4, reg.), and by recognizing to the competent authorities powers which in some cases are expressly traced back to those already provided for by other provisions (see for example art. 11, par. 1, paragraph 3, reg.), or completely different, such as the power to ask the operators to adopt corrective measures concerning the business plan, the DLT market infrastructure rules, the legal framework for investor protection, market integrity or financial stability (art. 11, par 3, reg.).

ESMA is recognized as having a coordination role among the competent authorities, with the aim of promoting «a common understanding of distributed ledger technology and DLT market infrastructure, to establishing a common supervisory culture and the convergence of supervisory practices, and to ensuring consistent approaches and convergence in supervisory outcomes» (art. 11, par. 5, reg.), to achieve which the mutual exchange of information is required from the competent authorities and ESMA, and ESMA is required to monitor the authorizations, exemptions and compensatory and corrective measures ordered by the competent authorities, reporting to the Commission on these (art. 11, par. 6, reg.). Obviously, the coordination of supervisory practices could also occur spontaneously through the exchange of information - this aim, together with that of encouraging the dissemination of information about these practices among operators, would also appear to be pursued by the interim report that ESMA must publish periodically annual pursuant to art. 15, reg. – although it seems likely that the latter will be requested above all for the purpose of providing ESMA with the materials to refer to in the development of its guidelines and non-binding opinions provided for by other provisions of the regulation, and the Commission elements to be taken in to account for the future initiatives, including legislative ones, on the matter (see art. 14, par. 2, reg.).

V. CONCLUSIONS: INNOVATIVE NATURE OF ESMA'S COMPETENCES ON DLT MARKET INFRASTRUCTURES

It is now necessary to determine whether the supervisory system emerging from the rules mentioned above is consistent or not with the provisions on the ESFS, and specifically with the provisions of regulation (EU) no. 1095/2010 establishing ESMA[5].

5. The problem of the compatibility with the european Treaties of the powers attributed to ESMA by regulations subsequent to its establishment has already been addressed by the Court of Justice in the Judgment of the Court (Grand Chamber) of 22 January 2014, Case C-270/12, which, in relation to the provisions contained in the art. 28 reg. (EU) no. 236/2012, ruled out that: i) there is a violation of the principles regarding the delegation of powers set out in the Meroni/High Authority Judgment due to ESMA having been invested with discretionary power, when the Authority's decisions are "circumscribed by various conditions and criteria which limit ESMA's discretion" (paragraph 45); ii) there is a violation of a principle enunciated in the Romano Judgment, due to the Authority having been invested with the power to adopt "quasi-legislative acts" of general scope of application, since " the institutional framework established by the FEU Treaty, in particular the first paragraph of Article 263 TFEU and Article 277 TFEU, expressly permits Union bodies, offices and agencies to adopt acts of general application" (paragraph 65); iii) there is no delegation of powers incompatible with

Preliminary to any evaluation is the problem of the lack, within the regulation (EU) no. 1095/2010, of references to the regulation on DLT market infrastructures, where the competences of ESMA are identified by referring to the matters falling within the scope of application of some legislative acts specifically indicated by the art. 1, par. 2, reg. (EU) no. 1095/2010. In the case of the repeal of the legislative acts referred to in art. 1, par. 2, reg. (EU) no. 1095/2010, European legislators have generally made use of comparison tables, which have had the function of indicating which act needs to be looked at following the repeal, but it is clear that this system can not be used in this case, which would have instead required an express modification or

---

Articles 290 TFEU and 291 TFEU, since "while the treaties do not contain any provision to the effect that powers may be conferred on a Union body, office or agency, a number of provisions in the FEU Treaty none the less presuppose that such a possibility exists" (paragraph 79); iv) there is no violation of Article 114 TFEU, since "the EU legislature, in its choice of method of harmonisation and, taking account of the discretion it enjoys with regard to the measures provided for under Article 114 TFEU, may delegate to a Union body, office or agency powers for the implementation of the harmonisation sought. That is the case in particular where the measures to be adopted are dependent on specific professional and technical expertise and the ability of such a body to respond swiftly and appropriately" (paragraph 105).

On the problems posed by the powers attributed to ESMA see P. Iglesias-Rodríguez, *ESMA as a Residual Lawmaker: The Political Economy and Constitutionality of ESMA's Product Intervention Measures on Complex Financial Products*, in *European Business Organization Law Review*, July 2021; D. Adamski, *The ESMA Doctrine: A Constitutional Revolution and the Economics of Delegation*, in *European Law Review*, December 2014, 812-834, E.J. Howell, *The Evolution of ESMA and Direct Supervision: Are there Implications for EU Supervisory Governance?,* in *Common Market Law Review,* June 2017; M. van Rijsbergen, M. Scholten, *ESMA Inspecting: The Implications for Judicial Control under Shared Enforcement*, in *European Journal of Risk Regulation*, September 2016, 569-579; G. Deipenbrock, *Direct Supervisory Powers of the European Securities and Markets Authority (ESMA) in the Realm of Credit Rating Agencies. Some Critical Observations in a Broader Context,* in *European Business Law Review*, April 2018, 169-203; D. Kull, *Legal Implications of the Establishment of the European Securities and Markets Authority*, in *SSRN*, August 2011; C. Di Noia, M. Gargantini, *The European Securities and Markets Authority: Accountability Towards EU Institutions and Stakeholders*, in *SSRN*, January 2013; Idem, *Unleashing the European Securities and Markets Authority: Governance and Accountability After the ECJ Decision on the Short Selling Regulation (Case C-270/12),* in *European Business Organization Law Review*, March 2014, 1-57; P. Schammo, *The European Securities and Markets Authority: Lifting the Veil on the Allocation of Powers,* in *Common Market Law Review*, November 2011; N. Moloney, *The European Securities and Markets Authority and Institutional Design for the EU Financial Market – A Tale of Two Competences: Part (1) Rule-Making*, in *European Business Organization Law Review*, March 2011, 41-86; Idem, *The European Securities and Markets Authority and Institutional Design for the EU Financial Market – A Tale of Two Competences: Part (2) Rules in Action*, in *European Business Organization Law Review*, June 2011, 177-225.

integration of the provision of art. 1, par. 2, reg. (EU) no. 1095/2010 which, however, has not been adopted. Nonetheless, the fundamental obstacle to the subsumption of the supervisory powers provided for by the regulation (EU) 2022/858 is not only a consequence of the contents of art. art. 1, par. 2, reg. (EU) no. 1095/2010, but mainly of art. 8, par. 1, letter a), reg. (EU) no. 1095/2010 which after having established that ESMA contributes «to the establishment of high- quality common regulatory and supervisory standards and practices», specifies that this contribution is achieved «by providing opinions to the Union institutions and by developing guidelines, recommendations, and draft regulatory and implementing technical standards which shall be based on the legislative acts referred to in Article 1(2)» and therefore without the possibility of misinterpreting the will of the European legislators to limit ESMA's competence only to measures and acts that may be traced back to the provisions of the legislative acts specifically indicated by the art. 1, par. 2, reg. (EU) no. 1095/2010. It is therefore clear that all the responsibilities falling to ESMA based on the reg. (EU) 2022/858 constitute new competences that integrate those provided for by the reg. (EU) no. 1095/2010, and which must be considered legitimate having been provided for within a provision of the same nature as that used for the original assignment of tasks to the authority.

The innovative nature of reg. (EU) 2022/858 is evident not only from the point of view of the authority's competences, but also from a procedural point of view. Having regard to the guidelines, the regulation does not indicate particular procedural requirements, and this raises the problem of establishing whether – since the competences provided for by the regulation are not the same provided in (EU) no. 1095/2010 – the procedure regulated in art. 16 reg. (EU) no. 1095/2010 must be observed, or whether the obligations envisaged by this same article, regarding prior consultation and "cross-examination" in the event of disagreement by the supervisory authority, can still be applied as an expression of a principle of reasonableness in administrative action. Also the ESMA opinions required by the reg. (EU) 2022/858 do not find any correspondence in the procedures regulated by the Reg. (EU) no. 1095/2010, which also allows ESMA the possibility to express its opinion to the competent authorities as a tool to build « a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union» (art. 29, par. 1, reg. (EU) no. 1095/2010), but without regulating its object or procedure, and above all without providing for its inclusion within authorization procedures under the competence of the national authorities. Despite the impossibility of tracing them back to provisions of the regulation

establishing ESMA, these measures and their regulation must in any case be considered legitimate from a formal point of view, being foreseen within a provision having the same rank of reg. (EU) no. 1095/2010 in the European system of sources of law.

Labour law

The digitalization of public employment services: different European practices and models compared

[1]Federica Nizzoli*

SUMMARY: I. INTRODUCTION - II. THE DEMATERIALISATION OF ACTIVE LABOUR MARKET POLICIES AND ITS IMPLICATIONS - III. THE ROLE OF DIGITAL PLATFORMS IN PUBLIC EMPLOYMENT SERVICE - IV. THE ALGORITHMIC PROFILING - V. THE AUTOMATED JOB-MATCHING APPLICATIONS - VI. THE EXPERIENCE OF ONLINE-BASED TRAINING - VII. CONCLUSIONS AND FUTURE PERSPECTIVES

ABSTRACT: This essay analyses the increasing role played by the dematerialization of public services due to the process unanimously acknowledged as digitalisation in several European countries, taking into account its implications especially among active labour market policies.

Subsequent to the needs arising from the Covid-19 pandemic, attention will be focused on four fields related to work: the role of digital platforms; the algorithmic profiling process; the automated job-matching platforms as well as the so-called web-based training, each of them is deeply connected with the aims set inside the "Recovery and Resilience Facility" along with the EU-wide investment plan known as "Next Generation EU". The role of public employment services will also be tackled in the light of beneficing customers in terms of accessibility, transparency, and inclusivity of provisions regarding dematerialisation.

KEYWORDS: Public employment services; digitalization; job-matching; platforms; online-training; profiling; algorithm.

* PhD Student, Unviersity of Modena and Reggio Emilia.

I. INTRODUCTION

Global economy and labour markets have been badly impacted by the Covid-19 issue. In the context of this crisis, we have had the opportunity to notice how social policies of States had a drastic impact on the work of people and on business operations to the extent that they have been identified as "part of a broader strategy that encompasses public health and macro-economic concerns"[1].

In particular, most employment services were forced to migrate their support and intermediation services on platforms or deliver them over the phone during the pandemic. In order to guarantee an acceptable response from the Employment Services in terms of providing fundamental services themselves, the pre-emptive deployment of technology and the capacity for swift adaptation proven to be success factors. We have had to make decisions on a variety of internal reorganization-related difficulties, while juggling a rapidly expanding workload, changing service demand, supporting the employment of disadvantaged individuals, and responding to changes in the demand for services (e.g. the recruitment of new staff with more digital skills or the reallocation of existing staff).

The pandemic has accelerated the digital transformation process and the latter influenced the demand for new skills in the labour market. At the same time, technological change also brings with it the possible transformation or replacement of traditional occupations. Therefore, if the supply of skills keeps up with the demands coming from the labour market, such transitions could raise concerns about the possibility of technological unemployment and create chances in new professions[2]. This can also bring up consequences in terms of organizational changes in the workplace and which require new ways of carrying out work performance, together with the need to invest in training or retraining of the workforce by companies and institutions.

For instance, she so-called Italian Employment Centres (*Centri per l'impiego*) – which are intended to use technology more and more in their operations –

1. See B.T. Haar, E. Menegatti, I. Senatori, E. Sychenko, *Editorial*, in *Italian Labour Law e-Journal*, n. 13/2020, 1, specifically, although precautions suggested by the epidemiologic science to mitigate the spread of the disease were the same worldwide, national governments and legislators translated them into specific policies and normative solutions, according to each field of interest.
2. C. Frey, M.A. Osborne, *The future of employment: How susceptible are jobs to computerisations?*, in *Technological Forecasting and Social Change*, Elsevier, 114(C), 2013, 254-280; E. Brynjolfsson, A. Mcafee, *The second machine age: work, progress and prosperity in a time of brilliant technologies*, New York, WW Norton & CO, 2014.

will likely see increased demands from both internal and external sources[3]. Customers' requests for services will vary dramatically, and one of the key areas to pay attention to will be the support for vulnerable worker groups, such as those with limited digital skills, long-term unemployed, those in their 50s or older, or those with impairments. However, it is anticipated that these measures will change from being financial incentives to programmes involving training.

The aim of this paper is therefore to assess the dematerialisation of public employment services, meaning how the digital transformation is affecting the labour market by carrying out a comparative analysis among various Member States, characterized by different models and approaches to employment services and digitalization as well[4].

Given the complexity and heterogeneity of the fields under consideration, it is important to take into account also how technological innovation does not only change the typology of professions required, but also the methods of research and recruitment of staff by entrepreneurs[5]. In view of the difficulty of listing all the measures that characterize the dematerialisation of public employment services, it is appropriate to focus on four distinct areas: digital platforms; algorithmic profiling process; automated job-matching platforms and web-based training.

This choice is explained by the fact that these areas represent the field of active labour policy most sensitive to the issue of digitalisation, considering how new technologies can impact access of services way beyond procedures for registering and taking care of unemployed persons.

Furthermore, the biggest difficulty consists in how to design and organise a structure to make optimal use of the available technologies. In this sense, digitalization has been so far fundamental in order to activate, increase and expand the employment services to support job seekers and business affected by recent crisis. As a matter of fact, new IT tools are appearing and developing faster and faster, creating a state of constant change in which

3. Concerning the general measures adopted by the Italian Government to protect workers and undertakings from the impact of the COVID-19 pandemic see C. Gaglione, I. Purificato, O.P. Rymkevich, *COVID-19 and Labour Law: Italy*, in *Italian Labour Law e-Journal*, n. 13/2020.
4. The reference is to Austria, Denmark, Estonia, France, Greece, Germany, Italy, Netherlands, Portugal, Spain, and Sweden.
5. See European Commission, *Annual Report. European Network of Public Employment Services (PES)*, Luxembourg, Publications Office of the European Union, 2022.

public employment services need to develop flexible strategies suitable for their own organizational models.

We might also consider how regular jobs – like registering job seekers or those requiring more complicated duties, like job matching and self-assessment tools – have changed as a result of automation and digitization. Rapid data and information processing, which will increase organisational efficiency and effectiveness and boost customer satisfaction, is a crucial component for achieving these objectives. The biggest problems in the coming years will concern data availability and quality. They will result in a quicker matching process and more accurate subject profiling, but they will also increase the emphasis on privacy, transparency, and the necessity for us to arm ourselves with proper computer security technology. These are topics originally almost exclusively pertaining to computer science and which become of interest for the field of organizational studies and public policies only in recent times.

II. THE DEMATERIALISATION OF ACTIVE LABOUR MARKET POLICIES AND ITS IMPLICATIONS

As previously mentioned, during the pandemic, public employment services introduced several organizational and preventive measures related to the necessity to provide services in the emergency. Many of the aforementioned changes consisted of investments in IT infrastructures[6]. Generally speaking, public employment services dematerialization is likely utilised interchangeably with the term "digitalization of services", even though these two concepts should not be totally overlapped with each other.

Currently we are witnessing a process of dematerialization of services, which is a widespread practice across all public services. Broadly defined "dematerialization" means the progressive increase in computerized document management and the replacement of the traditional supports of administrative documentation in favour of the computer document. In simple terms, we are working to reduce the number of materials required for the service offering itself. In order to accomplish this, information and communication technologies must be used, and this is how digitalisation of services comes into consideration. Moreover, in addition to enabling new kinds of collaboration and knowledge sharing, ensuring the security and

6. For instance, many ways of managing work performance were introduced, such as: remote or mixed work (presence-home alternation), the increasingly digitalised modes of providing services, the initiation of a generalised cultural change.

integrity of company data, and providing solutions to maximise the use of commercial spaces and resources more effectively, is crucial for enabling access to work services and products at any time, from anywhere[7].

On the basis of what we just pointed out, with the help of the digitalization process, employment services have unquestionably been major drivers of this progress. In fact, they can be seen as having a dual value that is both passive (via instruments that support income) and active (through initiatives that increase the employability of groups affected by the ongoing transformations). Active employment strategies and public employment services are especially important given the need to develop new skills. In addition, active policies themselves are impacted by technological change to the extent that the ways in which interventions are organized and delivered change, particularly as a result of data-intensive technologies that enable the processing of massive amounts of data[8]. These innovations offer the possibility of speeding up decision-making processes, reducing complexity for citizens and allowing companies and public institutions to provide services and assistance to their users in real time.

The recent Industry 4.0 debate has led to increased attention in the public sector for Data-driven decision making (DDD); the practice of basing decisions on the analysis of data rather than purely on intuition and whose benefits have already been demonstrated conclusively[9]. For the purposes of this discussion, however, the goal is rather to understand the extent to which approaches based on data analysis can replace or complement traditional approaches in determining relevant choices within an organization[10].

In particular, DDD research has become increasingly popular in recent years, particularly in light of the interest in machine learning and artificial intelligence applications that could "automate" public sector operations and decision-making processes. Databases that feed these apps, in exchange,

7. N. Lettieri, *Making smart working smarter. Intelligenza artificiale e prospettive di evoluzione del lavoro agile*, in R. Zucaro (ed.), *Verso lo smart working? Un'analisi multidisciplinare di una sperimentazione naturale*, INAPP Report, n. 30, Roma, 117-131.
8. As a matter of fact, the most recent technological changes are characterized by the growing availability of data and the continuous improvement of the ability to manage this information.
9. E. Brynjolfsson, L.M. Hitt, H.H. Kim, *Strength in numbers: How does data-driven decision making affect firm performance?*, in *SSRN working paper*, 2011.
10. F. Provost, T. Fawcett, *Data science and its relationship to big data and data-driven decision-making*, in *Big data*, n. 1/2013, 51-59.

enable long-term monitoring of the services offered[11]. Greater efficiency, quicker decision-making, cheaper costs, and improved impartiality of the resulting decisions are all advantages of automated administrative decision-making in public administration[12].

Nevertheless, leaving aside the listed benefits, not all national public employment services are able to take advantage of these technologies. The problematic aspects can in fact be traced back mainly to two types of reasons. In the first place, reference is made to issues related to the technological infrastructural endowment and the skills of operators and users[13]. Specifically, the potential absence of personal electronic devices, access points, broadband or ultrabroadband network coverage, as well as basic digital skills, could pose a risk of producing unintended consequences, as the introduction of new technologies in these circumstances would end up limiting rather than improving service accessibility[14]. Second, it should be noted that the ability of the operators to accept the resulting changes should not be overlooked, nor should the possibility that they may exhibit some resistance in the face of such innovations. The successful integration of existing and emerging technologies in this context depends not only on the users' skills and the available technological equipment. Thus, it is crucial to develop the required training programmes to give operators a sense of security and competence as well as to build the tools so that they are able to meet their goals[15]. In this scenario, therefore, the observation made in a recent report according to which "the success of any technological innovation is determined by the degree to which people are able to interact with it"[16] seems to be true.

---

11. P. Morrel-Samuels, E. Francis, S. Shucard, *Merged datasets: an analytic tool for evidence based management*, in *California Management Review*, n. 52/2009, 120-139.
12. E. Wihlborg, H. Larsson, K. Hedström, *"The Computer Says No!" – A Case Study on Automated Decision-making in Public Authorities*, Paper fort the 49th Hawaii International Conference on System Sciences (HICSS), 2016.
13. Indeed, a frequent theme in the public debate concerns access to digital media by the most vulnerable groups lacking the necessary skills to make the best use of the available services.
14. T. Hooley, J. Hutchinson, A.G. Watts, *Careering Through The Web The potential of Web 2.0 and 3.0 technologies for career development and career support services*, UK Commission for Employment and Skills, London, 2010; European Commission, *European Network of Public Employment Services: dematerialisation of services in EU PES*, 2020, 13 ss.
15. G. Scarano, *Politiche attive del lavoro e servizi per l'impiego: tra miti e riforme*, Milano, 2021, 280.
16. W. Pietersen, *Digital technologies and advanced analytics in PES*, in *www.ec.europa.eu*, EC, Brussels, 2019.

Many academics have focused on additional user-related issues, including privacy concerns, the existence of discrimination through the intensive use of data, transparency issues, and the so-called "explainability of algorithms"[17]. In fact, users in this setting are routinely exposed to billions of online devices that passively gather information without the users' complete knowledge. To balance the interests of all parties involved, it is crucial to comprehend how data is generated and how much the individual is involved in its generation and gathering[18].

According to the interests and goals established by national governments, many countries have adopted various strategies aimed at integrating new digital technology in public employment services. The goals themselves frequently discuss the need to save expenses while attempting to raise service quality through new innovations. It is important to take into account multi-channel management[19], which refers to the coexistence of many channels for interaction and communication between operators and users, as one of the earliest methods created for remote user management. In other words, the channels are interchangeable and each one can offer each service in a different way, allowing the consumer to select their preferred media freely[20].

The conditions have been set for some national public employment services to start developing a so-called "digital first" or "digital only" strategy, which establishes that digital channels are the primary ones for accessing and using services. These conditions have been created by recent technological advancements, along with the effects of the economic crisis,

17. See M. Veale, M. Van Kleek, R. Binns, *Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making*, in Atti della *CHI'18 – Conference on Human Factors in Coputing Systems*, Montréal, 21-26TH April; J.P. Olsen, Democratic Order, Autonomy and Accountability, in Governance, n. 28/2015, 425-440; M. Buiten, Towards Intelligent regulation of Artificial Intelligence, in European Journal of Risk Regulation, 10, 2019, 41-59.
18. WEF, *Data-Driven Development. Pathways for Progress*, World Economic Forum Report, Cologny, 2015.
19. The official definition given by Teerling et al. states that multi-channel management "is the effective and efficient deployment of channels for the communication, interaction, transaction with and/or distribution of products/services to the client", see M. Teerling (ed.), *Multi-channel management; de stand van zaken. [MultiChannel Management; State of the Art]. Enschede: Telematica Instituut*, 2007.
20. W. Pieterson, *The challenges and obstacles towards PES digitalisation and* differentiation, in *Centre for e Government studies*, Twente, 4-5th December 2017; European Commission, Blended service delivery for jobseekers, in Peer Review Comparative Paper, Brussels, 2014; P.G. Bresciani, A. Sartori, Innovare i servizi per il lavoro : tra il dire e il mare... : apprendere dalle migliori pratiche internazionali, Milano, 2015.

which have forced severe cuts in public spending in many countries. In order to concentrate on-site assistance on users who demonstrate a greater disadvantage, this approach can vary depending on whether the user is only required to register on the services website before visiting an office or whether he is required to use digital channels only (digital only), without the possibility of going to the office before a certain period has passed. In recent years, countries that have taken this path have gone beyond simply improving internet channels by gradually incorporating tools that support effective DDD using AI and machine learning-based technology[21].

Finally, it seems necessary to say a few words limited to the issue of e-government[22]. Digitization in the public sector has in fact already attracted, in the past, the attention of studies dedicated precisely to e-government, as an area of public sector reform. Leaving aside the tripartition of definitions provided by the OECD on the subject[23] - which are, however, overlapping -, it is sufficient to recall how e-government and digitalization are related to public employment services in many ways. For instance, e-government initiatives in the realm of public employment services often involve the creation of online job portals or platforms where job seekers can search for job opportunities, submit their resumes, and apply for positions. These online resources can make the job search process more efficient and give users access to a wider variety of positions. Moreover, digitalization allows for the development of automated job matching algorithms. These algorithms use job seekers' qualifications and preferences to match them with suitable job openings, increasing the chances of successful job placements. Again, digital platforms can provide access to online training and education resources, enabling job seekers to acquire new skills and improve their employability as well as collect and analyse data on job market trends, unemployment rates, and skills demand. Overall, it is possible to conclude by stating that the digitalization of public employment services through e-government initiatives aims to create a more accessible, efficient, and user-friendly

21. Nt. (13), 281.
22. Generally speaking, the term refers to the use of digital technologies and information and communication technologies (ICTs) to provide government services, facilitate interactions between government and citizens, businesses, and other government entities, as well as improve the efficiency and transparency of government processes. The goal of e-government is to enhance the accessibility, convenience, and effectiveness of public services while streamlining administrative processes.
23. OECD, *Managing Decentralization: a new role for labour market policy,* Paris, OECD Publishing, 2003.

experience for both job seekers and employers while contributing to more effective labour market outcomes and economic growth[24].

III. THE ROLE OF DIGITAL PLATFORMS IN PUBLIC EMPLOYMENT SERVICE

Digital platforms have emerged as game-changing technologies that are redefining the landscape of job-seeking and public employment services in a time when technology is constantly evolving. A new paradigm has emerged as a result of the convergence of e-government projects and digitalization, one in which both employers and job searchers must negotiate a sort of linked universe of virtual chances. The influence of new technology on service access, however, goes beyond the simple computerization of processes for registering and managing unemployed people. In fact, these are connected to counselling and guidance activities as well as new channels via which people can learn about their options for work, education, and training[25]. In this sense, researchers are now focusing on the remote and flexible ways that online services might offer counsel, guidance, and support.

Since the development of the Internet has accelerated over the past 20 years, public employment services have been able to create their own websites and online platforms that anybody can access right away from anywhere. In this sense, expanding service accessibility would be made feasible through the creation of novel and distinctive modes of engagement and communication[26]. In reality, many of these innovations were initially designed to make it simpler for those who live far from offices or in outlying locations to access services[27].

---

24. See V. Homburg, V. Bekkers, *E-government and NPM: a perfect marriage?*, in V. Bekkers, V. Homburg (eds.), *The information ecology of e-government: E-government as institutional and technological innovation in public administration*, Amsterdam, IOS Pess, 2005; A. Cordella, *E-government: towards the e-Bureaucratic Form?*, in *Journal of Information Technology*, n. 22/2007, 265-274.
25. J. Bimrose, J. Kettunen, T. Goddard, *ICT – the new frontier? Pushing the boundaries of careers practice*, in *British Journal of Guidance and Counselling*, n. 43/2015, 8-23; J. Kettunen, *Career practitioners conceptions of social media in career services*, in *Finnish Institute fort Educational Research Studies*, n. 32/2017.
26. T. Hooley, J. Hutchinson, A.G. Watts, *Careering through the web: the potential of web 2.0 and 3.0 technologies for career development and career support services*, in *UK Commission for Employment and Skills*, London, 2010.
27. Part of the debate, in this regard, has focused on the relationship between online and face-to-face services, questioning the possibility that the former can completely replace the latter or integrate with them, to improve the quality of services. In this

However, these platforms have an impact that goes beyond simple convenience. They have the ability to fundamentally alter how public employment services are provided. The power of big data is now being used by automation and artificial intelligence algorithms to provide personalised job recommendations that match candidates' talents, qualifications, and aspirations with open openings. This seamless digital integration speeds up the hiring process, improving effectiveness and encouraging a more diverse labour market.

Nevertheless, it is indisputable that since the pandemic emergency, the significance of these technologies has grown with time. As was already noted, Covid-19 has contributed to the diversity of user communication channels by acting as an accelerant. Every nation has been compelled by the restrictions to shift towards hybrid or entirely remote means of delivery. Among them, situations where digital tools and multi-channel tactics have already been deployed for a while were recognised as having greater speed and efficacy in adaption[28].

Moreover, it is possible to note how the network can be used for procedures, such as registration in the public employment services system[29]. Typically, this results in the development of a personal account with the user's personal information on the web platforms of the public employment services. The portals might also include broad data on job listings, skill demand patterns, and labour market trends. Some platforms provide specialized tools that are typically meant to encourage self-exploration of the platform and assessments that try to match a person's interests with professional or academic fields or reveal the need for more intense help. The operator and user can communicate by phone, email, through the platform itself, or by being automatically referred to a following interview (online or in person).

On the basis of what said it is possible to note how, on the one hand, for employers these platforms provide an avenue to showcase their organizations, interact with potential candidates, and expedite the recruitment process. Digital platforms allow clear and effective communication between

regard, see A.G. Watts, *The role of information and communication technologies in integrated caeer information and guidance systems: a policy perspective,* in *International Journal for Educational and Vocational Guidance*, n. 2/2002, 139-155.

28. CEDEFOP, *Online working and learning in the Coronavirus era,* in *CEDEFOP Briefing Note – 9148,* 2020.

29. This registration is often a procedure that is necessary for an unemployed person who intends to apply for certain economic benefits.

businesses and job seekers by improving the information flow, expediting the recruiting process and reducing pointless administrative barriers. On the other hand, for job seekers digital platforms represent an evolution in the job-seeking process. They offer convenience, efficiency, and empowerment, enabling individuals to navigate a competitive job market with greater confidence and strategic acumen. These platforms serve as guiding lights for job seekers, enabling a more inclusive and accessible employment ecosystem as e-government efforts and digitalization continue to transform public employment services.

Having briefly analysed the main implications of digital platforms in the context of public employment services, it is now possible to consider the experiences of certain platforms used by some European states witnessing the progressive dematerialisation of services along with the development of technologies in active labour market policies.

Greece has established a specialised online platform called myOAEDlive to enable counselling services via teleconferencing as an alternative to in-person or on-site supply[30]. When it was first introduced in December 2020, the platform's initial goal was to offer tele-counselling services to companies and unemployed people in the Covid-19 crisis. As a result of the success of this effort, this customer support system was made permanent. Individuals can get interpretation services in a variety of foreign languages and Greek sign language through this programme. The platform also provides customised counselling for vulnerable populations experiencing major employment challenges, such as young people, migrants, refugees, and persons with impairments[31]. Generally speaking, the platform aims to support both employers and unemployed by guaranteeing the provision of uninterrupted services by the public employment services themselves. The key tasks accomplished as a result of this platform included the ability to create a detailed strategy for tele-counselling implementation, send out an invitation of interest to counsellors who wanted to join the team on a volunteer basis, and train counsellors technically.

Regarding the Danish experience, Jobnet.dk – an online platform for public employment services – must be taken into account. Users are required

30. Concerning digital transformation in Greece in the last years *see* A. Vratimos, *Digital Transformation & COVID-19: the Case of Greece*, in *European Scientific Institute*, 2022; about the myOAEDlive platform *see* European Commission, *MyOAEDlive: Tele-counselling services to jobseekers and employers*, in *www.ec.europa.eu*, 2021.

31. OECD, *Harnessing digitalisation in Public Employment Services to connect people with jobs*, in *www.oecd.org*, 2022.

to post their curriculum so that operators and businesses can view it, which is how many other platforms operate. Companies can publish job offers to the platform, allowing job seekers to independently apply. After registering on the platform, the user can also book a meeting with an operator, thanks to which a real activation program (called My Plan) will be defined. Through the website, the operator can stay in touch with the user directly and stay updated on their research activities. A particular notification will appear on the user's account in cases where an application should receive positive reviews. The operator as well will also receive this communication from the platform[32]. Jobnet represents the labour market policy principles of empowerment of jobseekers, customisation of services, and user-friendliness by allowing jobseekers to search amongst all job vacancies in Denmark. It also enables jobcentres, Unemployment Insurance Funds (UIF), employers, and jobseekers to better communicate and exchange information, as well as permitting job counsellors to monitor job-seeking activities, and employers to find suitable candidates for vacancies.

Even the Italian context is not devoid of examples regarding digital platforms in public employment services. Specifically, MyAnpal is an online platform developed by ANPAL (*Agenzia Nazionale Politiche Attive del Lavoro*), the National Agency for Active Labor Policies. By providing a variety of features, such as job searching, job matching, and career development tools for job seekers, it serves as a comprehensive digital link for employment and job-related services in Italy[33]. Additionally, it offers resources so that companies may interact with people and publish job openings. To help users in making well-informed decisions, the online tool integrates data on the labour market, training possibilities, and employment markets. By fostering effective and transparent communication within the labour market, MyAnpal seeks to close the communication gap between companies and job seekers. Therefore, MyAnpal plays a crucial role in enhancing employability, job matching, and workforce development across Italy's labour landscape, contributing to a more effective and efficient employment ecosystem. Users can access tailored job recommendations and training suggestions through personalized profiles.

Among the European experiences just reported, the French one is certainly characterized by its peculiarity: in fact, it is not a platform merely

32. T. Dall Schmidt, T. Mitze, *Crisis and the welfare state: the role of public employment services for job placement and the Danish flexicurity system during COVID-19*, in *Cambridge Journal of Regions, Economy and Society*, n. 16/2023, 65–79.
33. N. Duell, *PES working group on new forms of work*, in *www.europa.eu*, 2020, 20.

dedicated to the possibility of bringing together job supply and demand by registered users and companies, but rather a new form of dialogue on innovation between management and counsellors. The French public employment services (*Pôle Emploi*) used the online platform InnovAction to function initially around challenges, ideas, and practise submission to stimulate participation from all public employment services employees. The initial platform was modified and split into two in June 2019. Even though employees of public employment services can still submit their ideas outside of the challenges, InnovAction has grown into a more ergonomic platform with a greater focus on challenges. Employees participate in the ideas and challenges by offering and debating their own concepts. The management of local, regional, and national public employment agencies selects ideas from the InnovAction idea pool to test out on a small-scale. Each idea tested is followed up by the Department for Innovation, which informs the public employment services General Management Committee about the developments[34].

IV. THE ALGORITHMIC PROFILING

In the ever-evolving landscape of public employment services within the European context, a new dimension has emerged that holds the potential to revolutionize how job seekers and employment agencies interact: algorithmic profiling. In an era driven by data and digital transformation, algorithms have become pivotal tools that enable public employment services to enhance their effectiveness, efficiency, and precision in matching job seekers with suitable opportunities. However, as these algorithms delve into the intricate realm of individual profiles and preferences, questions arise about fairness, transparency, and the ethical implications of algorithmic decision-making. Understanding the advantages and difficulties of algorithmic profiling, its effects on both job searchers and agencies and the procedures in place to ensure a fair and balanced approach are all necessary for navigating its complexities in the European public employment services scene. This investigation reveals the complex nature of algorithmic profiling and how it will affect the way in which employment services are provided in the future throughout the European Union.

That being said, undoubtedly, user profiling is the process that has the greatest implications from the point of view of the intensive use of data and

34. European Commission, *InnovAction: a collaborative platform to put ideas into practice*, in *www.europa.eu*.

algorithmic technologies in employment services. Differentiated approaches have emerged as a result of the increasing sophistication of the technology used in this field. The comparison of the various profiling models created in multiple countries actually takes up a significant portion of the discussion surrounding the digitization of public employment services.

Recent studies have offered an overview of some profiling tools developed, distinguishing three different models: procedural rule-based approaches; approaches based on the operator's discretion through service guidelines and data-intensive approaches which envisage the use of statistical and algorithmic processing[35]. Because they are thought to be able to guarantee a more "objective" and standardised treatment of users than approaches based on the operator's discretion, models based on data-intensive approaches have particularly attracted the growing interest of scholars and policy-makers among the profiling tools mentioned[36].

It should be noted that similar profiling techniques also help establish which subjects need to intervene with priority in countries that use a digital first rationale for their public employment services. In this manner, we identify the users who need to be called for an appointment in person with an operator and more easily employable users who can manage themselves. Further potential also derives from the possibility of effectively using click-data to obtain information related to user behavior in terms of active job search.

The European reality requires us to consider some examples of algorithmic profiling worthy of note. In some circumstances, profiling can be used to determine whether individuals need to get assistance from public or private providers, with the most disadvantaged individuals requiring more specialized services available on the market. In order to improve the effectiveness of its counselling process and active labour market programs, the Public Employment Service Austria (AMS) developed a specific algorithmic profiling of job searchers[37]. The system, which has come to

35. *See* S. Desiere, K. Langenbucher, L. Struyven, *Statistical profiling in public employment services: an international comparison,* in *OECD Social, Employment and Migration Working Papers*, 224, Paris, 2019.

36. See A. Loxha, M. Morgandi, *Profiling the unemployed: a review of the OECD experiences and implications for emerging economies,* in *Social Protection & Labour Discussion Paper,* 1424, 2014; P. Arni, A. Schiprowski, *The effects of binding and non-binding job search requirements,* in *IZA Discussion Paper*, 8951, 2015.

37. D. Allhutter, F. Cech, F. Fischer, G. Grill, A. Mager, *Algorithmic Profiling of Job Seekers in Austria: How Austerity Politics Are Made Effective*, in *www.frontiersin.org*, 2020,

be known as the AMS algorithm, is built to categorise clients of the AMS into three groups: those with high chances to find a job within half a year; those with mediocre prospects on the job market; and those clients with a poor outlook of employment in the next two years. Different types of assistance will be provided to job seekers in (re)entering the labour market depending on the category they fall under. Less assistance will be provided to those in the least problematic categories because it is assumed that they will find employment on their own; however, those in the categories with poor employment prospects will be outsourced to private services because they need the most expensive activation programmes.

It should also be added that among the public employment services that have consolidated a profiling tool capable of effectively managing behavioral variables is the case of the Dutch so-called Work Profiler. Almost all registered unemployed people receive electronic service under this type of programme during the first three months of registration. E-services include a digital portal for each jobseeker to organise their search and integration activities as well as an online tool for profiling. Employment counsellors keep an eye on the activities and offer jobseekers guidance and other sorts of help for successful job searching[38].

In this sense, the use of algorithmic profiling systems it is something findable as well in the Portuguese country, where in 2022 IFEP – the Portuguese public employment services – started a partnership with a research team at NOVA School of Business and Economics to develop an intelligent new profiling system based on big data approaches using machine learning algorithms[39].

That said, although algorithmic profiling is a digital practice that is finding sufficient diffusion in many European countries, this does not imply that it is free from problematic aspects and limitations on the perspectives of both operators and users. The first, on the one hand, point out how developing and maintaining accurate and effective algorithms requires significant resources,

---

investigates crucial conceptual, technical, and social implications of the aforementioned system; P. Lopez, *Reinforcing Intersectional Inequality via the AMS Algorithm in Austria*, in *Proceedings of the STS Conference Graz*, 2019.

38. M.A. Wijnhoven, E. Dusseldorp, M. Guiaux, H. Havinga, *The Work Profiler: Revision and maintenance of a profiling tool for the recently unemployed in the Netherlands*, in *International Social Security Review*, 2023; European Commission, *The 'Work Profiler' and the 'Personal Work Folder'– a digitalised master plan for integration into the labour market*, in *www.ec.europa.eu*, 2017.
39. European Commission, *Piloting a new digital profiling system*, in *www.ec.europa.eu*, 2022.

including technical expertise, time, and financial investments and how, since algorithms depend on data quality, if the data is biased or incomplete, it can lead to skewed results and reinforce existing inequalities. The main concerns of the latter, on the other hand, were about lack of transparency and loss of personalization. By virtue of these considerations algorithmic technology may have unintended consequences, where the initial goals of impartiality and standardisation are replaced with new kinds of user injustice. On the other hand, proponents of data-intensive techniques highlight how these technologies really enable the creation of prejudice that is embedded in the labour market and that is discounted in public discourse[40].

V. THE AUTOMATED JOB-MATCHING APPLICATIONS

Public employment agencies have recently started utilising cutting-edge technology and algorithms to match job applicants effectively and accurately with suitable job openings. This phenomenon falls under the notion of automated job-matching and entails examining job seekers' abilities, credentials, preferences, and other pertinent data before comparing it to the specifications of open positions. This procedure attempts to speed up the hiring and job search processes, enhancing the effectiveness of job placement and raising the possibility of successful matches.

More specifically, the use of big data and algorithms can enable the creation of software that examines the skill sets needed in connection to job offers and finds potential matches with candidate profiles. These procedures lead to the automatic matching of a job opening and a topic profile that the software determines to be compatible with the necessary competencies. These tools are intended to make it easier for users to use the online platforms for the services on their own.

The matches found by job-matching programmes in this regard may arise from the user entering certain parameters or may show up as automatic notifications. In both situations, this knowledge can direct and affect the user's following searches[41]. In some particularly innovative cases, the combinations are identified considering not only the user's skills, but also the behavior and search preferences of the same through the monitoring and collection of click data on the service platform. For instance, in this regard it is good to spend a few words on platforms such as the well-known LinkedIn.

40. See nt. (13), 284.
41. M. Belot, P. Kircher, P. Muller, *Providing advice at job seekers at low cost: an experimental study on online advice*, in *IZA Discussion Paper n. 10068*, 2016.

LinkedIn's job suggestion system is an example of an existing automatic matching engine that takes into account both user talents and behaviour/search preferences. LinkedIn users create detailed professional profiles that include their skills, work experience, education, and preferences. The platform then evaluates the skills listed on users' profiles and ranks them based on relevance and demand in the job market. Machine learning algorithms are used as well to analyse users' profiles, skills, and engagement behaviour. The system then combines skills analysis and behaviour data to generate a dynamic score for each job recommendation. This score reflects how well a job aligns with a user's skills and matches their engagement behaviour and preferences. The job recommendation system on LinkedIn is therefore an example of how combining user behaviour and preferences with talent analysis may produce a personalised and successful job matching experience, increasing the likelihood of successful job placements.

More frequently, the pairings correspond to tools intended to support the activities of the operators. The latter are typically free to direct the same subject to alternative roles or call him into the office to discuss the potential match detected by the programme without being constrained by the match identified by the software[42]. However, a potential limitation of these systems is represented by the fact that job offers published by companies can sometimes be not very detailed and do not present enough information for an optimal match from the point of view of the required skills.

Moreover, it is possible as well to point out a couple of examples of how automated job-matching works in Europe. For instance, in Germany StepStone is one of the leading online job-matching platforms that help connect job seekers with relevant job opportunities. It makes personalised employment recommendations to users based on their talents, certifications, and preferences using algorithms and technology. When creating a profile on StepStone, job seekers typically provide details about their talents, employment history, education, and preferred jobs in order to participate in the matching process. Following registration, StepStone's algorithms examine the data supplied by job seekers and contrast it with the specifics of open job advertisements. The algorithms are designed to find the greatest matches based on a variety of criteria, including job title, industry, location, necessary abilities, and more. StepStone provides job seekers with a list of suggested positions that closely match their qualifications and preferences based on algorithmic analysis. Overall, StepStone's job-matching approach

42. J. Bollens, B. Cockx, *Effectiveness of a job vacancy referral* scheme, in *IZA Journal of Labour Policy,* n. 6/2017, 1-24.

aims to streamline the job search process for users by presenting them with tailored job recommendations based on their profiles and preferences.

In conclusion it is therefore possible to note how automated job-matching possesses many advantages in terms of accelerating the job search process, providing job seekers with relevant job recommendations quickly; personalization in terms of tailored job suggestions based on skills and preferences and equal opportunity, since algorithms can help reduce bias and ensure fair treatment by considering objective criteria. However, automated job matching does present certain difficulties as well. In this way, for example, users may not fully comprehend how the algorithmic matching process works, raising concerns about fairness and transparency; algorithms may as well unintentionally perpetuate biases present in historical data; and finally, the collection and use of personal data for job-matching raises privacy concerns that need to be addressed. Therefore, automated job-matching has obviously the potential to revolutionize public employment services by making the job search process more efficient, tailored, and responsive to both job seekers' and employers' needs. Nevertheless, its implementation requires careful consideration of ethical and transparency issues to ensure equitable outcomes for all parties involved[43].

VI. THE EXPERIENCE OF ONLINE-BASED TRAINING

Online-based training refers to educational courses and programmes that are offered online to those who want to improve their knowledge and abilities in the areas of workforce development, employment services, and related subjects[44]. These training programmes are created to give job searchers, employers, employees of employment agencies, and other market participants quick and accessible learning possibilities. The accessibility of online solutions may also enable governmental employment agencies to expand their training portfolio and successfully meet the rising demand for skills.

The shorter wait times and improved accessibility are the key benefits in this sector. In practical terms, web-based training enables participants to

43. *See* K. Kroft, D.G. Pope, *Does online search crowd out transitional search and improve matching efficiency? Evidence from Craigslist*, in *Journal of Labour Economics,* n. 32/2010, 259-303; P. Kuhn, H. Mansour, *Is Internet job search still ineffective?*, in *IZA Discussion Paper n. 5955,* 2011.

44. E. Pollard, J. Hillage, *Exploring e-learning,* in *Institute for Employment Studies n. 367*, Brighton, 2001.

learn at their own pace and convenience without having to travel to actual training facilities. This saves time that could be spent learning or fulfilling other obligations. Another important feature that works in this training's benefit is the participants' rapid access to the course materials and the ability to fit their learning around other obligations. In fact, training represents the most time-and resource-intensive active policy. At the same time, web-based training transcends geographical barriers since participants can access the training without the need to travel and thanks to a 24/7 availability, which makes this type of training suitable for people with disabilities as well, ensuring a more inclusive learning experience.

Nevertheless, as academics have noted, there are some drawbacks to online education. The technology part itself is one of the first limitations. On the one hand, not everyone has equal access to the internet or devices required for web-based training. This can create an inequitable situation, where those without access are further disadvantaged in terms of skill development and employability. On the other hand, web-based training assumes a certain level of digital literacy among participants. Previous studies have shown how a low level of digital skills is related to lower learning outcomes through these modalities since individuals might struggle to navigate online platforms and effectively engage with the training content[45]. Skills could be linked to a second restrictive factor. Some talents, particularly those that are practical or hands-on, may necessitate physical training and practical experience that cannot be adequately recreated in an online environment. In this sense, some web-based training may place a strong emphasis on theoretical ideas and leave little room for hands-on experience or opportunity for practical application.

It is possible to make a couple of examples showcasing the efforts of public employment services and related organizations across Europe to provide web-based training resources that empower job seekers with the skills and knowledge needed to navigate the job market effectively. These programmes are essential for increasing employability, boosting self-assurance, and improving the overall job search process for people looking for career prospects.

45. C.J. Bonk, R. A. Wisher, *Applying collaborative and e-learning tools to military distance learning: a research framework,* in *United States Army Research Institute for the Behavioural and Social Sciences*, 2000; E. Welsh, C. Wanberg, K. Brown, M. Simmering, *E-learning: emerging issues, empirical results and future directions*, in *International Journal of training and development*, n. 4/2003, 245-258.

The Spanish *Servicio Público de Empleo Estatal* (Public Employment Service) offers web-based training resources to assist job seekers in Spain. These tools cover subjects like digital skills, interview practise, and job seeking strategies. The platform seeks to give users the tools they need to improve their employability[46]. In Estonia, the Unemployment Insurance Fund offers web-based training classes for job searchers to advance their job search abilities, including producing strong CVs, boosting digital literacy, and preparing for interviews. The website offers resources and tools to make it easier for people to navigate the employment market[47]. Moreover, the Swedish Public Employment Service provides online workshops and courses to assist job searchers in Sweden. Strategies for finding a job, networking, and career planning are discussed topics. For the purpose of enhancing job seekers' employability, the platform provides a combination of online training and virtual workshops. Lastly, web-based training courses can be found in Portugal as well, where the Institute of Employment and Vocational Training focuses on career planning, interviewing skills, and job seeking strategies. These tools are intended to aid people in their job-search efforts.

VII. CONCLUSIONS AND FUTURE PERSPECTIVES

There is no question that the dematerialization of services will advance, and this is obvious in many of the examined countries, since all public employment services are actively planning for it.

For instance, the "Spanish strategy for Employment Activation" will include a plan for increased ICT investment, greater efforts to train jobseekers, employers, and staff and management of public employment services in digital skills, as well as enhancements to the telephone-based unemployment benefits service (RATEL)[48]. And all of this will be carried out with full consideration for any data protection regulatory framework's standards. Additionally, the public employment services in France intend to increase their course offerings to customers and strengthen their collaboration with organisations around the country. Another example is represented by Sweden, where the public employment services is soon to embark on an

46. See *www.sepe.es*.
47. See *www.tootukassa.ee.*
48. L. López Cumbre, *Spain's Activation Strategy for Employment*, in *Gòmez-Acebo & Pombo*, 2018. This strategy could be linked as well to the more recent Spanish Digitalization Plan (2021-2025), which is an ambitious public program that includes a set of measures, reforms and investments aimed at promoting more sustainable and inclusive growth from a digital point of view.

EU-founded project named "Democratic Digitalisation" that will give an in-depth examination over a 30-month period of how public employment services themselves can guarantee that all users' needs are identified and met throughout the organisation[49]. The results of the project will probably have a wider applicability and will be of much interest.

According to the analysis carried out previously, it is evident that all public employment services understand the importance of ensuring that users, such as employers or jobseekers, have the skills necessary to fully use digital services even if the digitalization of services will continue to grow. It is also evident that the digitalization of services is occurring at various rates for public employment services.

Generally speaking, the accessibility, transparency, and inclusivity of services can all be significantly improved for customers as a result of the dematerialization of services. Additionally, there are more benefits that come with public employment services, such as lower prices and better job matching, along with broader social advantages including environmental and economic ones[50]. The dematerialization of services must also proceed at a rate that takes into account the demands and preferences of every client, which cannot be classified into a single group. Some sub-groups will undoubtedly need special consideration if they are to gain from improvements[51]. Additionally, the early detection of digital abilities and the planning of remedial training depend heavily on the function that profiling new consumers plays. However, the customer's element of choice must remain in this process, and their choices should be regularly evaluated[52].

In this light, it is essential to increase the digital abilities of users of public employment services in order to give them better access to services themselves. In fact, the chance to improve jobseekers' IT skills could have far more positive effects than just enabling them to use public employment services[53]. Improving their digital skills can be tackled with a range of distribution options – such as local delivery, flexibility to represent the diversity of the client base, and the potential applications of those learning

49. Nt. (12), 22.
50. With particular reference to the environmental and economic benefits, just think, in relation to the first, of the decrease in travel and, in relation to the second, to the possibility of making the labor market more efficient.
51. See nt. (12).
52. The reference is, for instance, to customer surveys, counsellor feedback, etc.
53. Specifically, IT training should go beyond simple operational tasks to incorporate more complex generic aspects of learning, recognising has as a key skill.

the skills – such as taking into account access to new technologies and the internet in general. Within public employment services' staff, they all need to have a sufficient level of IT competence to enable them to help users fully embrace the digitalisation of services. It is likely that there will never be a wholly digitalised service delivery in public employment services, but a carefully planned dematerialisation process can maximise the level of digital services within a multi-channel delivery system to the benefit of customers and public employment services themselves[54].

Considering especially the Italian field, the challenges that the public employment services will have to face will be on multiple fronts. They will concern structural changes in the labour market; the management and integration of foreign workers; the shortage of skilled works specifically in some sectors as well as the development of new services to meet the changing needs of its customers. As previously mentioned, the future is linked to the development of new key staff, in particular digital ones, but also those definable as transversal and managerial. That is why we will be soon asked to modify the internal organizational management by paying attention to issues such as efficiency, quality and protection of privacy and sensitive data, but also opening to collaborations with external subjects, both institutional and private[55].

BIBLIOGRAPHY

D. ALLHUTTER, F. CECH, F. FISCHER, G. GRILL, A. MAGER, *Algorithmic Profiling of Job Seekers in Austria: How Austerity Politics Are Made Effective*, in *www.frontiersin.org*, 2020.

P. ARNI, A. SCHIPROWSKI, *The effects of binding and non-binding job search requirements,* in *IZA Discussion Paper*, 8951, 2015.

M. BELOT, P. KIRCHER, P. MULLER, *Providing advice at job seekers at low cost: an experimental study on online advice*, in *IZA Discussion Paper n. 10068*, 2016.

J. BIMROSE, J. KETTUNEN, T. GODDARD, *ICT – the new frontier? Pushing the boundaries of careers practice,* in *British Journal of Guidance and Counselling*, 43, 2015, 8-23.

54. See nt. (12).
55. European Commission, *PES network work programme 2023-2024*, Luxembourg, Publication Office of the European Union, 2023.

J. BOLLENS, B. COCKX, *Effectiveness of a job vacancy referral* scheme, in *IZA Journal of Labour Policy,* 6, 2017, 1-24.

C. J. BONK, R. A. WISHER, *Applying collaborative and e-learning tools to military distance learning: a research framework,* in *United States Army Research Institute for the Behavioural and Social Sciences*, 2000.

P. G. BRESCIANI, A. SARTORI, *Innovare i servizi per il lavoro : tra il dire e il mare... : apprendere dalle migliori pratiche internazionali*, Milano, 2015.

E. BRYNJOLFSSON, A. MCAFEE, *The second machine age: work, progress and prosperity in a time of brilliant technologies*, New York, WW Norton & CO, 2014.

E. BRYNJOLFSSON, L. M. HITT, H. H. KIM, *Strength in numbers: How does data-driven decision making affect firm performance?*, in *SSRN working paper*, 2011.

M. BUITEN, *Towards Intelligent regulation of Artificial Intelligence*, in *European Journal of Risk Regulation,* 10, 2019, 41-59.

A. CORDELIA, *E-government: towards the e-Bureaucratic Form?*, in *Journal of Information Technology,* 22, 2007, 265-274.

T. DALL SCHMIDT, T. MITZE, *Crisis and the welfare state: the role of public employment services for job placement and the Danish flexicurity system during COVID-19*, in *Cambridge Journal of Regions, Economy and Society*, 16, 2023, 65-79.

S. DESIERE, K. LANGENBUCHER, L. STRUYVEN, *Statistical profiling in public employment services: an international comparison,* in *OECD Social, Employment and Migration Working Papers*, 224, Paris, 2019.

N. DUELL, *PES working group on new forms of work*, in *www.europa.eu*, 2020;

European Commission, *Annual Report. European Network of Public Employment Services (PES)*, Luxembourg, Publications Office of the European Union, 2022.

European Commission, *Blended service delivery for jobseekers*, in *Peer Review Comparative Paper*, Brussels, 2014.

European Commission, *European Network of Public Employment Services: dematerialisation of services in EU PES*, 2020.

European Commission, *InnovAction: a collaborative platform to put ideas into practice*, in *www.europa.eu.*

European Commission, *MyOAEDlive: Tele-counselling services to jobseekers and employers*, in *www.ec.europa.eu*, 2021.

European Commission, *PES network work programme 2023-2024*, Luxembourg, Publication Office of the European Union, 2023.

C. FREY, M.A OSBORNE, *The future of employment: How susceptible are jobs to computerisations?*, in *Technological Forecasting and Social Change*, Elsevier, 114(C), 2013.

C. GAGLIONE, I. PURIFICATO, O. P. RYMKEVICH, *COVID-19 and Labour Law: Italy*, in *Italian Labour Law e-Journal*, 13, 2020.

B. T. HAAR, E. MENEGATTI, I. SENATORI, E. SYCHENKO, *Editorial*, in *Italian Labour Law e-Journal*, 13, 2020.

V. HOMBURG, V. BEKKERS, *E-government and NPM: a perfect marriage?*, in V. BEKKERS, V. HOMBURG (eds), *The information ecology of e-government: E-government as institutional and technological innovation in public administration*, Amsterdam, IOS Pess, 2005.

T. HOOLEY, J. HUTCHINSON, A. G. WATTS, *Careering through the web: the potential of web 2.0 and 3.0 technologies for career development and career support* services, in *UK Commission for Employment and Skills*, London, 2010.

J. KETTUNEN, *Career practitioners conceptions of social media in career services*, in *Finnish Institute fort Educational Research Studies*, 32, 2017.

K. KROFT, D. G. POPE, *Does online search crowd out transitional search and improve matching efficiency? Evidence from Craigslist*, in *Journal of Labour Economics*, 32, 2010, 259-303.

P. KUHN, H. MANSOUR, *Is Internet job search still ineffective?*, in *IZA Discussion Paper n. 5955,* 2011.

N. LETTIERI, *Making smart working smarter. Intelligenza artificiale e prospettive di evoluzione del lavoro agile*, in R. ZUCARO (a cura di), *Verso lo smart working? Un'analisi multidisciplinare di una sperimentazione naturale*, INAPP Report, n. 30, Roma, 117-131.

L. LÓPEZ CUMBRE, *Spain's Activation Strategy for Employment*, in *Gòmez-Acebo & Pombo*, 2018.

P. LOPEZ, *Reinforcing Intersectional Inequality via the AMS Algorithm in Austria*, in *Proceedings of the STS Conference Graz*, 2019.

A. LOXHA, M. MORGANDI, *Profiling the unemployed: a review of the OECD experiences and implications for emerging economies,* in *Social Protection & Labour Discussion Paper,* 1424, 2014.

P. MORREL-SAMUELS, E. FRANCIS, S. SHUCARD, *Merged datasets: an analytic tool for evidence based management, in California Management Review*, 52, 2009, 120-139.

J. P. OLSEN, *Democratic Order, Autonomy and Accountability,* in *Governance,* 28, 2015, 425-440.

W. PIETERSON, *The challenges and obstacles towards PES digitalisation and* differentiation, in *Centre for e-Government studies,* Twente, 4-5th December 2017.

F. PROVOST, T. FAWCETT, *Data science and its relationship to big data and data-driven decision-making*, in *Big data,* 1, 2013, 51-59.

E. POLLARD, J. HILLAGE, *Exploring e-learning,* in *Institute for Employment Studies n. 367*, Brighton, 2001.

G. SCARANO, *Politiche attive del lavoro e servizi per l'impiego: tra miti e riforme*, Milano, 2021;

M. VEALE, M. VAN KLEEK, R. BINNS, *Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making*, in Atti della *CHI'18 – Conference on Human Factors in Computing Systems*, Montréal, 21-26TH April.

A. VRATIMOS, Digital Transformation & COVID-19: the Case of Greece, in European Scientific Institute, 2022.

A. G. WATTS, The role of information and communication technologies in integrated career information and guidance systems: a policy perspective, in International Journal for Educational and Vocational Guidance, 2, 2002, 139-155.

WEF, *Data-Driven Development. Pathways for Progress*, World Economic Forum Report, Cologny, 2015.

E. WELSH, C. WANBERG, K. BROWN, M. SIMMERING, *E-learning: emerging issues, empirical results and future directions*, in *International Journal of training and development*, 4, 2003, 245-258.

E. WIHLBORG, H. LARSSON, K. HEDSTRÖM, *"The Computer Says No!"– A Case Study on Automated Decision-making in Public Authorities*, Paper fort the 49th Hawaii International Conference on System Sciences (HICSS), 2016.

Procedural law

How Technology is Changing Witness Testimony: Few Remarks from an Italian Perspective

[1]Giacomo Pailli*

SUMMARY: I. INTRODUCTION - II. ITALIAN LAW OF EVIDENCE AND THE IMPACT OF TECHNOLOGY - III. WITNESS TESTIMONY: TRADITIONAL ISSUES - IV. ...AND NEW FRONTIERS: 'SOFTWARE AS THE WITNESS', VIDEOCONFERENCING AND EMOJIS - V. CONCLUDING REMARKS

ABSTRACT: A contribution assessing how technology is reshaping Italian civil litigation, although the rules of evidence are some 80 years old, with a specific focus on witness testimony. Old and new issues are analysed, such as a marked distrust towards human narrative and a preference over "software as the witness"; the change in communication produced by social media and emails and the need for lawyers and judge to understand emojis; and finally the growing importance of video-conferencing in cross-border disputes as a mean to allow direct taking of evidence by the requesting judge.

KEYWORDS: Evidence; civil procedure; technology; witness testimony.

I. INTRODUCTION

The interaction between technology and civil procedure easily invites the scholar's mind to travel and speculate on futuristic scenarios that might lie ahead, when a computer – or, as often said, an algorithm – will process claims, defences and evidence to issue decisions and settle disputes between the litigants (and between computers, as well?).

* Post-graduate fellow (*assegnista di ricerca) in Comparative Private Law, University of Florence.*

While this is an incredibly interesting perspective that deserve careful attention, the goal of this short contribution is more prosaic and perhaps less inspiring: try to account what kind of influence technology has today on Italian civil procedure[1], and how existing rules are coping with the fast pace of the digital revolution. The focus of this short contribution is on how technology is (re)shaping witness testimony, in a country where civil procedure rules are anachronistic and players show a marked favour for documents and the output of technological tools, over human narrative.

II. ITALIAN LAW OF EVIDENCE AND THE IMPACT OF TECHNOLOGY

When it comes to the Italian law of evidence, no comprehensive reform has ever taken place in the country. As a result, the field of evidence is still regulated by an old body of law, largely crystalised in arts. 191-266 of the Code of civil procedure, with some important rules to be found elsewhere, especially in arts. 2697-2739 of the Civil code. Beside a patchwork of new provisions on minor aspects, often outside the codes, the rules enacted in 1940 and 1942 respectively are still basically the same in force today, despite that almost eighty years have passed and despite all technological developments that took place in between[2].

1. Some resources in English language on Italian civil procedure are N. Trocker, G. Pailli, *Italian Civil Procedure, in* A. De Luca, A. Simoni (eds.), *Fundamentals of Italian Law, Milano, Giuffrè, 2014, 163-183;* N. Trocker, M. De Cristofaro, *Civil Justice in Italy, Nagoya University, 2010; and more recently* M.A. Lupoi, *Civil Procedure in Italy, III ed., Milano, Wolters Kluwer, 2018. On the Italian code of civil procedure, see* S. Grossi, M.C. Pagni, *Commentary on the Italian Code of Civil Procedure, Oxford, OUP, 2010.*
See also R. Caponi, *Electronic civil procedure between written and oral procedure/Il processo civile telematico tra scrittura e oralità*, in *Revista Eletrônica de Direito Processual*, 17(1), 2016, 193. On the relation between technology and access to justice in the context of small claims and ADR, see E.A. Ontanu, *Technological Progress and Alternatives to the Cross-Border Enforcement of Small Claims, in* J. von Hein, T. Kruger (eds.), *Informed Choices in Cross-Border Enforcement, Intersentia, 2020, 483;* C. Rule, *Renventing Justice with online Dispute Resolution, in Giustizia Consensuale, 2021, 169-189.*

2. As C. Silvestri, *L'evoluzione darwiniana dei mezzi di prova: il ruolo della prova atipica nella modernizzazione del sistema delle prove*, in *diritto.it*, 20 July 2020, accessible at *www.diritto.it/levoluzione-darwiniana-dei-mezzi-di-prova-il-ruolo-della-prova-atipica-nella-modernizzazione-del-sistema-delle-prove/* (last accessed on 29.08.2023) notes "In una situazione di inalterata vetustà normativa e sotto le spinte dell'evoluzione scientifica e tecnologica, il sistema delle prove, in una sorta di evoluzione darwiniana imposta da necessità di sopravvivenza, si è pur reso portatore di un certo grado di novità quale risultato combinato di azione e di inazione. Con questa espressione intendo dire che l'inerzia legislativa ha dato in qualche settore frutti fecondi, consentendo al sistema

Rules are organised in formal categories of what may be considered *typical* evidence. Civil proceedings envisage three main categories of typical evidence: witness testimony[3], documents and inspections. Whatever does not fit neatly into one of these categories, may still be admitted as *atypical evidence*[4]: a long list of items, not regulated by the law, that includes writings coming from third parties (which cannot be included in art. 2702, as they are not writings made by the parties), reports prepared by party-appointed experts, or evidence collected in other proceedings. Much of the novelty that is produced by the technological revolution is a suitable candidate for being considered atypical evidence.

There is no real qualitative difference between typical and atypical evidence: except where the law provides otherwise (e.g,, the binding value of confessions made by a party during the proceedings, according to art. 2733 of the Civil code) all evidence is freely assessed by the judge on equal footing, according to the judge's careful (*prudente*) evaluation (art. 116 of the Code of procedure).

No express and general exclusionary rule for technological evidence or evidence acquired through technology exists in the context of civil

---

di accogliere ed elaborare in autonomia elementi di novità proposti, oso dire, dallo spirito del tempo". A longer and more detailed version appeared as C. Silvestri, *Profili evolutivi del diritto alla prova nel processo civile*, in G. Conte, S. Landini (eds.), *Principi, regole, interpretazione. Contratti, e obbligazioni, famiglie e successioni. Scritti in onore di Giovanni Furgiuele*, vol. I, Mantova, 2017, 417.

3. Witness testimony in contract cases is (apparently) limited by arts. 2721 of the Civil code but, with the possible exception of contracts that must be made in writing according to art. 1350 of the Code (such as to transfer ownership of real estate), in practice it is up to the judge to decide whether to allow witnesses testimony or not. See G. Verde, *Diritto processuale civile*, Bologna, 2014, 95.

4. On the topic see C. Silvestri, *Profili evolutivi*, cit., highlighting that the broad acceptance of atypical evidence is a consequence of a renewed role assigned to the 'truth' in social sciences, that also characterises civil proceedings; G.F. Ricci, *Le prove atipiche*, Milano, 1999, and Idem, *Atipicità della prova, processo ordinario e rito camerale*, in *Rivista trimestrale di diritto e procedura civile*, 2002, 409; L.P. Comoglio, *Le prove civili*, Milano, 2010, 41; M. Taruffo, *La prova nel processo civile*, Milano, 2012, 74; and Idem, *Le prove atipiche e convincimento del giudice*, in *Rivista di diritto processuale*, 1973, 389; B. Cavallone, *Il giudice e la prova nel processo civile*, Milano, 1991, 335. Scholarship is not unanimous in considering atypical evidence as permissible or 'good' evidence, see, ia, A. Proto Pisani, *Lezioni di diritto processuale civile*, Napoli, 2014, 438; cfr. B. Cavallone, *Critica della teoria delle prove atipiche. Il giudice e la prova nel processo civile*, Padova, 1997, 335; G. Verde, voce *Prova (teoria generale e diritto processuale civile)*, in *Enciclopedia del diritto*, XXXVII, Milano, Giuffrè, 1988, 606; A. Carratta, *Prova e convincimento del giudice nel processo civile*, in *Rivista di diritto processuale*, 2003, 52.

proceedings[5]. A fragmented use of exclusionary rules in civil proceedings[6] may be seen in the context of employment law[7], often relating to technological apprehension of information by spying the employee's business email account, tracking GPS installed in vehicles and other devices used for work, but also by scrolling the 'private' Facebook account of the employee.

Case law appears also split on whether violation of data protection laws may lead to an exclusion of evidence[8], and also on whether messages and posts taken from chats and social networks may always be used as good evidence in civil proceedings, regardless of the author's intention to keep it reserved, for example when a chat-message is sent in a closed chat-group or the 'visibility' option in a social network post is set to 'only friends'[9] and

5. On the contrary, the Code of criminal procedure contains many rules on specific aspects of digital evidence, eg, arts. 234bis, 240 and 242; and especially relating to its (lawful) acquisition: e.g., arts. 244, comma 2, 247, comma 1-bis, 248(2), 254bis, 256, 259(2), 260, 266-71, 352(1bis), 354(2). This does not seem an isolated trend, according to X. Kramer, *Challenges of Electronic Taking of Evidence: Old Problems in a New Guise and New Problems in Disguise*, in *La Prueba en el Proceso. Evidence in the process*, Atelier, 2018, 394: "in some countries, electronic evidence is discussed primarily in the area of criminal law, and to date has received relatively little attention in the area of civil law and procedure'; and 399: 'In Europe, very few countries have more comprehensive rules on electronic evidence in civil matters. Most rules only or primarily concern e-signatures that were implemented into national legislation as a result of the eSignature Directive, now replaced by the eIDAS Regulation that has direct effect in the Member States".
6. See P.C. Ruggieri, *Ancora sull'utilizzabilità in giudizio dei documenti ottenuti o prodotti in violazione della privacy*, in *Judicium*, 11 June 2020, available at *www.judicium.it/38857-2/* (last accessed on 29.08.2023). See, in general, N. Minafra, *Contributo allo studio delle prove illecite nel processo civile*, ESI, 2020; L. Passanante, *La prova illecita nel processo civile*, Torino, 2017; D. Dalfino, *Illegally Obtained Evidence and the Myth of Judicial Truth in the Italian System*, in *Derecho, Justicia, Universidad, Liber amicorum de Andrés de la Oliva Santos*, Madrid, 2016, 897 ff.; V. Breda, M. Vricella, *English Pragmatism and Italian Virtue. A Comparative Analysis of the Regime of Illegally Obtained Evidence in Civil Law Proceedings between Italy and England*, in *Maastricht Journal of European and Comparative Law*, 21(3), 2014, 428.
7. The exclusionary rule is far from being absolute and is derived by a qualified prohibition of remote control of employees provided by art. 4 of the Workers' Charter (Law no. 300/70), see E. Fameli, *La rilevanza giuslavoristica dei social network, tra diritti dei lavoratori e prerogative datoriali di controllo*, in *Rivista italiana di informatica e diritto*, 2019, 5, and the case law and scholarship cited therein. See, also, P. Salazar, L. Failla, *Facebook e rapporto di lavoro: nuove frontiere per i comportamenti extra-lavorativi*, in *Il lavoro nella giurisprudenza*, 2019, 635.
8. See L. Passanante, *Prova e* privacy *nell'era di* internet *e dei* social network, in *Rivista trimestrale di diritto e procedura civile*, 2018, 535.
9. Another interesting line of case examined whether the fact that an examiner and an examinee are 'friends' on a social network may invalidate a public competition,

not to 'everyone'[10]. As rightly stated "courts and lawyers [ought to] have […] an understanding of social media, the technical options (for instance privacy settings), and the way people use these media"[11], otherwise they risk misunderstanding what is happening and which rules should be applied.

III. WITNESS TESTIMONY: TRADITIONAL ISSUES...

Witness testimony is not the most effective tool of Italian civil procedure. There is no direct or cross-examination, no surprise effect "à la Perry Mason", no witness preparation by the attorneys: lawyers have to submit beforehand to the judge all the written questions they would like specific witnesses to answer; the judge will then scrutinise the requests (alone, in the silence of her chamber) and admit only those questions that she deems both admissible and relevant for the decision of the case. It is not uncommon that lawyers prepare a long list of questions and the judge only admits a few. The court's decision on which questions are to be admitted may also be telling of the judge's inclination regarding the case. From the moment in which lawyers have submitted their request to the judge and witnesses are finally called to the stand (in fact, the judge's desk in her room), it is common that one or two years have already lapsed.

Witness testimony is still very analogic: witnesses give an oath and are then deposed directly by the judge who poses the questions previously vetted as deemed admissible and relevant. Lawyers are not allowed to talk directly to the witness but may ask the judge to pose additional questions (something that the judge may also do *proprio motu*). No audio or video recording is envisaged in civil proceedings, therefore witnesses' answers are not recorded, but simply summarised by the judge in the hearing's minutes.

---

reaching a negative answer: see C.E. Guarnaccia, *La prima giurisprudenza sul rapporto tra pubblico impiego e social media*, in *Informatica e diritto*, 2017, 368-370.

10. See E. Fameli, *La rilevanza giuridica*, cit., 25, who also notes that the exclusionary rules in the context of social media posts and chat messages are largely adapted from the massive jurisprudence developed for the criminal offence of defamation (libel and slander). See Trib. Milano 01/08/2014, with note of P. Salazar, *Facebook e rapporto di lavoro: quale confine per l'obbligo di fedeltà*, in *Il lavoro nella giurisprudenza*, 2015, 287 and Corte d'appello Torino, 17/07/2014, n. 164 mentioned in M. Cottone, *Social Network: limiti alla libertà d'espressione e riflessi sul rapporto di lavoro (il "Like")*, in *Il lavoro nella giurisprudenza*, 2017. See also C.E. Guarnaccia, *La prima giurisprudenza*, cit., 371 ff.; F. D'Aversa, *Il diritto di critica (anche sindacale) nell'epoca dei* Social Media, in *Labour Law Issues*, 2019, 56-60.

11. X. Kramer, *Challenges*, cit., 409.

As the decision on the merits will be taken after months, or even years, the judge's live memory of what was actually said by the witnesses, their body language and all other crucial information that can be drawn from actually hearing and seeing a witness, will be lost. With the possible exception of simple "yes and no" answers, the assessment of the witness testimonies will be then yet another matter of interpreting a written document, analysing a sentence that was not even written by the witness, but was filtered by the judge's summary. After one or two years, what was perceived live as a strong supporting testimony may fade to a pale confirmation of the events, while a weak and uncertain reply may emerge from the written minutes of the hearing as a strong and convincing evidence of one of the party's claim. There is also no guarantee that the judge who heard the witness will be the same judge to issue the decision on the merits, as it is not uncommon that a judge will move to a different court or position, leaving the whole docket to the next judge[12].

IV. ...AND NEW FRONTIERS: 'SOFTWARE AS THE WITNESS', VIDEOCONFERENCING AND EMOJIS

The context of mandatory car insurance shows a tension between human and technological 'witnesses'. With the declared aim to "prevent and combat fraudulent behaviour in the context of mandatory car insurance", in 2012 a 'database of witnesses' and a 'database of damaged individuals' was created in the private insurance field, to expose repeated players who could be suspected of being 'con artist'. Then in 2017 it was added that in cases of collisions with damages limited to objects (i.e., without personal injury), only witnesses named by the parties from the very beginning of the case or specified in the police report are allowed, as the law provides that "identification of witnesses at a later stage means that the testimony is inadmissible"[13].

While restricting 'human' witness evidence, deemed intrinsically unreliable, the 2017 reform went further building a priority lane for 'technological witnesses' or 'software as the witness'[14]. Insurance providers

12. In 2009 the possibility to file written testimony was introduced as a new art. 257*bis of the Code of procedure, but this option never took off. C.* Silvestri, *L'evoluzione darwiniana*, cit., refers to written testimony as an "istituto ombra" and "mero feticcio di modernizzazione" to stress the purely symbolic value of this procedural reform.
13. Art. 135(3bis) of the Legislative decree no. 209/2005 (Insurance Code).
14. The idea of 'software as the witness' is taken from S. Mason, *Towards a Global Law of Electronic Evidence? An Exploratory Essay*, in *Revista de concorrência e regulação*, 2015, 256.

may offer car owners to install a 'black-box' on the insured vehicles, in exchange for a lower insurance premium[15]. Data recorded by the black-box (the nature of which the car owner is largely unaware) is given full proof in civil proceedings, unless the interested party is able to prove the malfunctioning of the device[16]. The black-box may be considered a sort of 'live witness' in the sense that it (or should we say, she?) is *present* on the scene at the moment of the collision and records a set of parameters (speed, brakes, manoeuvres, etc.); yet its output is acquired as a document (e.g., as a PDF printout of the black-box log) or by way of an expert report. Either way, the results of the device are legally and technically very hard to question: the story told by the digital witness trumps any contrary 'human' narrative, in what may be described as yet another case of acritical faith in the absolute truth told by technology[17].

While we could be tempted to "believe" black boxes (after all, why should they lie?)[18], recent technological developments cast serious doubts on the soundness of placing acritical faith on technology and preferring it over human witnesses: for instance, today it is already very hard, or impossible, to tell whether images, videos and sounds are the truthful depiction of real life or computer-generated fiction, including that produced by free or very cheap software or online services, easy to use and available to the public at large. Sooner or later, we can guess, this 'fiction' will become part of the strategy of creative parties and lawyers, entering the courtroom in the form of fake proof of a fact. If the judge's (and lawyers') human eyes and ears alone are not able to tell the difference between real and fake, two roads open: employing another software to detect fake evidence (if technically and economically feasible) or resorting back to the imperfection of human testimony to confirm whether what is shown in the image, video, or recording is in fact something that really happened, or not[19].

15. Windscreen cameras (so called 'dashcams') are not popular on Italian cars, possibly due to privacy constraints.
16. Art. 145*bis of the Insurance Code.*
17. See S. Bratus, A. Lembree, A. Shubina, *Software on the witness stand: what should it take for us to trust it?*, in A. Acquisti, S. Smith, A. Sadeghi (eds.), *Third International Conference on Trust and Trustworthy Computing*, Berlin-Heidelberg, 2010, 396.
18. For many aspects related to technological evidence see the essay of A. Roth, *Machine Testimony, in The Yale Law Journal, 2017, 1972.*
19. Readers interested in diving into the technical complexities of this perspective, may begin from M. Maras, A. Alexandrou, *Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos, in The International Journal of Evidence & Proof, 2019, 255.*

Technology may produce a small revolution also in the context of cross-border taking of evidence. Beside digitalising all (authentic) communications between judicial and central authorities, saving time and money, the use of videoconferencing to depose witnesses and experts is increasingly being indicated as the preferred method for an effective cross-border taking of evidence. Instead of delegating the requested authority to oversee a taking of a witness testimony of which that authority knows nothing and for which it has no real interest, and instead of having a delegation from the requesting authority travelling across the world to be present, three alternatives are possible: establishing a secure video-link to allow the requesting authority to be present (but not active) at the taking; using the video-link to allow the requesting authority to directly manage the taking of the evidence; finally depose a willing witness abroad with a video-link, without even the assistance of the requested judicial authority.

The (otherwise unambitious)[20] reform of the European Regulation no. 1206/2001/CE on the cross-border taking of evidence within the European Union[21] approved at the end of 2020[22] provides expressly for increased use of direct taking of evidence through videoconferencing (art. 20) and the preferential use of digital means for communications and transmission of documents and communications between authorities (art. 7). Greater importance of video-link in the context of cross-border taking of evidence may be seen in the application of the Hague Evidence Convention. While the text of the Convention, drafted in 1970, does not envisage the remote taking of evidence, the 2019 Guide to Good Practice for The Use of Video-Link[23] released by the Bureau accounts for the increased use of this method

20. G. Cuniberti, *The Unambitious Reform of the Evidence Regulation*, EAPIL Blog, 16 March 2020, available at *www.eapil.org/2020/03/16/the-unambitious-reform-of-the-evidence-regulation/* (last accessed on 29.08.2023).
21. Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (OJ L 174, 27.6.2001, p. 1).
22. Regulation (EU) 2020/1783 of the European Parliament and of the Council of 25 November 2020 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (taking of evidence) (recast) (OJ L 405, 2.12.2020, p. 1), to be applied from 1 July 2022, with the exception of art. 7 on digital transmission of requests (cited below) that will apply three years after the entry into force of implementing legislation.
23. Guide to Good Practice on the Use of Video-Link under the Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters (Evidence Convention), The Hague, 2019, available at *www.hcch.net/en/publications-and-studies/details4/?pid=6744&dtid=3 (last accessed 29.08.2023).* As specified in the Guide, p. 9: "The Evidence Convention was concluded at a time when the modern technologies

for a direct taking of evidence by the requesting court, with the assistance of the requested authority.

If cross-border direct taking through video-conferencing may be seen as a beneficial development, issues still remain as to the respect of the sovereignty and public policy of the requested State, or the application of perjury rules[24]; it does not come as a surprise that such method appears to have the highest potential when the witness is voluntary and there is no need for compulsion[25]. As far as Italy is concerned, there is no general regulation or protocol on videoconferencing (although certain courts have issued their own protocols) and not all courtrooms are equipped with necessary technical devices to perform it[26].

---

of today were not widely used, yet the technology-neutral language adopted by the drafters allows for the use of such technologies".

24. M. Davies, *Bypassing the Hague Evidence Convention: Private International Law Implications of the Use of Video and Audio Conferencing Technology in Transnational Litigation*, in *American Journal of Comparative Law*, 2007, 221-227, concludes at 237: "Without cooperation on such matters as perjury, contempt and privileges, the probative force of evidence taken remotely from a witness in a foreign country may be less than that of evidence given by witnesses who are physically present in court".

25. See M. Davies, *Bypassing the Hague Evidence Convention*, cit., 205, reporting how Rule 43(a) of the FRCP was amended in 1996 so that "[f]or good cause in compelling circumstances and with appropriate safeguards, the court may permit testimony in open court by contemporaneous transmission from a different location". Similarly, according to the English CPR Rule 32.3 "[t]he court may allow a witness to give evidence through a video link or by other means", further specified by Practice Direction 32, Annex 3 'Video Conferencing Guidance', expressly modelled after the protocol of the Federal Court of Australia. See Federal Court of Australia Act (1974), s. 47(A)-(F). Both the English and the Australian guidelines caution that a "It should not be presumed that all foreign governments are willing to allow their nationals or others within their jurisdiction to be examined before a court in England or Wales by means of VCF", see Annex 3 mentioned above. In Australia: "If you are seeking to examine a witness who is outside Australia via videoconference, you must first consider the relevant legislation and requirements in Australia, and the relevant legislation and laws in place in the country where the witness is to give his or her evidence […] prohibitions or restrictions may exist in some of these countries" see *www.fedcourt.gov.au/going-to-court/videoconferencing-guide* (last accessed on 29.08.2023).

26. A limited upgrade of hardware was made in the context of the pandemic, to allow remote hearings. However, in civil proceedings a vast majority of judges preferred to take on a new possibility granted by the emergency legislation (art. 83(7)(h) of the Law Decree no. 18/2020), that of replacing the in person oral hearings with an exchange of written documents digitally filed by the lawyers (so-called '*note di trattazione scritta'), so that no hearing does take place; this is just exposing an obvious truth: all the hearings that may be replaced by short written submission, are simply useless hearings in the first place.*

A third 'frontier' aspect that involve witness testimony, broadly intended, is the increased relevance of emojis in deformalised digital written communications, such as chats or social media posting. The importance of emojis (or 'emoticon' as they are still called in Italy) cannot be underestimated as these signs give an emotional connotation to the literal meaning of the words used, thereby altering its significance, just as actually hearing a person speaking may tell the listener much more than just the literal sense of words used. Case law is abundant of examples: the existence of a series of funny emojis may mark an employees' group chat as an informal environment and excuse the otherwise hard language used by one employee against the employer, saving her from being dismissed[27]; and a smiley kissing face may also save an employer from the claim of mobbing brought by an employee[28]. On the contrary, writing 'A ♥ B forever' on a Facebook status may prove infidelity during the marriage[29]; while putting an angry face and adding the emojis 'clap – strong arm – smiley face' to show approval under a public post containing a harsh statement against the employer, may cost the job to the 'unfaithful' employee[30].

Other written interactions may have 'witness-like' meaning. A single *like* on a derogatory post made by others may be considered enough to grant a temporary suspension from the job without salary to a prison guard[31]. In a recent decision the court found that the husband was legally liable for the dissolution of the marriage, *ia*, because witnesses testified that he set his Facebook status to 'single', adding 'I like women', while he was still married: a sort of extra-judicial admission by the husband that he was considering himself freed from the duty to be faithful to the wife[32].

27. Tribunale Parma, 07/01/2019, in *Diritto dell'Informazione e dell'Informatica*, 2019, 495.
28. Tribunale Roma, 12/03/2018, n.1859, in *DeJure.it (last accessed 29.08.2023), where an emoji of a kissing face saved the day for the employer. One is left wondering whether the outcome would be the same in other jurisdictions.*
29. Tribunale Pistoia, 29/04/2020, n. 260, in *DeJure.it (last accessed 29.08.2023)*.
30. Corte appello Genova, sez. lav., 26/02/2019, n. 101, in *DeJure.it* (last accessed 29.08.2023).
31. TAR Milano, sez. III, 03/03/2016, no. 246 with note of M. Cottone, *Social Network*, cit., 381; also mentioned in E. Fameli, *La rilevanza giuridica*, cit., 27.
32. See Tribunale di Palmi, 2 January 2021, no. 6 (the international reader may be interested to know that the proceedings were instituted in 2015 and decision came only six years later). The text of this unpublished decision is available at *www.studiocataldi.it/articoli/41064-addebito-al-marito-che-si-dichiara-single-su-facebook.asp (last accessed on 29.08.2023). The duty to be faithful is one of the basic obligations of marriage according to Italian law (art. 143 of the Civil code).*

V. CONCLUDING REMARKS

In this short contribution, we tried to show a few ways technology is changing witness testimony in Italy, despite the lack of any update to the rules of evidence. Pressured by the growing importance of technological witnesses, and transformed by the interpretation of emojis scattered through social media posts, live witness testimony still remains an unavoidable and important means of trying to reach a judicial truth.

The lack of new rules, means that the judiciary bears the biggest part of the burden of taking the country's civil procedure up to speed with the complexity of modern times, and this in turn leads to a non-homogeneous approach[33] and, ultimately, to inequality of treatment of litigants. Embracing the examples of other countries (such as USA, England and Australia) and the suggestions coming from supra-national sources (such as the CoE Guidelines)[34], it is about time for Italy to update evidentiary rules that are eighty-years old, bringing to uniformity a patchwork of very different attitudes by lawyers and judges, and ensuring certainty and equal treatment before the law[35].

33. In Italy, as in many other countries belonging to the so-called 'civil law' tradition, case law is not a formal source of law: this means that a court is not bound to follow what other colleagues (or higher courts) did in previous case, and each judge is (relatively) free to give their own interpretation of the law. As the scope of this contribution is not on *stare decisis, let us refer on this topic to the classical writing of* J.H. Merryman, *The Italian Style III: Interpretation, in Stanford Law Review, 1966, 583. A more recent perspective may be found in* L. Baccaglini, G. Di Paolo, F. Cortese, *The value of judicial precedent in the Italian legal system, in Civil procedure review, 2016, 3.*

34. See, e.g., the *Guidelines for Electronic Evidence in Civil and Administrative Proceedings and Explanatory Memorandum, adopted by the Council of Europe on 30 January 2019, CM(2018)169-add1final*, Fundamental Principles: "It is for courts to decide on the potential probative value of electronic evidence in accordance with national law. Electronic evidence should be evaluated in the same way as other types of evidence, in particular regarding its admissibility, authenticity, accuracy and integrity. The treatment of electronic evidence should not be disadvantageous to the parties or give unfair advantage to one of them".

35. This is not to hide that 'time' is the fundamental flaw of Italian civil proceedings: it can take ages before first instance proceedings reach a decision on the merits, let alone embarking on an appeal or a third instance before the Supreme Court. This is no place to expand further on this topic, which is widely discussed, see, ia, R. Caponi, *The Performance of the Italian Civil Justice System: An Empirical Assessment, in The Italian Law Journal, n. 2/2016, 15;* S. Chiarloni, *Civil Justice and its Paradoxes: An Italian Perspective, in* A.A.S. Zuckerman et al (eds.), *Civil Justice in Crisis. Comparative Perspectives of Civil Procedure, Oxford, OUP, 1999;* E. Silvestri, *Goals of Civil Justice When Nothing Works: The Case of Italy, in* A. Uzelac (ed.), *Goals of Civil Justice and Civil Procedure in Contemporary Judicial Systems, Ius Gentium: Comparative Perspectives on Law and Justice, Springer, 2014,*

Updating rules, upgrading the infrastructure and removing existing technical limitations (e.g., to file-types and the size of each filing) is just a part of the effort, as the human factor appears critical. Focused and continuing training of lawyers, judges, clerks and judicial officers is indispensable[36], and all players should be made fully aware of the potential and the limits and risk of technology in comparison to the, surely imperfect, 'truth' spoken by human witnesses.

79; B. Capponi, *Lo stato attuale del processo civile in Italia, in Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, 2019, 99.*

36. See *CoE Guidelines*, *supra* note 34, no. 33: "All professionals dealing with electronic evidence should have access to the necessary interdisciplinary training on how to handle such evidence".

Private comparative law

Handling Artificial Intelligence and Data Control: a few considerations on the European and U.S. approach

[1]Cinzia Valente*

SUMMARY: I. THE UBIQUITY OF ARTIFICIAL INTELLIGENCE AS A PRIVACY THREAT - II. THE DIMENSIONS OF PRIVACY: BALANCING CONFIDENTIALITY AND CONTROL IN THE EUROPEAN AND AMERICAN FRAMEWORK - III. CALIFORNIA'S REGULATION OF DATA CIRCULATION: TRANSPARENCY AS AN INSTRUMENT OF PROTECTION - IV. GDPR AND CPRA FACE THE DATA-DRIVEN SOCIETY: IS IT A DIFFERENT APPROACH? - V. DATA FLOWS IN THE USA AND EUROPE: SOME CONCLUDING REMARKS

ABSTRACT: The pervasive utilization of technology has yielded substantial advantages across diverse sectors. However, it has also necessitated meticulous deliberation concerning the potential risks associated with the rapid dissemination of personal data.

This paper aims to scrutinize the European and American approaches concerning the equilibrium between safeguarding data and fostering technological advancement. The deliberate, incremental, and sectorial regulatory trajectory initiated in the USA, notably in California, juxtaposed with Europe's professed aspiration to assume a prominent role in the technological domain, prompt reflections on the validity of the perspective that portrays the USA as proponents of technological advancement and Europe as defenders of individual rights.

KEYWORDS: Technological innovation; data protection; regulatory intervention; US-EU framework.

* Researcher in Comparative Private Law, University of Modena and Reggio Emilia.

I. THE UBIQUITY OF ARTIFICIAL INTELLIGENCE AS A PRIVACY THREAT

In recent decades, the use of artificial intelligence (AI) has become common in a multitude of fields impacting markets, public services, individuals and research, often enhancing the quality of life and services. Its influence extends to healthcare, agricultural efficiency, production and manufacturing, safety, environmental protection; moreover, it includes the collection and processing of data with applications in robotics, particularly in the medical sector, as well as in the management of daily services (such as banking) or social networks. AI plays a role in our lives even when we underestimate its presence, as it often operates imperceptibly in certain contexts (consider, for instance, text message or search engine results).

The legal sphere[1] has not remained untouched by this 'contamination' leading to questions regarding the legitimacy of AI applications and their functionality at both national and international levels. While certain aspects have been regulated at the European level recognizing the need to control AI tools and curbing their unethical use, many areas still lack regulation, also in the international panorama. These "uncharted territories of law" demand particular attention, especially concerning the protection of individual rights, such as personality rights, when they meet the rapid advancement of technology that brings about the risk of unauthorized data dissemination, the distortion of information, the spread of false information, or even the theft of sensitive personal data. In the most severe cases associated with hacking, privacy breaches can take on critical consequences and may even result in identity theft. Indeed, all the data disseminated online, consciously

1. The bibliography on the subject is extensive; among others see: V. Zeno-Zencovich, *Data protection[ism]*, in *Media Laws*, n. 2/2022, 11 ff.; G. Sartor, *L'intelligenza artificiale e il diritto*, Giappichelli, 2022; A.M. Gambino, D. Mula, *Diritti fondamentali, protezione dei dati e cybersecurity*, in A.M. Gambino, A. Stasi, *La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele*, Pacini, 2020, 23 ff.; S. Zullo, R. Brighi, *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Roma, Aracne, 2015; A. Santosuosso, C. Boscarato, F. Caroleo, *Robot e diritto: una prima ricognizione*, in *NGCC*, n. 7-8/2012, 494-516; M. Durante, *Intelligenza artificiale. Applicazioni giuridiche*, in *Digesto Italiano. Terza appendice di aggiornamento della IV edizione. Discipline Privatistiche*, II, 2007, 714 ff.; R. Pardolesi, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003; S. Rodotà, *Tecnologie e diritti,* Bologna, il Mulino, 1995; G. Taddei Elmi, *I diritti dell'"intelligenza artificiale" tra soggettività e valore: fantadiritto o ius condendum?*, in L. Lombardi Vallauri, *Il meritevole di tutela*, Milano, Giuffrè, 1990, 685-711.

or unconsciously, contribute to construct our personal digital profile and even our digital identity[2].

The advent of the internet has amplified the methods of data dissemination and the sheer volume of data flowing into the network, which technology can process rapidly. AI instruments conduct analysis and link data that, on their own, might seem insignificant but, when combined, can lead to user identification enabling companies to gain insights into our habits, preferences, purchases, and even products we've merely considered.

This monitoring not only enables companies to influence our choices (by offering specific products or services) but has also a significant economic value that can be traded or leveraged.

When big data[3] are processed on a large scale by algorithms[4], additional risks arise alongside the loss of control over our information. The use of predictive technology tools in various domains, including medicine, justice, and the financial sector, presents a challenge for users since it often conceals the operational system of the algorithm and may lead to discriminatory outcomes[5]. For instance, consider the use of the Compas program in the United States, which came under scrutiny by the Wisconsin Supreme Court[6]. In assessing the risk of recidivism, this algorithm considered factors such as the ethnic origin and level of education of the accused. Similarly,

2. For a detailed analisys on this topic: D.G. Ruggiero, *Persona e identità digitale*, ESI, 2023; G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e Impresa*, 2017, 723; G. Resta, *Identità personale ed identità digitale*, in *Diritto dell'informazione e dell'informatica*, 2007, 511.
3. See: A.C. Amato Mangiameli, *Intelligenza artificiale, big data e nuovi diritti*, in *Rivista Italiana di Informatica e Diritto*, n. 1/2022, 93 ff.; V. Zeno- Zencovich, *Dati, grandi dati, dati granulari, e la nuova epistemologia del giurista*, in *Media Laws*, n. 5/2019, 32 ff.; G. Della Morte, *Big Data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, Editoriale Scientifica, 2018.
4. On the relationship between privacy and algoritm: T.E. Frosini, *La privacy nell'era dell'intelligenza artificiale* in *DPCE Online*, n. 1/2022, 273 ff.; G. Finocchiaro, *Considerazioni su intelligenza artificiale e protezione dei dati personali*, in U. Ruffolo, *XXVI Lezioni di diritto dell'intelligenza artificiale. Saggi a margine del ciclo seminariale "Intelligenza Artificiale e diritto"*, Torino, Giappichelli, 2020, 331 ff.; E. Pellecchia, *Privacy, decisioni automatizzate e algoritmi*, in E. Tosi, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice della Privacy*, Milano, Giuffrè, 2019, 417 ff.
5. See on this topic: B.W. Goodman, *A Step Towards Accountable Algorithms? Algorithmic. Discrimination and the European Union General Data Protection* in *Proceedings 29th Conference on Neural Information Processing Systems* (NIPS 2016), Barcelona, Spain.
6. S. C. Wisconsin, State of Wisconsin v. Eric Loomis, case n. 2015AP157 – CR – July 13, 2016.

data subjected to automated decisions for access to credit or the evaluation of reputational ratings can have significant consequences in the users' life, and these automated processes are not always transparent to the individuals they impact.

All these risks underscore the importance of robust data security measures, privacy regulations, and vigilance in an increasingly interconnected digital world.

In this background my contribution aims to analyze the evolution of the European and American legal frameworks on data circulation considering the impact of technology on the protection of individuals rights.

II. THE DIMENSIONS OF PRIVACY: BALANCING CONFIDENTIALITY AND CONTROL IN THE EUROPEAN AND AMERICAN FRAMEWORK

The advent of technology and the proliferation of intrusive tools in individuals' lives has facilitated the projection of our "image" into an increasingly indefinite, sometimes perpetual, space-time context, stimulating reflections about the impellent necessity to find effective means for the protection of rights while balancing public and private interests.

Technology has facilitated the introduction of new goods or the provision of some services to the benefit of the individual (i.e., preventing crimes) obliging a responsible use of data which must enclose a fair and ethical approach[7] for societal and economic advancement.

Identifying new and evolving equilibriums between technology and individual rights requires to consider their dynamic development.

The protection of 'jus solitudinis' (i.e., the need to shield one's privacy from external intrusions[8] as initially appeared in the US context) has evolved to overcome the idea of "confidentiality" and has paved the way for discussions on the right to 'informational self-determination'[9]. Indeed, the

7. See: R. Kitchin, *The data revolution. Big data, open data, data infrastructures & their consequences*, Sage, 2014, 165 ff.
8. I refer to the "right to let be alone" theorized by S. Warren, L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, vol. 4, no. 5. (Dec. 15, 1890).
9. On the evolving significance of "privacy" see: H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, 2010; M. Zimmer, *Privacy on Planet Google: Using the Theory of "Contextual Integrity" to Clarify the Privacy Threats of Google's Quest for the Perfect Search Engine*, in *Journal of Business and Technology*

initial stages of privacy protection were marked by a negative connotation, stressing the necessity to prevent any intrusion into private life. In contrast, contemporary emphasis on controlling data circulation represents a positive[10] interpretation of the right to privacy reflecting a subsequent evolution rooted in the individual's interest[11] in monitoring their own information[12]; an active participation in the information circuit is crucial to determine how we present ourselves, whether truthfully or otherwise, to the external world.

This is essential to protect related rights, including freedom (the ability to choose what and how much to disclose about oneself), dignity (shielding against the inappropriate use of personal information), and equality (preventing discriminatory consequences stemming from specific technological tools like automated processes).

The foundational concept of the new relationship between personal data and the right to information also incorporates the necessity for awareness and control (a qualitative change) over the quantity of data intentionally or unintentionally disclosed to the external world through technology (a quantitative change), and promptly 'processed' by systems beyond our control[13].

The tension between the need to safeguard these individual rights and the imperative to foster technological development and the marketplace has led the European and U.S. legal systems to divergent positions.

Law, n. 3/2008, 109; D.J. Solove, *Understanding Privacy*, Harvard University Press, 2008.

10. The positive and negative aspects of privacy approaches in the American and European contexts are explored by B. Andò (B. Andò, C. Valente, *Children's Informational Privacy and "Digital Parenting" in the U.S. and Italy: A Cleavage in the Western Legal Tradition*, in F. Swennen, E. Goossens, T. Van Hof, *Rethinking Law's Families and Family Law. Proceedings of the 18th World Conference of the International Society of Family Law*, Edward Elgar Publishing, forthcoming).
11. This "control-based" definition was also accepted by A.D. Moore, *Privacy rights. Moral and legal foundations*, Pennsylvania State University Press, 2010.
12. The idea of ownership is used in a non-technical sense as the transition from a proprietary data regime to a personal one is now clear, as explained S. Scagliarini, *Identità digitale e tutela della privacy*, in *Convegno annuale Associazione Gruppo Pisa-Genova, 18-19 giugno 2021, Il diritto costituzionale e le sfide dell'innovazione tecnologica*, available online: *https://www.gruppodipisa.it/eventi/convegni/484-18-19-giugno-2021-genova-il-diritto-costituzionale-e-le-sfide-dell-innovazione-tecnologica*.
13. See V. Cuffaro, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e impresa*, n. 3/2018, 1102.

At the time of writing, the approval of the European Regulation on Artificial Intelligence[14] has entered its final phase, awaiting evaluation by specialists, jurists, and the Commission; the project aims to govern the use of technology avoiding the risk of redundancy and clashes of an excessive regulation.

Pending the enactment and its subsequent gradual implementation over a three-year period, the European Regulation 2016/679 of 27 April 2016 (hereafter GDPR[15]) and its regulatory instruments are the legal source for balancing privacy and technology. The inflexibility of the hard law enclosed in GDPR is tempered by the introduction of 'soft law' principles to be implemented on the regulatory level which involve technical considerations and ethical concerns.

The nature of the fundamental right[16] recognized for personal data protection[17] is confirmed by repositions of the individual at the forefront and by the protection of *'any information concerning an identified or identifiable natural person'*, art. 4 GDPR, aiming to promote safeguarding at all stages of the data's life cycle. This becomes particularly vital in the current landscape marked by the proliferation of online markets and the unregulated expansion of digital tools, resulting in the circulation of vast volumes of data that must also be ensured.

14. Artificial Intelligence Act European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).
15. S. Sica, V. D'Antonio, G.M. Riccio, *La nuova disciplina europea della privacy*, Padova, Cedam, 2016.
16. Privacy is already safeguarded at the European "constitutional" level under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union as well as Article 8 of the European Convention on Human Rights which grants a vertical and horizontal protection. An interesting view on the digital constitutionalism is in G. De Gregorio, *Digital constitutionalism in Europe. Reframing rights and powers in the Algorithmic society*, Cambridge University Press, 2022; O. Pollicino, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Dir. Inf.*, 2014, 569.
17. GDPR lacks a definition of "privacy" and some authors, taking up the American doctrine, speak of "(in)definition" even of personal data: C. Colapietro, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento Ue 2016/679 parametro di legittimità della complessiva normativa italiana sulla privacy*, Napoli, Editoriale Scientifica, 2018, 66.

The European framework embarrasses a risk assessment policy founded on the belief that the processing of personal information carries a high risk of infringing upon fundamental rights; in this context security and accountability must serve as instruments to balance data circulation and technology, providing both protection and a degree of autonomy in business operations[18]; protective tools (including 'privacy by design,' which involves minimizing data, pseudonymization, and 'privacy by default' which emphasized the processing of the data necessary to achieve a specific purpose and to restrict third-party access) become operational preventing strategies.

Moreover, the need to govern technological dynamism (as well as to preserve certain specificities of national legal systems) has led the European legislator to entrust more flexible instruments for regulation; 'soft law' can reasonably find widely acceptable uniform solutions in evolving contexts requiring high specialization and may contribute to fostering the climate of trust, as envisioned in GDPR, and as also invoked in the proposed AI Regulation. Codes of conduct (to be developed by associations or representative bodies), sector-specific regulations together with the strengthened role of the supervisory authorities are intended to manage private needs and public control, aiming to identify tailor-made solutions.

In the USA, the historical approach to these issues is tied to the deliberate fragmentation of state and federal regulations, where entrepreneurial interests, private autonomy, and individual freedom have played a decisive role in choosing a 'self-regulating' and sectoral system[19].

Lacking a comprehensive regulation governing either data circulation (largely fragmented into federal provisions for consumer protection or a few examples of state legislation) or artificial intelligence (some regulatory efforts fall within the realm of labor law), the American system operates under the oversight of independent authorities and is primarily entrusted to common law principles[20].

In the United States, the first legislative act related to privacy, Fair Credit Reporting Act ('FCRA') in 1970 (now included in the Consumer Credit Protection Act) imposed certain limits on data sharing in the consumer credit

18. F. Pizzetti, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in F. Pizzetti, *Intelligenza artificiale, protezione dei dati e regolazione*, Torino, Giappichelli, 2018 5 ff.
19. W. Prosser, *Privacy*, in *California Law Review*, 1960, 48, 383 ff.
20. On this topic: U. Pagallo, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, Giuffrè, 2008, 61 ff.

sector; in the same period, the government recommended the adoption of a code (Code of Fair Information Practices, FIPs) concerning automated data processing with the aim to ensure the reliability of the system. Its fundamental principles (removal of the secret data collections, individuals' right to kwon the nature of collected information and their use, prohibition of processing data for undeclared purpose, data rectification) formed the basis of the Federal Privacy Act of 1974, which was limited to data collection by federal agencies.

In the recent decades, the prevailing need to safeguard citizens from public "surveillance" (amplified by the terroristic attack or operated by Google Street View) has also resulted in the adoption of specific regulations at different times, focusing on matters of general interest with the aim of restraining public intrusion into private affairs.

Gradually, various legislative initiatives have led to the enactment of limited regulations in both the public and private sectors, at both the federal and state levels involving primarily the protection of the user/consumer.

Indeed, in the United States, federal laws also addressing the intersection of AI[21] and privacy are often sector-specific, focusing on precise categories of data or recipients. For example, the Gramm-Leach-Bliley Act governs consumer financial privacy, while the Health Insurance Portability and Accountability Act pertains to sensitive data and particularly health data; the Children's Online Privacy Protection Act (COPPA) is directed at specific beneficiaries such as minors.

Nevertheless, the need to protect individual rights has been reiterated in recent years; we observe a certain legislative activity, both at the state and federal levels, which appears to align with some principles of the GDPR, notably the necessity to ensure privacy compliance in the design phase (privacy by design) of systems using data, the principle of minimization, and more broadly, the adoption of risk assessment as a reference standard. These needs have been highlighted as far back as 2010 by the Federal Trade Commission (FTC), a key player in the existing U.S. system and have also recently been reflected in the proposed federal bill, the American Data Privacy and Protection Act (DPPA), introduced in 2022 - specifically in sections 101 and 103 and in Title III. The bill assigns the operational aspects to soft law tools (guidelines to be developed or existing standards in specific sectors)

21. At now, also the management of generative AI application is under discussion, see K.E. Busch, *Generative Artificial Intelligence and Data Privacy: A Primer*, in *CRS Report* (R47569).

whose enforcement has to be granted by FTC, potentially strengthening in its role.

III. CALIFORNIA'S REGULATION OF DATA CIRCULATION: TRANSPARENCY AS AN INSTRUMENT OF PROTECTION

In the U.S.A., at the state level, there is a varied landscape concerning the legislative panorama; some countries[22] have adopted comprehensive privacy regulations, while others maintain a fragmented regulatory environment, especially concerning AI. Recently, there has been a sudden acceleration in the legislative and policy developments in California where some of the most significant international companies dealing with Big Data, like Google and Apple, have their headquarters.

The national legal framework includes the California Online Privacy Protection Act (CalOPPA, enacted in 2004 and later amended in 2013[23]) and the California Consumer Protection Act (CCPA) of 2018, amended in 2020 by the California Privacy Rights Act[24] (CPRA, which came into force on January 1, 2023 but fully enforceable on July 2023).

Both the laws have the common goal of protecting consumers[25] within the state of California, with a focus on commercial activities. While CalOPPA primarily targets commercial websites and online services, the CCPA/CPRA extends its scope to cover large businesses, often with specific thresholds related to revenue and the volume of users or devices, as well as intermediaries involved in the sharing and selling of personal data.

22. I refer, for example, to the following recent regulations: Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA), Utah Consumer Privacy Act (UCPA), Connecticut Data Privacy Act (CTDPA).
23. Indeed, the California Online Privacy Protection Act (CalOPPA) introduced changes to the Business and Professions Code in Division 8 Chapter 22 of the California law. Specifically, CalOPPA added Section 22575-22579 to the California Business and Professions Code, which addresses online privacy policy requirements for operators of commercial websites and online services that collect personally identifiable information (PII) from California residents.
24. See: D. Felz, A.C. Kortz, *California's CPRA: The Golden State Sets the Tone for U.S. Data Privacy Laws*, in *Privacy & Cybersecurity Law Report*, 2021; S.L. Pardau, *The California consumer privacy act: Towards European-style privacy regime in the United States*, in *Journal of Technology Law & Policy*, 2018, 68-114.
25. According to CalOPPA, CA Bus & Prof Code § 22577 (2022), "the term 'consumer' means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes".

The CCPA/CPRA and the CalOPPA remain separate regulations, and their requirements can apply to businesses simultaneously.

CalOPPA primarily concentrates on transparency and disclosure[26] of data practices lacking an exhaustive data processing discipline and protection of sensitive data; it has forward-looking approach ensuring individuals make informed decisions about the services and businesses they engage online. The consideration that consumers often provide personal information before any actual purchase or lease demands the anticipatory protection of individuals who are in the process of seeking or researching goods, services, money, or credit for personal, family, or household purposes. The essence of CalOPPA regulation lies in enhancing transparency, with a primary focus on disclosing data collection practices for online services. Indeed, website and app managers are required (CA Bus & Prof Code § 22575, 2022) to identify the information collected (disclosing the types of personal information collected from users and informing users about any third parties with whom their information might be shared), to describe how users can request to review and modify their personal information, to provide a notification of the privacy policy (users are informed about the existence of a privacy policy and where to find it). A specific requirement is the disclosure of tracking technology usage and the arrangement for "Do Not Track" requests from users.

The CCPA/CPRA establishes a comprehensive legal framework for safeguarding consumer privacy[27], encompassing a wide range of aspects related to data privacy and the responsibilities of businesses. It grants

26. CalOPPA places specific requirements on website operators and online service providers regarding the publication of their privacy policies. The aim is to make these policies conspicuous and easily accessible to users: it should be easy to find and access by users. Typically, it is recommended to include a direct link to the privacy policy on the homepage or another prominent page of the website or online service. CalOPPA suggests using an easily viewable icon to represent the link to the privacy policy. This icon should be distinguishable from other content on the website and contain the word "privacy", using contrasting colors and a larger font size. The content of the privacy policy should be presented in a clear and understandable language so that users can easily comprehend how their data is collected, used, and shared.

27. This aspect is confirmed by the detailed and comprehensive definition of personal information which typically refers to any data that can be linked to a specific individual or household, directly or indirectly [CA Civ Code § 1798.140 (2022): "'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of

consumers substantial rights, emphasizes the principle of data minimization, introduces additional safeguards for sensitive personal information, requires companies to perform risk assessments and promotes a higher degree of accountability by establishing the Privacy Authority.

The CCPA marked an essential milestone in establishing consumer rights. The right to be informed about data processing, the right to deletion (against any controller or third party), and the right to opt out of data sale[28] or sharing are foundational aspects of the regulation introduced in 2018 (and took effect on 1 January 2020) which also applies to data broker. Importantly, it emphasizes the guiding principle of non-discrimination in the exercise

---

being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:
(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
(B) Any personal information described in subdivision (e) of Section 1798.80.
(C) Characteristics of protected classifications under California or federal law.
(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
(E) Biometric information.
(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.
(G) Geolocation data.
(H) Audio, electronic, visual, thermal, olfactory, or similar information.
(I) Professional or employment-related information.
(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).
(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
(L) Sensitive personal information]".

28. Indeed, the CPRA takes a comprehensive approach to the definition of "sale" in the context of personal data. The definition includes not only the traditional sense of selling data for monetary exchange but also encompasses a broader range of activities related to the transfer of personal data for consideration or valuable consideration; it covers situations where personal data is exchanged for monetary compensation or a financial transaction. Disclosing personal data to a third party is deemed a form of sale when the sharing or dissemination of data to others involves an exchange for consideration. This consideration can take various forms, including goods, services, discounts, access to features, or any other value.

of these rights. The expansion of protection in 2020 by adding (with the CPRA) the right to correct inaccurate information (impacting digital identity) and the right to restrict the use and disclosure of sensitive information (for limited purposes i.e., the access to required service) represents a significant advancement in safeguarding consumer privacy.

The CPRA has also introduced new protective measures, such as the requirement to use data solely for the declared purpose during processing, the deletion and destruction of data after processing, and the implementation of security measures based on the "sensitivity" of the data being used.

The enhancement of the mentioned rights is realized by the requirement for businesses to inform consumers about their data processing practices adopting the company's privacy policy. This notification must include details about the categories of data being processed and should contain links to the opt-out and data sharing selection forms as well as to the limitation use of sensitive data.

While the CPRA doesn't explicitly focus on algorithms, businesses subject to the law should consider the compliance with the regulation requirements when process data involving algorithms.

On one hand, the use of algorithms can help to achieve certain protection goals to detect breaches and trigger notifications, assist in identity verification, facilitate the classification of data exchanges, and identify, process, or categorize sensitive information; some modern tools like Global Privacy Control (GPC) or Advanced Data Protection Control (ADPC) has gained popularity among online users[29].

On the other hand, the risks connected to the use of AI instruments are known, for example algorithms used for personalized pricing, recommendations, or service delivery may affect the personal data or those employed for profiling or automated decision-making could produce discriminatory results.

In the absence of a specific regulatory framework that harmonizes the interests of technological development with the requirements of data circulation, the CPRA extends to the processing of data carried out using automated systems or any process intended for profiling purposes.

29. GPC is a privacy control system that allows users to easily block the sale and sharing of their data through web browsers, exercising privacy preferences while navigating online.

The role of monitoring and enforcing compliance with these regulations has been entrusted to the Office of the Attorney General (OAG)[30], which has been succeeded by the California Privacy Protection Agency (CPPA). These agencies are responsible for ensuring that companies adhere to the legislation and have the authority to investigate and impose sanctions for non-compliance on specific aspects. Additionally, the authority possesses regulatory powers related to the enforcement of privacy legislation with the aim to address emerging privacy challenges, it provides guidance and education to businesses and consumers about rights and obligations under privacy laws and it holds the task to favor public input when developing regulations, ensuring that a diverse range of perspectives is considered in the rulemaking process.

The regulatory phase of the CCPA was initiated in March 2023, and the finalized text, following the public consultation, was scheduled to take effect in July 2023. The significant resistance from companies towards the new and more stringent regulations led to the Supreme Court's decision in late June to delay the implementation of several rules providing companies with additional time to adjust and comply with the new regulations.

The regulatory powers of the agency reflect the awareness of the Californian legislator[31] about the intricate task of striking a balance between the substantial interests at play including the need to align with the broader legal frameworks of trade secrets and copyright.

The state's commitment to addressing privacy and AI is further evident through various bills that focus on some specific aspects. Notably, the Assembly Bill No. 331 of 2023 (CA A 331) expresses concerns about the use of automated systems in various domains, including employment, education,

30. The involvement of the Attorney General in various cases during their mandate demonstrates the importance and active role of regulatory authorities in enforcing privacy laws and protecting consumers' rights in California. Some common cases and situations in which the Attorney General intervened concern web tracking and data sharing (companies using web tracking tools for third-party advertising or data analysis services without clear user consent or proper disclosure); loyalty programs (instances where businesses misuse loyalty programs to collect personal information from customers without transparent disclosure or obtaining proper consent); privacy policy violations (cases where companies fail to comply with privacy policy regulations, which are essential for informing users about how their data is collected, used, and protected). The references to the anonymized cases are available on the following website *https://oag.ca.gov/privacy/ccpa/enforcement*.

31. See: J. Frankenreiter, *The missing "California effect" in data privacy law*, in *Yale Journal on Regulation*, 2022, 1068.

housing, healthcare, utilities, family planning, financial services, and the criminal justice system with the declared aim to enhance risk assessment and ensure human intervention for reviewing automated decisions. Other proposed bills in the healthcare sector (CA A 1502) and government agencies (CA A 302) underscore the growing need for legislative interventions to govern AI applications in these areas.

IV. GDPR AND CPRA FACE THE DATA-DRIVEN SOCIETY: IS IT A DIFFERENT APPROACH?

The Californian data protection system is considered one of the most attentive among the American states regulating data circulation suggesting its place alongside the GDPR encouraging other U.S. countries to adopt comparable regulation.

We do not ignore that while the Californian regulation is primarily focused on safeguarding consumers within a narrower economic context, applying to companies that meet specific size requirements, the European GDPR, which doesn't introduce company size limitations, adopts a more extensive and anthropocentric view, prioritizing the protection of individuals and their personal data across a broader spectrum of situations; this also explains the reason why the GDPR applies not only to companies based in the EU but also to those treatments that refer to the offer of goods or services within the European space (if the company is based in another territory).

However, some points of convergence could be evaluated as the GDPR and the CCPA/CPRA emphasize considerable transparency, the recognition of major data subject rights, and the arrangement of data protection measures.

The current structure of Californian regulation is constructed with the aim of overseeing the flow of data to ensure citizens' control over its circulation, as occurred in the GDPR.

In California, this objective has been prominently featured in the law since 2018 when the intention to bolster the protection of the right to privacy, already guaranteed at constitutional levels[32] was declared. The

32. The constitutional recognition of privacy in the United States has been a subject of discussion and interpretation, as there is no explicit provision in the U.S. Constitution that explicitly mentions the right to privacy. However, privacy rights have been inferred and established through judicial interpretation. The most common interpretation includes the right to privacy in the IV Amendment which protects individuals from unreasonable searches and seizures by the government and requires probable cause

law's intentions, strengthened by the 2020 reform, appear focused on the consumer's right to understand how data is utilized (and its economic value) and to grant or withhold consent for its dissemination.

The recognition of a significant information asymmetry introduced by technology into the modern landscape which demands an express declaration of consumer rights and corresponds to a specific obligation for active involvement on the part of companies is at the basis of both European and Californian legal framework. Both the legal systems also underline the awareness of the pervasive use of technology in today's world and the need of technological advancement stressing the necessity to find a balance in a rapidly evolving digital environment where innovation should be encouraged, but not at the expense of individual privacy and data protection.

A duty to publicize the privacy policy adopted and to emphasize the consumer's ability to exercise the option "opt-in" (in Europe) and "opt-out" (in California) represents a tool that both systems have regulated to establish a primary form of protection. Under the GDPR, Article 13 and Article 14 specifically require organizations to provide clear and comprehensive information to data subjects about the processing of their personal data. This includes details on the purposes of data processing, the legal basis for processing, data retention periods, and the rights of data subjects. Similarly, under the CCPA/CPRA, businesses are required to provide a detailed privacy policy explaining consumers' rights and the types of personal information collected, sold, or disclosed. They must also inform consumers about how to exercise their rights.

---

and a warrant for searches. The rule's aim is the protection from government intrusion, but it has been interpreted to include elements of personal privacy. Also, the First Amendment which protects freedom of speech and expression, has implications for privacy and the Third Amendment prohibiting the quartering of soldiers in private homes reflects a historical concern for the privacy. Several Supreme Court's decisions have played a significant role in defining privacy rights in the United States; often these cases are related to family matter [Griswold v. Connecticut 381 U.S. 479, 1965 established a right to privacy in the context of marital relations and the use of contraception; Roe v. Wade 410 U.S. 113 (1973) recognized a woman's right to privacy in decisions related to abortion; Lawrence v. Texas 539 U.S. 558 (2003) and Obergefell v. Hodges 14 US 556 (2015), extended privacy rights to include intimate relationships and marriage, regardless of sexual orientation] but an evolving situation is remarkable. See D. Raymond, *The right to information data privacy on the Internet*, in *European Journal of Humanities and Social Sciences*, n. 6/ 2022, 81 ff.

Notwithstanding, the obstacle for users to give truly informed consent[33], in the digital sphere[34], the GDPR places consent at the foundation of lawful data processing within an opt-in framework and, therefore, requires its presence before data processing, reinforcing the individual protection.

The California's regulation provides for a general rule embracing an opt-out system. It is used in relation to the sale and sharing of data, which is done unless the consumer denies it; this implied consent is a less effective requirement of the Californian regulation whose effect are partially mitigated by the introduction of an opt-in system reserved for specific cases (namely sensitive data processing, data of minors, or when there are express exceptions to the consumer's request for data deletion, e.g., for scientific purposes when consent has been given). This important corrective has also been introduced for the frequent financial incentive program, often associated with various other services with which the user is in contact with the "provider".

Alike GDPR, consent is defined as a freely given, specific, informed, and unambiguous affirmative statement (by the consumer or their guardian or representative). It is further clarified (a specific aspect absents in the EU regulation) that the acceptance of general conditions or a similar document containing a description of data processing alongside unrelated information does not constitute valid consent. Specifically, according to CA Civ Code § 1798.140 (2022) "hovering over, muting, pausing, or closing

33. We consider that users may grant authorization by clicking a button without having read or understood the meaning of the information and the consequences of the choice made; it frequently happens that the need to obtain a good or service or simply to access a web page leads the user to give consent effectively "extorted" by the circumstances in which it is required. On this topic: G. Comandè, *Leggibilità algoritmica e consenso al trattamento dei dati personali*, in *Danno e responsabilità*, 2022, 33 ff.; E. Trosi, *Decisione algoritmica, Black-box e AI etica: il diritto di accesso come diritto a ottenere una spiegazione*, in *Juscivile*, 2022, 969 ff.; R. Messinetti, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contratto e Impresa*, 2019, 861 ff.; S. Watcher, B. Mittelstadt, L. Floridi, *Why a right to explanation od automated decision-making does not exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, 76, ff.

34. On this topic see: B. Steffes, S. Salemi, D. Feth, E.C. Groen, *Generic Consents in Digital Ecosystems: Legal, Psychological, and Technical Perspectives* in N. Gerber, A. Stöver, K. Marky, *Human Factors in Privacy Research*, Springer, 2023, 255 ff. The authors sustain the idea of acquiring a generic and valid consent for a series of services to address the challenge of obtaining specific consents, especially in contexts where users are bombarded with numerous consent requests. An allow-list of generic consents can provide a structured and user-friendly approach to addressing the challenges associated with consent management.

certain content does not constitute consent. Likewise, consent obtained using dark patterns does not constitute consent".

The GDPR and the CPRA lack a specific definition of "privacy" but refer the discipline to data circulation; the definition of personal information introduced in California through the CPRA (as compared to the CCPA) has expanded the scope of protection to encompass information related to and associated with the consumer, aligning more closely with the EU General Data Protection Regulation, which takes a general approach by referring to any information related to an individual regardless of type and context.

The rights recognized by the CPRA overlap the protection recognized by the GDPR: the right to know the data processing in the CPRA could be associate to that of access in EU regulation, the right to delete and correct information, the right to disclosure and that of restriction of processing of personal data or to object to such processing (even for sensitive data) are included in both regulations.

Moreover, the California privacy law, as reformed in 2020, aligns with some fundamental principles present in the GDPR, demonstrating a point of contact between the two regulatory frameworks, namely data minimization and risk assessment. On the one hand, data processing should be limited to what is "reasonably necessary and proportionate" for the declared purpose, preventing the collection or processing of more data than what is required to achieve a specific lawful purpose.

The concept of assessing and mitigating risks associated with data processing is a shared concern in both regulatory frameworks. The California privacy law, like the GDPR, highlights the importance of conducting a risk assessment before commencing data processing, particularly when dealing with sensitive data. The GDPR also mandates a Data Protection Impact Assessment (DPIA) for processing operations that are likely to result in high risks to individuals' rights and freedoms; on the other hand, CPRA provides for cybersecurity audit when significant risks to consumer are involved.

Both regulations provide for the empowerment of independent authority with the task of assuring the enforcement of the laws and issuing regulatory acts; this is a particularly interesting aspect that will determine the effectiveness of the legislation adopted. However, it still requires some time for observation, as the implementation phase in California has not yet concluded.

V. DATA FLOWS IN THE USA AND EUROPE: SOME CONCLUDING REMARKS

The data exchange characterizes the current economy and forces all legal systems to face the new challenge in safeguarding personal information and preventing the risk of fragmentation of investments in the technological field.

The evolution of the relationship between privacy and technology in the European and American legal framework led to consider their position as antagonistic[35]; the choice to prioritize the protection of personal rights or the development of commercial business has been a determining factor distinguishing the two approaches for a long time, but an analysis of the recent changes registered in those systems could provide valuable insights for additional suggestions.

At the European level, characterized by a consolidated tradition based on the legislative formant, a comprehensive privacy discipline has been approved while on the AI side there are a cautious evaluation of an ad hoc regulation that doesn't rule out the use of soft law instruments. The European focus on human centric concern still strongly safeguards data, with an approach that prioritizes risk prevention and imposes clear obligations on companies. Compliance with these obligations is subject to scrutiny by the Data Protection Authority.

The American approach is influenced by the multilevel structure, federal and state, combined with the awareness that the legislative intervention could undermine a flexible context necessary for technological innovation; this scenario has characterized for a long time the development of a peculiar scheme in which some specific laws appear disordered and confused making difficult the building of an appropriate individual protection[36].

35. For a comparative analysis: G. Smorto, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in *DPCE Online*, n. 1/2023, 339 ff.; P.M. Schwartz., D.J. Solove, *Reconciling personal information in the United States and European Union*, in *California Law Review*, 2014, 102, 877.

36. The regulatory gaps and the lack of privacy protection in certain areas sometimes result in attempts to indirectly safeguard privacy by applying rules from other legal domains. However, these alternative rules often serve conflicting interests, complicating the landscape of data protection. A recent class action lawsuit filed in California provides an opportunity for public reflection on this issue. The case revolves around an artificial intelligence system called the Reface APP, which can alter the faces and voices of famous individuals in images. These modified images can resemble true deepfakes, distorting the portrayal of the individuals involved. In the

At the federal level we register a mosaic of legislation, with detailed laws addressing specific sectors, types of data, and potential harm whose enforcement is supported by the Federal Trade Commission. At the state level, recently, some states have taken the initiative to implement domestic data privacy regulations (i.e., California, Virginia, Colorado, Connecticut), in some other countries no bills have even been presented (i.e. Arizona, Kansas, Nevada) while some legislative proposals in residual states have not yet been passed (i.e. Florida, New York, Maine). In many of the states that have introduced data protection regulations these regulations are scheduled to take effect between 2023 and 2026. We do not ignore that the adoption of the GDPR could serve as a robust regulatory model (not immune to criticisms) that has likely influenced the enhancement of personal data protection in various legal systems worldwide[37], sometimes accelerating legislative processes stagnant or lacking; maybe, this is also due to the stringent requirements established for the transfer of data to other countries,

absence of specific legislation addressing compensation aspects, the class action seeks to apply the right of publicity, which prohibits the reproduction of images without the consent of the individuals depicted. The lawsuit challenges the use of others' identities, the commercial exploitation of these images, and the damages arising from such unauthorized use. The case has progressed through the procedural phase related to the admissibility of the class action, despite the defendant's opposition based on anti-SLAPP rules. The court found that the defendant's actions aligned with users' right to free speech, a right often in opposition to the right to privacy. Final assessments will have to await the conclusion of the trial [Kyland Young v. Neocortext Inc (2023) United States District Court, C.D. California, Case No. 2:23-cv-02496-WLH(PVCx) Decided: September 05, 2023)]. This case has already generated significant public interest. On one hand, the First Amendment could potentially support the use of technology by justifying it as a form of public interest, parody, cultural expression, or entertainment. The entrepreneur's position could be strengthened by the possible application of Section 230 of the 1996 Communications Decency Act, which shields providers from liability for user-generated content. However, these arguments may be countered by copyright regulations (which were excluded in this case as the plaintiff did not contest the use of the images but rather the use of the name and likeness to attract customers) or common law principles. There have also been attempts by judges and scholars to provide constitutional protection to privacy, even though it is not explicitly enumerated in the U.S. Constitution. The heterogeneity of state and federal regulations, coupled with varying interpretations by state judges, could lead to inconsistent outcomes in cases like these.

37. On the so-called Bruxelles effect: A. Bradford, *The Brussels effect: How the European Union rules the world*, Oxford University Press, 2020; M. Rustad, T.H. König, *Towards a global data privacy standard*, in *Florida Law Review*, 2019, 71(2), 365-454.

outlined in Article 45 of the GDPR, demanding an assessment of adequacy of the third system[38].

Notwithstanding the states with dedicated data privacy laws remain in the minority it's evident that there is a growing awareness of the importance of establishing a structured framework for data protection and pose challenges when it comes to evaluating the tangible effects of this emerging trend in regulating data circulation; in California where the right to privacy is declared in the Constitution (sec.1), the social pressure against the companies' abuse in the data processing and public awareness and concern on the risks of data collection have gained the lawmaker attention.

A common aspect of the state approach to data protection is the linkage of regulatory applicability to the size and activities of the companies handling data. While California (along with a few other states) has set a revenue threshold, which is typically around $25 million, most other state regulations have specified both the percentage of annual revenue derived from the sale or transfer of data (from 50% to 20% range) and the number of potential consumers within each individual state as criteria for determining applicability (from 4.5% to 50% of the total citizens' number). This political strategy primarily aims at regulating data circulation on a broad scale while in smaller-scale the data protection appears less obvious or robust and contributes to create a complicate overall assessment of data protection.

The American framework's emphasis on the commercial and economic aspects is reflected in the legislation that often refers to the "consumer" as data protection is considered depending on "commercial" relationship; in the United States, a market-driven approach acknowledges the economic value of data and its role in the digital economy.

This perspective is distinct from the European approach, which places a stronger emphasis on individual rights and data protection as a fundamental right, providing comprehensive protection for individuals.

This different attitude is confirmed by the discipline involving the consequences of the regulation's violation; while GDPR imposes significant fines (with a maximum of € 20 million or 4% of global annual turnover), the American penalties result in a less burden for companies.

38. This evaluation considers three essential elements when permitting data transfers to third countries: a) the rule of law and respect for fundamental rights, including legislation on privacy, in the third country; b) the existence of an effective supervisory authority in the third country; c) the international commitment to data protection.

The European data protection model indeed aligns closely with the "prohibition unless permission" principle, which is realized through the opt-in regime established by the GDPR and provides for an informed consent to legitimate data processing, with a strong emphasis on transparency, data minimization, accuracy, and conformity to the declared purpose.

In contrast, the American system, while informed by transparency instruments, generally follows an "opt-out" model, allowing data processing until the consumer makes a different declaration. This approach is typically less stringent and assumes that data processing is permissible unless the consumer actively chooses to opt out or withhold consent and places a greater burden on individuals to take action to protect their privacy[39].

A remarkable common point is that the adoption of specific discipline for AI is considered central in the current lawful panorama.

The European approach to the technological instruments is undoubtedly challenging[40], as evidenced by the prolonged delay in the approval of AI regulation[41] and the publication of the White Paper[42] indicating the

39. Consensus-based legislative models can indeed be subject to criticism; one of the primary concerns relates to the potential increase in regulatory burdens and its impact on market functioning. Some authors argue that steps can be taken to ensure that smaller or less influential stakeholders are not marginalized in the consensus-building process. See: R.D. Gopal, H. Hidaji, S.N. Kutlu, R.A. Patterson, N. Yaraghi, *Law, Economics, and Privacy: Implications of Government Policies on Website and Third-Party Information Sharing*, in *Information Systems Research*, 2023, *https://doi.org/10.1287/isre.2022.1178*; L. Bergkamp, *Eu Data Protection Policy The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, in *Computer Law and Security Review*, 2002, 18, 31 ff.

40. E. Bassoli, *Intelligenza artificiale nel diritto*, in Idem, *Intelligenza artificiale, tutela della persona e dell'oblio*, Pacini, 2021, 1 ff.; E. Cirone, *Big Data e tutela dei diritti fondamentali: la ricerca di un (difficile) equilibrio nell'ambito delle iniziative europee*, in S. Dorigo, *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini, 2020, 143 ff.

41. C. Casonato, B. Marchetti, *Prime osservazioni sulla Proposta di Regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 2021, 415 ff.; A. Oddenino, *Intelligenza artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulla recente proposta di regolamento della UE, con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica*, in A. Pajino, F. Donati, A. Ferrucci (eds.), *Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e regolazione*, Bologna, il Mulino, 2022, 165 ff.; G. Alpa, *Quale modello normativo europeo per l'intelligenza artificiale?*, in S. Buzzelli, M. Palazzo, *Intelligenza artificiale e diritti della persona*, Pacini, 2022, 17 ff.

42. European Commission, White Paper on Artificial Intelligence: a European approach to excellence and trust, (COM(2020) 65 final) at *https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en*.

advantages of AI and the associated risks. A widespread ethical movement emphasizes the importance of maintaining a human-centric approach and a climate of trust relying on principles such as transparency and accountability (already fundamental principles of data protection). The European Commission has therefore accompanied the regulation[43] with a Coordinated Plan[44] (in collaboration with the member states) to encourage investments in AI and act to implement the action programs. Also recurring in the documents accompanying the proposed regulation is the reference to respect for fundamental rights alongside the objective of placing Europe among the world leaders in the development of AI.

The novel aspect introduced by the proposed regulation is that it departs from the traditional view that pits the risks of AI against the protection of rights; the basis of the reform should rethink the protection of rights considering the technological innovations[45]. The goal is to adopt a proportionate and risk-based strategy, aimed at integrating the GDPR, along with sector-specific legislation, accompanied by a public consultation and analysis conducted by a group of experts (AI HLEG). There is an ongoing need to ensure, on one hand, the protection of fundamental rights while considering the opacity

43. The division of AI systems into high and low risk categories is a defining feature of the draft regulation. High risk instruments are subjected to specific control about their transparency, reliability and human control; the regulation requires assessments compliance, certifications, registration obligations and operation monitoring forms, while for systems considered to be of limited risk it is necessary to inform the user about the use of AI. The draft regulation includes specific prohibitions on the use of AI in situations particularly perilous to fundamental rights, such as systems capable of employing subliminal techniques or exploiting individuals' vulnerabilities. It entails dedicated authorities and involves the data protection authority in the case of AI systems in the experimental phase that utilize personal data, subject to stringent safeguards such as anonymization, a protected environment, prohibition of data transfer, and data deletion, among other measures. Some scholarships highlight some critical aspects of the risk approach based on the difficult identification of the specific dangerous categories (F. Donati, *Quale disciplina per l'intelligenza artificiale*, in V. Falce, *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Giappichelli, 2023, 51).

44. The Coordinated Plan has been initially published in 2018 and the recent version (on 2021) is now available at *https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review*.

45. F. Donati, *Diritti fondamentali e algoritmi nella proposta di regolamento europeo*, in A. Pajino, F. Donati, A. Ferrucci, *Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e regolazione*, Bologna, il Mulino, 2022, 111 ff.; a critical approach to the GDPR concerning the lack of specific discipline of AI is developed by G. Finocchiaro, *Riflessioni su intelligenza artificiale e protezione dei dati*, in U. Ruffolo, *Intelligenza artificiale. Il diritto, i diritti, l'etica,* Milano, Giuffrè, 2020, 237.

of AI systems and potential discriminatory risks[46], and on the other, to facilitate investments and market development. At present, critical issues persist due to the rigidity of a centralized system that regulates evolving risks, particularly in sectors like technology; moreover, the implementation of a 'generic' regulation applicable to all forms of artificial intelligence and the ensuing compliance costs for entrepreneurs are additional factors to be taken into account. Additionally, the absence of specific data protection measures and the reliance on GDPR regulations for data protection further compound the challenges.

On the U.S. front, there is expectancy for the enactment of federal privacy legislation that is assumed to include some references to artificial intelligence. At the state level, the reformed California privacy law has explicitly encompassed profiling activities in its protection framework, thereby regulating data processing in a consistent manner, whether conducted with or without automated systems. However, it's noteworthy that the need to establish essential rules for technological development has led to the introduction of two bipartisan bills in June 2023. The first bill aims to regulate the relationship between individuals and the government when using AI systems, while the second bill is geared towards promoting technological advancement to enhance international competitiveness. Alongside these initiatives, the establishment of the National Artificial Intelligence Research Resource (NAIRR) seeks to foster trust in AI.

Such initiatives suggest that the protection of personal rights has not been absent from public discourse; indeed, the White House has launched the Blueprint scheme for an AI Bill of Rights.

The objective is to foster a dialogue with various public and private stakeholders in order to enhance the quality of life for citizens while mitigating potential technological risks. Several fundamental principles underlie these efforts, including the importance of being informed about the use of AI systems, the ability to exercise the opt-out option, safeguarding personal data (with individuals retaining control over it), and ensuring the security and efficiency of the system.

Finally, the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence of October 2023 establishes

46. G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto*, 2019, 199.

the principles for the responsible development of AI. Once again, emphasis is placed on a safe and secure use of technology[47], underlining the importance of transparency in the application of AI systems and the need to protect personal data with adequate policies and available technical tools, including privacy enhancing technologies (PET).

The analysis of the essential characteristics of European and American data protection regulations still highlights that the culture of data protection is diffused and has led to the recognition of fundamental principles (the right to know about data process, the right to data erasure and correction, and the possibility of withdrawing consent and provides for protection concerning "special" data categories, such as sensitive data[48]). In both systems, a regulatory power is recognized to specific authorities[49] to enhance the protection on more technical aspects as it is evident that integrating legislation through operational rules, codes of ethics or sectoral guidelines remains a preponderant part of the regulation. Regulating technical aspects could naturally lead to a certain level of convergence and the development of shared solutions, especially in specific market sectors that have paradoxically gained international relevance. Furthermore, the mechanisms associated with the establishment of regulatory bodies in both the European and American contexts are designed to ensure the broad participation of various stakeholders, making their consent indispensable for the practical realization of a balanced solution.

47. For an overview on the benefit of AI in the protection of personal data see: A. Scripa Els, *Artificial Intelligence as a digital privacy protector*, in *Harvard Journal of Law & Technology*, 31, 1, 2017, 217 ff.

48. Prominent legal scholarship questioned the validity of this partition, emphasizing factors such as the methods of data use, the potential harm associated with data exposure, and the risks of data utilization. Indeed, apparently innocuous data could unveil sensitive information (e.g., dietary habits indicating religious beliefs), while sensitive data may not always be treated as confidential in specific contexts (e.g., involving a political leader). Beyond the challenges in differentiating between the two categories, the distinct protection becomes precarious when considering the potential for cross-interference between sensitive and non-sensitive data, especially when artificial intelligence systems are involved. These systems have the capacity to effectively render all processing as "sensitive": adopting an approach that regulates data based on risk and potential harm could prove more efficient, albeit more complex to implement. See: D.J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 NW. U. L. REV., available at the following website: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198*.

49. Zuddas, *L'Autorità di controllo: il "nuovo" Garante per la protezione dei dati personali*, in S. Scagliarini, *Il "nuovo" codice in materie di protezione dei dati personali. La normativa italiana dopo il d. lsg. n. 101/2018*, Torino, Giappichelli, 2019, 263 ff.

It is evident that the effort to harmonize artificial intelligence potentialities and data protection at the legislative level should not be abandoned; the law must continue to serve as a mediator between public and private societal demands. An appropriate regulation should establish fundamental principles, leaving the soft law to adapt specific regulations to changing circumstances. Simultaneously, the legal framework, built on ethical principles, should prioritize the protection of fundamental rights while ensuring a balanced approach to the advancement of AI and technologies without ignoring the participation of all protagonists in the regulatory process for a shared enforcement.

Guía de uso

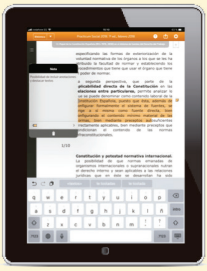
¡ENHORABUENA!

ACABAS DE ADQUIRIR UNA OBRA QUE **INCLUYE LA VERSIÓN ELECTRÓNICA.**
APROVÉCHATE DE TODAS LAS FUNCIONALIDADES.

ACCESO INTERACTIVO A LOS MEJORES LIBROS JURÍDICOS

ARANZADI

FUNCIONALIDADES



SELECCIONA Y DESTACA TEXTOS

Crea anotaciones y escoge los colores para organizar tus notas y subrayados.

USA EL TESAURO PARA ENCONTRAR INFORMACIÓN

Al comenzar a escribir un término, aparecerán las distintas coincidencias del índice del Tesauro relacionadas con el término buscado.

HISTÓRICO DE NAVEGACIÓN

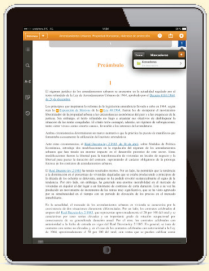
Vuelve a las páginas por las que ya has navegado.

ORDENAR

Ordena tu biblioteca por: Título (orden alfabético), tipo (libros y revistas), editorial, jurisdicción o área del Derecho.

CONFIGURACIÓN Y PREFERENCIAS

Escoge la apariencia de tus libros y revistas cambiando la fuente del texto, el tamaño de los caracteres, el espaciado entre líneas o la relación de colores.



MARCADORES DE PÁGINA

Crea un marcador de página en el libro tocando en el icono de Marcador de página situado en el extremo superior derecho de la página.

BÚSQUEDA EN LA BIBLIOTECA

Busca en todos tus libros y obtén resultados con los libros y revistas donde los términos fueron encontrados y las veces que aparecen en cada obra.

IMPORTACIÓN DE ANOTACIONES A UNA NUEVA EDICIÓN

Transfiere todas sus anotaciones y marcadores de manera automática a través de esta funcionalidad.

SUMARIO NAVEGABLE

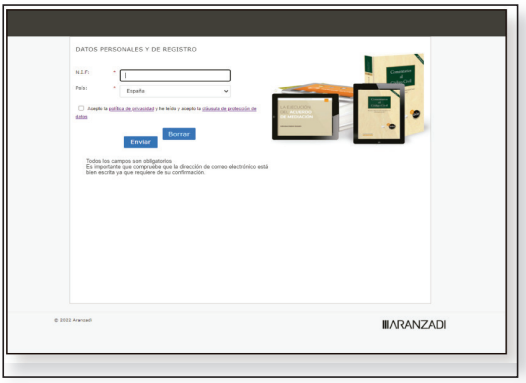
Sumario con accesos directos al contenido.

ARANZADI

INFORMACIÓN IMPORTANTE: Si has recibido previamente un correo electrónico deberás seguir los pasos que en él se detallan.

Estimado/a cliente/a,

Para acceder a la versión electrónica de este libro, por favor, accede a **http://onepass.aranzadi.es** Tras acceder a la página citada, introduce tu dirección de correo electrónico (*) y el código que encontrarás en el interior de la cubierta del libro.



A continuación pulsa enviar.

Si te has registrado anteriormente en OnePass, en la siguiente pantalla se te pedirá que introduzcas el NIF asociado al correo electrónico.

Finalmente, te aparecerá un mensaje de confirmación y recibirás un correo electrónico confirmando la disponibilidad de la obra en tu biblioteca.

Si es la primera vez que te registras en **OnePass,** deberás cumplimentar los datos para crear tu cuenta y poder acceder a tu libro electrónico.

- Los campos **"Nombre de usuario"** y **"Contraseña"** son los datos que utilizarás para acceder a las obras que tienes disponibles a través del navegador en la ruta www.proview.thomsonreuters.com

Servicio de Atención al Cliente

Ante cualquier incidencia en el proceso de registro de la obra no dudes en ponerte en contacto con nuestro Servicio de Atención al Cliente. Para ello accede a nuestro Portal Corporativo y una vez allí en el apartado del Centro de Atención al Cliente selecciona la opción de Acceso a Soporte para no Suscriptores (compra de Publicaciones).

ARANZADI