The fundamental rights of the person in the digital horizon. Law and technology: a possible combination?

Gaetana Natale*

"*Magna pars est profectus velle proficere*"
Lucius Annaeus Seneca

The challenges thrown down by unstoppable scientific and technical progress engage every branch of knowledge, especially the law, which is responsible for the inalienable functions of regulation and protection. Specifically, legal systems that give a central role to the person and his dignity are called upon to meet two opposing requirements: on the one hand, to ensure the protection of fundamental rights, and on the other, to allow the development of technology and science (1). In this regard, the European Economic and Social Committee has identified privacy (2) as one of the eleven areas destined to be changed/deleted using artificial intelligence. The possibility of monitoring tastes, preferences or habits, of controlling a person's movements, and even of learning about the most intimate aspects of his or her private life (3), makes it imperative to devise instruments that give the holder a power of control over his or her data. Thus, it is undeniable that the legal horizon of the digital revolution opens new scenarios in terms of fundamental rights, destined to change depending on the frame of reference. Indeed, as far as the right to privacy is concerned, it is now anachronistic to identify it with the absolute right to privacy ("right to be let alone") (4), meant as a categorical prohibition to

(*) Avvocato dello Stato, Professore di Sistemi Giuridici Comparati, Consigliere giuridico del Garante per la tutela dei dati personali.

Il presente articolo è la relazione presentata dall'Autrice nel corso dell'incontro di studio tenutosi presso l'Avvocatura Generale dello Stato in data 7 giungo 2023 con la Loyola University di Chicago.

(1) Consider the Italian legal system, in which the rights of the human person are defined as inviolable by article 2 of the Constitution, qualified as a general clause for the protection of the person and his or her interests. Given their universality, they find expression in important international and EU documents, such as the Universal Declaration of Human Rights (1950) and the Nice Charter (2000), in which the protection of man and his dignity, operates expressly as a limit both with regard to those who hold power and with regard to relations between private individuals. P. Stanzione, *Manuale di diritto privato*, Turin, 2021.

(2) CESE, Document C-288, 31 August 2017. "AI poses challenges for society": ethics; security; privacy; transparency and accountability; labour; education and skills; (dis)equality and inclusivity; legislative and regulatory arrangements; governance and democracy; warfare; superintelligence.

(3) Hence the gradual emergence of a tendency towards a surveilled society where all the social relations that take place online are naturally traceable. S. Zuboff, *Surveillance Capitalism. The future of humanity in the age of new powers*, Rome, 2019.

collect information, since now data is an unavoidable component of social life. On the contrary, it should be declined in terms of the right to procedural lordship, i.e. as the possibility to directly control the way information is collected and circulated, as well as the right to interrupt the processing if the person considers that it is damaging to his or her interests ("right to exit"). Moreover, it goes without saying that the relationship between rights and new technologies is of constant complementarity and integration.

In the view of the multidisciplinary nature of subject, after briefly outlining the state of the art, and analysing the main regulatory sources in the EU sphere, we will dwell on the main critical issues related to the use of artificial intelligence for the fundamental rights of the person, not without attempting to outline methods and tools useful in regulating the complex and constantly evolving relationship between man and machine.

Technical hints: AI and big data.

Prodromal to all questions concerning the new technologies' legal aspects is the understanding - at least in broad terms - of the phenomenon.

Defining the technology that is looming on the horizon, is already a difficult operation in itself for the jurist, first of all because he is a neophyte in the technological field, and then for the presence of a *mare magnum* of notions. Usually the definition of A.I. refers to the idea of human intelligence, which includes the ability to learn and extract, to reason and use language, to predict, to decide with varying degrees of autonomy (5). In fact, already in 1950, Alan Turing, considered the founding father of computer science, stated "the idea behind digital computers may be explained by saying that these machines are intended to carry out any operations which could be done by a human computer" (6). In other words, if the process is qualified as intelligent when performed by a human being, then it can also be qualified as intelligent when performed by a machine. On the regulatory level, however, we would like to point out the formula contained in Article 3 No. 1 of the European Commission's proposal for a regulation on artificial intelligence, whereby "artificial intelligence system means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with" (7).

---

(4) S. Warren, L. Brandeis, *The right to privacy*, in *Harvard Law Review*, 5, 1890.

(5) Thus B. Marchetti, voice *Digital administration*, in *Enciclopedia del diritto*, Milan, 2022.

(6) A. Turing, *Computering Machinery and intelligence*, in *59 Mind*, 1950, 436.

(7) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain Union legislative acts, 21 April 2021, COM (2021) 206 final, available online at the following link: *https://eur-lex.europa.eu/legal-*

With regard to operation, these machines are based on algorithms, i.e. ordered sequences of actions that, given certain input data (input), arrive at producing the desired end result (output), which constitutes the solution to the problem for which the algorithm was constructed. While this statement can be applied to any intelligent system, the phenomenon, as mentioned earlier, must necessarily be understood in plural terms, moving from the simplest expert systems, to gradually more refined devices, even capable of autonomous learning. In more detail, the following classifications are proposed (8):

a) model-based algorithms: they work according to hard rules, i.e. defined and unambiguous instructions provided by experts in a given field which, when executed, lead to a certain and defined result;

b) machine learning (ML) algorithms: starting from structured and categorised data, the systems learn how to classify new data according to type; they are optimised by human feedback, which indicates incorrect and correct classifications;

c) deep learning (DL) algorithms: like the former are characterised by the ability to learn autonomously from experience and to develop their own logic to arrive at the final result, but by exploiting neural networks they are able to process unstructured data. Unlike the latter, training by a developer is not necessary.

Briefly, there are at least two critical issues that the most sophisticated algorithms present, which are relevant from both an engineering and a legal point of view. The first, located in the learning phase, concerns the large amount of data (big data) required for the machines to provide reliable results (at least 100 million data points for DL systems). The second relates to its defect of explainability, since it is not possible to know the process by which the system, given certain inputs, arrives at certain outputs (black boxes) (9). Indeed, once the training phase is over, the algorithm develops, with experience, autonomous decision logics, which the programmer is neither able to predetermine or predict. It should not be forgotten that such results may be correct, incorrect and even discriminatory (bias). Hence the well-known difficulty of using these intelligent systems to assist or even replace humans in public decision-making processes, considering the high

---

content/IT/TXT/?uri=CELEX%3A52021PC0206. For a more precise definition see the one formulated by the High Level Expert Group on Artificial Intelligence appointed by the European Commission in the document on *A definition of AI*: *Main Capabilities and Disciplines*, Brussels, April 2019, available at the following link: *https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines.*

(8) *https://www.ionos.com/digitalguide/online-marketing/search-engine-marketing/deep-learning-vs-machine-learning/.*

(9) For all, compare F. Pasquale, *The black box society*, 2016.

level of guarantees provided by national legal systems and European and international law (10).

Legal aspects: data protection in the system of international and Community law sources.

It emerged from this concise discussion that in the age of artificial intelligence, data are essential resources for economic, social and technological development, representing the raw material on which technology feeds (11). In this regard, the Economist reported: "data will be (and perhaps already are) the oil of the future" (12). This statement aptly describes the phenomenon if one considers that the predictive capacity of algorithms, besides being used to pursue general interests, can also be employed to maximise the profit of private powers. In concrete terms, these machines predict consumption and market trends, the wear and tear of infrastructures, diagnoses and cures, disasters and political decisions, even electoral results. Of course, there is often a cost to this: economic exploitation and commodification of personal data. This mechanism needs to be regulated, as data is not just an input, from which a machine proceeds to arrive at a certain result, but encompasses a universe of information of an individual's life, which it detects as an object to be protected.

The protection of personal data is first and foremost a principle that has multiple normative foundations in international, supranational and domestic law. Proceeding by hierarchy, significant is the wording of Article 8 of the European Convention on Human Rights (ECHR), which, in recognising the right of every person to respect for his or her private and family life, home and correspondence, represents the parameter on the basis of which the Strasbourg Court ascertains possible violations of the right to privacy (13). Other normative references are Article 12 of the Universal Declaration of Human Rights, which states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such

(10) On this subject the literature is endless. *Ex plurimis*, E. Picozza, *Artificial intelligence and law. Politica, diritto amministrativo, and artificial intelligence*, in *Giur. It.*, 2019, no. 7; C. Casonato, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in *Biolaw Journal*, 2019, no. 2; F. Donati, *Intelligenza artificiale e giustizia*, in *Riv. AIC*, 2020, no. 415.

(11) M. Castells, *The rise of the Network society*, Oxford, 2000.

(12) *The world's most valuable resource is no longer oil but data. The data economy demands a new approach to antitrust rules*, in the *Economist*, 6 May 2017.

(13) In *Sidabras v. Lithuania*, the ECHR gave a very broad interpretation of the right to privacy under Article 8 of the ECHR. The Strasbourg judges held, in fact, that the protection provided by this article extends to encompass the right of each person to develop social relations free from all forms of discrimination or social stigmatisation, thus also allowing him or her the full enjoyment of his or her private life. The Court, therefore, considered the overall place of the person in society, stating that full respect for privacy is a condition for equality and the enjoyment of fundamental rights, such as the right to work.

interference or attacks" and Article 17 of the International Covenant on Civil and Political Rights, which incorporates it verbatim.

The European Union, in addition to Article 16 TEU, inserts the right to the protection of personal data in Article 8 of the Charter of Nice (CDFUE), making it a fundamental right that binds not only the EU institutions, but extends to all member states, pursuant to Article 51 of the same Charter. In particular, it represents a specific declination of the right to respect for private and family life referred to in Article 7 of the same document and already provided for in Article 8 of the ECHR. Precisely, the provision establishes: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data shall be processed fairly, for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Every person shall have the right of access to the data collected concerning him or her and the right to have them rectified. 3. Compliance with these rules shall be subject to control by an independent authority". What emerges from all these sources is a common conception of privacy that does not coincide with the traditional concept of the right to anonymity or to be let alone, but rather with the idea that everyone should have the right to control his or her own personal information, as a prerequisite for the exercise of many other rights of freedom, especially of a cyber nature (14).

The European Union, in its aim to assert a European "digital sovereignty", envisages the construction of a majestic regulatory framework, essentially based on four pillars:

a) protection and enhancement of personal data: the former covered by Regulation (EU) 2016/679 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (better known as GDPR); the latter by the *Data Act*, the *Data Governance Act* and the proposed regulation on the European health data space;

b) digital services and the digital market: the subject of the Digital *Services Act* and the *Digital Markets Act*;

c) digital identity: the 2014 E-IDAS regulation is to be revised in this respect;

(14) Reference is made to the doctrine of cyber-freedom, a theory that was put forward in 1981 and had its ideological matrix in the conception of a new liberalism. It was originally distinguished into positive and negative freedom. Negative freedom of information technology expresses "the right not to place in the public domain certain information of a personal, private, confidential nature (qualifications that may not coincide with each other in certain cases); positive freedom of information technology, on the other hand, expresses the faculty to exercise a right of control over data concerning one's own person that have escaped the circle of privacy because they have become input elements of an electronic programme; and therefore positive freedom of information technology, or the recognised subjective right, to know, correct, remove or add data in an electronic personal file". Thus V. Frosini, *La protezione della riservatezza nella società informatica*, in N. Matteucci (ed.), *Privacy and data banks*, Bologna, 1981, 37 ff. (later included in vol. *Id*., *Informatica diritto e società*, 2nd ed., Milan 1992, 173 ff.).

d) Artificial Intelligence: a proposal for a European regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain pieces of Union legislation is in the process of being adopted.

The GDPR: Regulation (EU) 2016/679.

In order to understand the transformation of privacy in the age of AI, it is necessary to start by analysing the GDPR Regulation (15). According to Article 2, it also applies to the processing of personal data carried out in whole or in part by artificial intelligence (16). Article 1, in defining object and purpose, states: "This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data, and rules relating to the free movement of such data". Already the first provision shows how the right to privacy is not protected absolutely, but must be combined with the need for free movement of data. Indeed, the purpose of the regulation is not only to guarantee the protection of personal data, but also to promote the development of the Digital Single Market (17).

To increase citizens' trust in the use of new digital services, a trustworthy digital environment must be created, in which the identity of the data controller, the procedures and the levels of protection are known. The regulation focuses on the principles of accountability and compliance, as set out in Article 5(2) ("The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability")"). These are primarily incumbent on the data controller, who is called upon to choose the most appropriate measures to prevent risks, to take the necessary decisions and to prove that they are adequate, on pain of liability under Article 24.

The GDPR's approach is based on risk assessment (*risk based*), a parameter against which the degree of accountability of the data controller or processor is measured. Obviously, the controller is bound by specific principles set out in the regulation: in particular, *privacy by design* and *by default* and *Data Protection Impact Assessment.* The principle of *privacy by design*, referred to in Article 25(1) of Regulation (EU) 2016/679, provides that, taking

(15) *https://protezionedatipersonali.it/privacy-by-design-e-by-default.*

(16) Art. 2 "Material scope" "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system". See G. Finocchiaro, *XVIII lezione: intelligenza artificiale, privacy e data protection*, in U. Ruffolo (ed.), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Turin, 2021, 331 ff.

(17) Recital 7 "Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced".

into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing, as well as the risks having different probability and severity for the rights and freedoms of natural persons constituted by the processing, the controller must implement, both when determining the means of processing and at the time of the processing itself, "appropriate technical and organisational measures, such as pseudonymisation" (referred to in Art. 4(1)(5)), designed to implement effectively the principles of data protection, such as data minimisation, and to incorporate in the processing the necessary safeguards to meet the requirements of the Regulation and to protect the rights of data subjects. Linked to this criterion is the principle *of privacy by default*, which is enshrined in the second paragraph of Article 25 of Regulation (EU) 2016/679: the data controller must implement "appropriate technical and organisational measures to ensure that only the personal data necessary for each specific purpose of the processing are processed by default". The individual is protected in a strengthened way since the provision establishes access to an indefinite number of natural persons by machines (without the intervention of the natural person) and provides that the obligation is calibrated on aspects such as the amount of data, the scope of processing, the retention period and accessibility. Also interesting is Article 35 of Reg. (EU) 2016/679, concerning the so-called *Data Protection Impact Assessment*: when a type of processing, involving in particular the use of new technologies, taking into account the nature, subject matter, context and purpose of the processing, may present a high risk for the rights and freedoms of natural persons, the data controller shall carry out, before processing, "an assessment of the impact of the intended processing on the protection of personal data" (18).

Despite its complexity - 173 *recitals* and 99 articles - and its proactive and flexible approach to the subject of personal data protection, the GDPR cannot be considered a self-sufficient and immutable body of legislation. The drafters themselves are aware of these qualities, and in Articles 12(8) and 43(8) they empower the European Commission to adopt delegated acts and implementing acts to lay down technical standards concerning certification mechanisms and data protection seals and marks, and delegate to the Member States the adoption of more specific rules to adapt the application of the Regulation. Furthermore, Article 97 provides for a review of the GDPR every four years, allowing the Commission the possibility of proposing amendments to the Regulation, taking into account "in particular developments in information technology and progress in the information society".

(18) *https://protezionedatipersonali.it/privacy-by-design-e-by-default.*

Proposed regulation on AI.

As much as the tools and principles provided by the GDPR lend themselves to extensive application in today's "data-driven society", there is an urgent need to develop models for regulating new technologies.

Self-regulation? Homogenous or sector-specific regulation? Whereas in the United States there has been a move towards a self-regulatory model, while in China there has been specific and detailed regulation, the European legislator has opted for a horizontal approach, with rules applicable to each sector (health, financial, etc.). The proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) aims to ensure that AI systems placed on the EU market are safe and ethical, comply with existing fundamental rights legislation, and respect EU values through a proportionate risk-based approach. AI systems are classified according to the risk they present into three categories: a) AI with unacceptable risk; b) AI with high risk; c) AI with low or minimal risk. Firstly, systems that present an unacceptable risk are banned. These include "real-time" remote biometric identification systems in publicly accessible spaces (19). Instead, for low-risk AI systems, certain transparency obligations are laid down and codes of conduct are encouraged. For instance, for AI systems intended to interact with individuals, it is required that they must be informed of the interaction with an AI system; for so-called "deep fake", systems that generate or manipulate images or audio or video content that closely resemble existing persons, objects, places or other entities or events and that could appear falsely authentic or true, it is required that users disclose that the content has been artificially generated or manipulated. Finally, the obligations for the adoption of high-risk AI systems are listed in detail. In particular, it is stipulated that such systems are subject to an *ex ante* conformity assessment procedure, which concludes with the affixing of the CE mark. In addition, high-risk AI systems must be designed and developed in such a way to guarantee, by means of automatic event logging and throughout their life cycle, the traceability of their operation, which must be sufficiently transparent to enable users to interpret their output and use it appropriately.

It is clear that the proposed new regulation borrows its main axes from the GDPR: from the risk-based approach, to the duties of transparency towards users, to certifications and codes of conduct. Furthermore, the unavoidable incidence point for both subjects is not marginal: the processing of personal data is functional to feeding artificial intelligence systems with a view to their au-

(19) This is the only system whose prohibition has exceptions, pursuant to Article 9 of the GDPR, in cases of searching for victims of crime, threats to life or terrorist acts, or searching for persons guilty of serious criminal offences. In these cases, the use of the system may be permitted, subject to authorisation by a judicial authority or independent administrative authority.

tomatic learning. It is evident, therefore, how errors or mistakes in the processing of data functional to the feeding of the machine are reflected in as many distortions of the algorithmic process (20). So there is an objective need to avoid the emergence of antinomies between the different disciplines mentioned, in order to make the regulation of the matter as a whole more organic and effective.

Law and technology: a possible combination?

In a climate of general mistrust towards technological and scientific progress, the European Union's attempt to regulate the artificial intelligence phenomenon is certainly to be welcomed, although aware that the speed at which artificial intelligence is progressing and the complexity of the issues carries the risk of making any regulation immediately obsolete. If law and technology travel at two different speeds, perhaps it would be appropriate to adapt legal instruments to the speed of the latter? Perhaps by opting for soft law instruments rather than hard law ones? Perhaps by preferring general rather than detailed legislation? One thing is certain: the transnationality of the phenomenon requires that all questions will be answered at a global level.

(20) C. Utz et al., *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, in *ACM SIGSAC Conference on Computer and Communications Security*, November 11-15, 2019, London, United Kingdom, ACM, New York, NY, USA.