This is an Accepted Manuscript of an article published by Wolters Kluwer in the Global Privacy Law Review 3(1): 4-18, available online here

Digital Humanism: The Constitutional Message of the GDPR

Edoardo Celeste and Giovanni De Gregorio

Abstract: This paper aims to analyse the constitutional message of the GDPR in the algorithmic society. Although the GDPR does not formally have any constitutional character, it can be said to play a para-constitutional role from a functional point of view: it translates and implements core constitutional principles in the context of the algorithmic society. This paper traces the legislative origin of the GDPR's framework on automated decision-making showing that it aims to enhance a series of key constitutional values, preserving human autonomy, increasing legal certainty, and providing more procedural safeguards. The paper finally highlights how the GDPR is promoting a constitutional message deeply rooted in a new form of 'digital humanism': a conception of the digital society where the human being and her dignity should resolutely outrank machines, technology and, ultimately, economic efficiency.

Keywords: artificial intelligence, GDPR, digital humanism, rule of law, human dignity, constitutionalism.

Der Mensch steht höher als Technik und Maschine.
– Article 12, Constitution of the Free Hanseatic City of Bremen

1. Introduction

While the Internet was still in its infancy, Sherry Turkle, in her book *Life on the Screen*,[1] had an intuition about the way the information society would have challenged the concept of human identity and its digital projection. She foresaw the emergence of a new kind of interactions between humans and machines, anticipating how the rise and development of artificial intelligence would have increasingly led human beings to rely on decisions taken by automated systems. Calculating the likelihood of criminal recidivism or providing access to credit are only two examples of how today algorithms can concretely shape the lives of individuals.[2] From a macro-level perspective, this change can be regarded as the apex of an ample parabola. Over the past few centuries, machines have progressively replaced human labour, thus, leading to a series of societal transformations. In this process, new technologies have relentlessly contributed to change the role and position of humans within society, by eroding human judgment, and increasing the centrality of machines in our daily life, even to make significant decisions based on predictive analytics.[3]

[1] Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (Simon & Schuster 1995).
[2] Brent Daniel Mittlestadt et al., 'The ethics of algorithms: Mapping the debate' (2016) 3 *Big Data & Society* 293.
[3] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform how We Live,*

In fifth century BC, Protagoras of Abdera affirmed that 'Of all things the measure is man, of the things that are, that they are, and of things that are not, that they are not'.[4] Yet, over the years, machines have gradually replaced human beings in their capability to discern, appreciate, and assess the external reality. Today, we rely on different technologies to accurately measure time, temperature and distance, just to mention some examples. We would never dare to defy the precision of a Swiss watch by simply observing the height of the sun. We have gradually moved from an approximate and indefinite world measured through our eyes to a precise universe where every aspect can be accurately calculated by modern technologies.[5] However, so far, there has been one tiny part of human judgment that has never been surrendered to machines. The most important decisions concerning the life of individuals, especially those related to their legal status, have been preserved in the hands of human beings. People rely on doctors to assess their health, judges to protect their legal right, banks to save their money. Humans have always been judged by other humans.

The impetuous development of artificial intelligence is now challenging this last bastion of humanity. Today, machines can automatically make decisions in a quicker and, at first sight, more neutral way than human beings. This can be explained by the fact that, in order to take decisions, humans need to consider and assess a series of information. From this point of view, machines largely overtake the human capability to analyse large amounts of data. In principle, automated decision-making systems can thus be more accurate, fast and fair than human beings.

Yet, this observation appears to collide with the approach adopted by data protection law in the EU. In fact, the general principles of the General Data Protection Regulation (GDPR)[6] restrict the possibility to use massive amount of personal data to feed mechanisms of automated decision-making without ensuring transparency and accountability. Read together with other norms of the GDPR,[7] the prohibition to subject an individual to a decision based solely on automated processing, as enshrined in Article 22, also provides grounds for individuals to defend themselves from potentially harmful consequences of the implementation of algorithms, most notably by creating a 'right to explanation' in respect of automated decision-making processes.[8]

This apparent contradiction begs a fundamental question: why, in principle, should the GDPR limit automated decision-making, if it appears to be more accurate and quicker than human judgment? Or, in more general terms: if machines can replace human reasoning with algorithmic calculation, and perform this task in an apparently more efficient way than us, why

Work, and Think (Houghton Mifflin Harcourt 2013).

[4] DK 80 B1 in Carol Poster, 'Protagoras' Internet Encyclopedia of Philosophy, <https://www.iep.utm.edu/protagor/> accessed 27 September 2019.

[5] Alexandre Koyre, *From the Closed World to the Infinite Universe*, (1st edn, Johns Hopkins University Press 1968).

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119

[7] Ibid Arts 13-14.

[8] See, in particular, Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation' (2017) 38 *AI Magazine* 50; Andrew D. Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 *International Data Privacy Law* 233.

should we design safeguards to such a technological development? This paper argues that an answer to this question clearly emerges from an analysis of the message of the GDPR from a European constitutional law standpoint. Although the GDPR does not formally have any constitutional character, it can be said to play a para-constitutional role from a functional point of view: it translates and implements core constitutional principles in the troubling context of the algorithmic society. This paper shows that the GDPR's framework on automated decision-making aims to preserve and enhance a series of key constitutional values, preserving human autonomy, increasing legal certainty, and providing more procedural safeguards.

Despite the opportunities triggered by the spread of artificial intelligence, these technologies have also raised new challenges for fundamental rights and democracy. We believe that, even if not exclusively, data protection is a critical piece of the puzzle to protect constitutional values in the algorithmic society. Therefore, unveiling the constitutional role of the GDPR provides a standpoint to interpret the safeguards on which individuals can rely to protect their rights and freedoms in the information society. For this reason, we highlight how the GDPR is promoting a constitutional message deeply rooted in a new form of humanism, which we call 'digital humanism': a conception of the digital society where the human being and her dignity should resolutely outrank machines, technology and, ultimately, economic efficiency.[9]

Our analysis will proceed as follow. In order to understand the rationale behind the GDPR's restriction of automated decision-making, we will first start from tracing the legislative origin of such norms. Interestingly, we will observe that early pan-European data protection law, although emerging as a response to automation, did not specifically include any provisions on automated decision-making. We will then explain that clauses limiting automated decision-making were incorporated in the 1995 Data Protection Directive under the influence of French data protection law, which was the only piece of legislation in Europe regulating that matter. In the following section, we will argue that the decision of the European legislator to restrict automated decision-making, thus following the unique approach adopted by French law, can be explained by looking at the crucial role that this piece of legislation plays in preserving the traditional human-centric stance of the European constitutional tradition. We will identify and analyse a series of constitutional values, focusing in particular on human dignity, the rule of law and due process. We will illustrate how, after being translated in the context of the digital society, they inform and justify the GDPR's approach to automated decision-making.

2. Data Protection Law as an Answer to Automation

The roots of data protection law in Europe are far from the algorithmic society. The path towards data protection started from the evolution of the concept of privacy elaborated since the end of the nineteenth century in the United States.[10] European data protection law epitomises the transition from a merely negative conception of privacy, characterised by liberal

[9] See, e.g., 'DIGHUM – Digital Humanism', <https://www.informatik.tuwien.ac.at/dighum/> accessed 10 March 2020.

[10] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harv. L. Rev.* 193; Peter Blume, 'Data Protection and Privacy – Basic Concept in a Changing World' (2010) 56 *Scandinavian Studies in Law* 151.

imprinting and intended as the right to be let alone, to a positive and dynamic set of rights enabling the individual to maintain control of, and therefore, protect their personal data.[11]

Such a development is mainly due to two related factors which emerged in the 1960s and characterised the following decades: the rise of automation and interconnection. In 1968, the Parliamentary Assembly of the Council of Europe recommended the institution of a committee of experts to examine whether 'the national legislation in the member States adequately protects the right to privacy against violations which may be committed by the use of modern scientific and technical methods'.[12] The report of the Committee eventually highlighted a series of privacy-related issues linked to the then emerging use of automated data banks. This new technology was introduced in the 1960s. According to the Oxford English Dictionary, the term 'database' first appeared in 1955.[13] The notion of database was not associated with all kinds of collection of data, but since the beginning denoted systems processing data in an automated way.[14] The advent of computing technologies for the first time made possible the storage and retrieval of an unprecedented amount of data at lower costs. At the same time, electronic communications networks increased the speed of transferring large sets of information, creating in this way systems of automated and interconnected data banks.

Thanks to the advent of these new technologies, the functioning of data management systems both in the public and private sector was significantly improved. However, at the same time, a series of new risks related to the automated processing of data emerged.[15] In 1983, the Bundesverfassungsgericht, the German federal constitutional court, struck down some provisions of a new federal law allowing for the collection and exchange of census data among national and regional authorities.[16] This decision, known as the *Volkszählungsurteil* or census case in English, became a leading precedent because it developed a right to 'informational self-determination' stemming from a combined reading of the Article 2.1 of the German Basic Law, enshrining a general right to personality, and Article 1.1, protecting the value of human dignity.[17] This ruling is paradigmatic because the Court pragmatically recognised the pros and cons of automated data processing in a broad context. The Bundesverfassungsgericht, on the one hand, acknowledged the significance of collecting and processing personal data for the development of public policies in an industrialised country such as Germany. On the other

---

[11] Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds.), *Reinventing Data Protection?* (Springer 2009) 77.

[12] Parliamentary Assembly of the Council of Europe, 'Recommendation 509 (1968) - Human Rights and Modern Scientific and Technological Developments', <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en> accessed 24 September 2019.

[13] See 'Database, n.', in *OED Online* (Oxford University Press), <https://www.oed.com/view/Entry/47411> accessed 24 September 2019.

[14] See 'Database | Definition, Types, & Facts', Encyclopedia Britannica, <https://www.britannica.com/technology/database> accessed 24 September 2019; Hector Garcia-Molina, Jeffrey D. Ullman and Jennifer Widom, *Database Systems: The Complete Book* (Pearson 2008).

[15] Council of Europe, 'Convention no. 108/1981 - Explanatory Report', <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434> accessed 4 December 2018.

[16] BVerfG 15 December 1983, 1 BvR 209/83, *Volkszählung*.

[17] See Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 *Computer Law & Security Review* 84; Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds.), *supra* n. 11.

hand, it warned against the risks that this phenomenon can create for the individuals, in cases where they may not be aware of the fact that their data have been stored, aggregated and potentially used for other purposes, including that of administrative enforcement of tax or social security law. In the words of the Court:

> Given the current and future state of automated data processing, [the right to self-determination] merits a special measure of protection. It is especially threatened since it is no longer necessary to consult manually assembled flies and dossiers for the purposes of decision making processes, as was the case previously; to the contrary, it is today technically possible, with the help of automated data processing to store indefinitely and retrieve at any time, in a matter of seconds and without regard to distance, specific information on the personal or material circumstances of individuals whose identity is known or can be ascertained (personal data (see s. 2.1 of the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG)). This information can also be combined – especially if integrated information systems are set up – with other collections of data to assemble a partial or essentially complete personality profile without giving the party affected an adequate opportunity to control the accuracy or the use of that profile. As a result, the possibilities for consultation and manipulation have expanded to a previously unknown extent, which can affect the conduct of the individual because of the mere psychological pressure of public access. [...] The usefulness and possible uses of the information are what are of decisive importance. This depends on the one hand upon the purpose served by the survey and on the other hand upon the possibilities for processing and collating information inherent in information technology. This is what makes it possible for data that are in and of themselves of no significance to take on new importance; in that respect, "unimportant" data no longer exist in the context of automated data processing.[18]

Electronic databases could process data related to the private life of individuals, such as records on medical status, income, social security or creditworthiness. Individuals could ignore the existence of those data, could be subject to decisions having significant effects on their life, and yet they could have no control over them.[19] In other words, if the right to privacy was initially enough to meet the interests of individuals' protection in the information society, a negative right was no longer sufficient. The widespread processing of personal data led to the rise of a positive dimension of this right, aiming to increase the degree of transparency and accountability in data processing.[20]

In Europe, national legislation addressing these issues emerged from the 1970s in response to the increasing use of new automated technologies.[21] In 1973 and 1974, the Council of Europe

---

[18] *Volkszählung*, *supra* n. 16, paras. C.II.1.a) ff. English translation available at <https://freiheitsfoo.de/census-act/> accessed 10 March 2020.

[19] Council of Europe, 'Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (1981) para. 2.

[20] It is interesting to recall the distinction between privacy as an instrument of opacity for the protection of the individual and data protection as a transparency tool. See Serge Gutwirth and Paul De Hert, 'Regulating Profiling in a Democratic Constitutional States' in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen* (Springer 2006) 271.

[21] David H. Flaherty, *Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden,*

adopted two resolutions 'on the protection of the privacy of individuals vis-à-vis electronic data banks' respectively in relation to the private and the public sector.[22] From the end of that decade, it was apparent that a plurality of different national statutes regulating data protection created a heterogeneous legal framework that could have potentially hindered the free flow of data within Europe. The OECD's Guidelines governing the protection of privacy and transborder flows of personal data of 1980 and the Council of Europe's Convention no. 108/1981 represented the first normative reactions to this issue. They both aimed to provide member states with a set of minimal rules on the processing of personal data and to introduce a common mechanism regulating transnational data flows. However, for the purposes of this paper, it is interesting to notice that the OECD Guidelines do not exclusively apply to automated data processing. In the Preface of the Guidelines, 'automatic data processing' is recognised as the primary factor requiring rules on data processing. Yet, the Guidelines do not restrict their scope to such a category of data processing. The Explanatory Memorandum justifies this choice as a way to prevent potential circumvention of data protection norms, given the unclear boundaries between automated and non-automated processing.[23]

Conversely, the Council of Europe's Convention no. 108/1981 focuses exclusively on 'automatic processing', solving the OECD dilemma by including semi-automated data processing within its scope of application.[24] The adoption of the Convention no. 108/1981 on the Protection of Individuals with regard to Automatic Processing of Personal Data constituted a crucial step in the relationship between data protection and automation. No other instruments at the international law level provide for a legally binding commitment in the field of data protection applying globally and horizontally to public and private sector processing.

These differences, of course, do not deny the crucial role that automation played as a trigger for data protection law in Europe. However, they clearly show that the regulatory approach that was eventually adopted in the old continent was more holistic. Both the OECD Guidelines and the Convention no. 108/1981 pragmatically regulated forms of processing that are not fully automated, but that present similar risks for the protection of individual rights. In an analogous way, the Data Protection Directive and the GDPR adopted a mixed approach. Their scope of application encompasses both wholly or partly automatic processing of data and manual processing, in the latter case at the condition that personal data become part of a structured filing system where data are easily accessible.[25]

France, Canada, And the United States (The University of North Carolina Press 1989).

[22] Respectively, Council of Europe Resolution (73) 22 *on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector* and Council of Europe Resolution (74) 29 *on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector*. See Lee A. Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014).

[23] Organisation for Economic Co-operation and Development, 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD', paras. 34–35, <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 24 September 2019.

[24] Council of Europe, 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (1981) Art. 1-2.

[25] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281, Art. 2-3, Recitals 15, 27; GDPR, Art. 2, 4, Recital 15.

Interestingly, early case-law and legislation in the field of data protection, although addressing issues related to automated data processing, did not focus on automated decision-making. In 1983, the Bundesverfassungsgericht assessed the possibility for German federal and local authorities to use data collected for statistical purposes in order to adopt social and economic policies, or to enforce specific areas of law, such as those related to taxes and social benefits. However, the Court did not directly address the issue of automated data processing embedded in a, at its turn automated, decision-making mechanism. Similarly, as we will see in the next section, both the OECD Guidelines and the Convention no.108/1981 did not originally regulate automated decision-making. Only in 2018, the modernized version of the Convention no. 108/1981 introduced a right not to be subject to decisions solely based on automated data processing,[26] including in its new Preamble a reference to human dignity as a guiding principle in the field of automated processing.

As the next paragraph will show, the provision regulating automated decision-making at EU level, once enshrined in Article 15 of the Data Protection Directive and, now, in Article 22 of the GDPR, did not derive from international data protection instruments and instead represents a direct legacy from French law.

3. From the Loi Informatique et Libertés to the GDPR

The Data Protection Directive explicitly recognised to represent the heir of the principles set in the Convention no. 108/1981.[27] Yet, it is interesting to notice that the Directive, as now the GDPR, regulate a specific aspect of automated processing that is not mentioned in either the Convention no. 108 or in the OECD Guidelines of 1980.[28] Article 15 of the Directive, and today Article 22 of the GDPR, establish a series of rules on automated decision-making, i.e. on that specific form of data processing that leads to the adoption of a decision.

Potential negative consequences for the protection of individual freedoms engendered by automated decision-making were certainly already known at the time of the adoption of the Convention no. 108/1981. Indeed, the Explanatory Report to the Convention explicitly refers to this phenomenon.[29] However, as said, the instrument of the Council of Europe did not set any particular norm to address this issue. Nor did any national data protection legislation – but one, as we will see – include any principles on automated decision-making prior to the adoption of the Directive. In conclusion, there is no doubt on the paternity of Article 15 of the Directive: it was clearly a legacy of the French national legislation on data protection, the so-called *loi informatique et libertés*.[30]

---

[26] Council of Europe, 'Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data' (2018) Art. 9(1)(a) <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf> accessed 10 March 2020

[27] Data Protection Directive, *supra* 25 Recital 11.

[28] The modernized version of the Convention no. 108/1981 now includes a similar provision at Article 9(1)(a). See Council of Europe, *supra* n. 26.

[29] Council of Europe, 'Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (1981) para. 2: 'In modern society, many decisions affecting individuals are based on information stored in computerised data files: payroll, social security records, medical files, etc'.

[30] See Lee A. Bygrave, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 *Computer Law & Security Review* 17; Isak Mendoza and Lee A. Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' SSRN (8 May 2017)

Back in 1974, the deputy of the French Assemblée Nationale, Pierre-Bernard Cousté, proposed the institution of a commission to monitor the developments of computing technology to ensure the respect of private life and other individual freedoms.[31] This initial idea eventually led to a bill backed by the Chirac government and presented two years later, in 1976.[32] The executive proposed the adoption of a statute relating to *informatique et libertés*, computing and freedoms. It not only provided for the institution of a permanent commission controlling the respect of data protection norms both in the public and private sector (Chapter 1), as in the original Cousté bill, but also established a series of general principles of lawful data processing (Chapter 2 and ff.).

Interestingly, the 1976 bill was opened by three general principles, two of them related to automated decision-making. Article 1 established that the respect of private life and individual and collective freedoms should be considered of paramount importance in the development of computing technologies. Article 2 specifically focused on automated decision-making: 'No judicial or administrative decision implying an assessment of human behaviour shall be solely based on automated data processing'.[33] Article 3 was more general, but was logically linked to Article 2, and therefore to the prohibition of fully automated decision-making: 'Everyone has the right to know and to contest the data and the logic employed in automated data processing that negatively affect her'.[34]

In 1977, the French Communist Party proposed a bill 'sur les libertés, les fichiers et l'informatique', identifying the triad of freedoms, files and computing that will eventually compose the final title of the French data protection law in 1978. The 1977 bill attempts to broaden the scope of Article 3 by providing the right to know and contest the data and the logic employed in automated and non-automated data processing.

A report of the Law Committee of 1977 marked the definitive change of the physiognomy of Articles 2 and 3.[35] The law that was finally promulgated by the French President in 1978 distinguished between judicial decisions and decisions taken by the public administration or by private entities. According to Article 2, 'No judicial decision implying an assessment of human behaviour shall be based on automated data processing defining the profile or the personality of the data subject'. Therefore, the norm not only bans those decisions based *solely* on automated processing, but more extensively all judgments founded on automated data processing. The Law Committee, in its report, explains that this clarification was justified by the intention to maintain 'the character of the judicial decision, certainly fallible, but essentially

<https://papers.ssrn.com/abstract=2964855>; Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 24 C*omputer Law & Security Review* 398.

[31] See 'Proposition de loi tendant à créer une Commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens' 1974, <https://www.senat.fr/leg/ppl73-1004.html> accessed 10 March 2020.

[32] See 'Projet de Loi relatif à l'informatique et aux libertés' 1976, <https://www.senat.fr/leg/pjl76-2516.html> accessed 10 March 2020.

[33] Ibid. our translation.

[34] Ibid. our translation.

[35] Rapport N° 72 (1977-1978) de M. Jacques THYRAUD, Fait au nom de la Commission des lois, déposé le 10 novembre 1977, 1977 <https://www.senat.fr/rap/l77-072/l77-072.html> accessed 10 March 2020.

human'.[36] Human beings should not escape their responsibilities, above all that of judging their counterparts.[37] Conversely, in relation to the decisions made by the public administration and private entities, the second paragraph of Article 2 specifies that only those *solely* relying on automated data processing are forbidden. Therefore, this norm further circumscribes its scope of application, and mitigates the outright ban established in relation to judicial decisions. Article 3 on the individual right to know and contest the data and the logic underlying the processing maintains its original formulation.

Notwithstanding the unicity of these norms in the European panorama of the time, in 1995, the European legislator decided to follow the French model and to incorporate specific provisions on automated decision-making in the text of the Data Protection Directive. This choice was mainly justified as a response to the increase in data usage and processing for providing public services in the context of the welfare state. At that time, the European Commission underlined that a norm on automated decision-making was necessary to 'protect the interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institutions deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'data shadow'.[38]

Article 15 of the Data Protection Directive established 'the right [of] every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.' Article 3 of the *loi informatique et libertés* concerning the rights to know and contest the data and the logic underlying the data processing was incorporated in Article 12 and 15(2) of the Data Protection Directive, respectively.

From a substantive point of view, the principle established in Article 15(1), which was at its turn qualified by a series of exceptions listed in the second paragraph of the Article, appears to be a mixture of Article 2 of the French bill of 1976 and its final version of 1978. The Directive does not distinguish between judicial decisions, and administrative and private decisions. It does not focus on the source of the decision, but, more pragmatically, on its effects. It encompasses both decisions having legal effects, and decisions that, although not having any legal effect, significantly affect the data subjects. Therefore, it potentially refers to decisions taken by judicial authorities, administrative and private bodies. Moreover, the Directive mitigates the absolute ban of Article 2(1) of the final version of the French statute prohibiting judicial decisions based on automated data processing. Only those decisions *solely* based on automated data processing are restricted in principle.

Article 22 of the General Data Protection Regulation, which entered into force in May 2018, essentially reiterates the content of Article 15 of the Data Protection Directive.[39] Its first

[36] Ibid. 22.

[37] Ibid.

[38] European Commission, 'Explanatory text for Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data' COM(90) 314 final, 29.

[39] For an exhaustive analysis of Article 22, see Stephan Dreyer and Wolfgang Schulz, 'The General Data Protection Regulation and Automated Decision-Making: Will It Deliver?: Potentials and Limitations in Ensuring

paragraph generally prohibits decisions having legal or similarly significant effects and that are solely based on automated data processing. Paragraph 2 lists three exceptions to this principle. Paragraph 3 enshrines a series of minimal rights that the data subject should enjoy when she is affected by a fully automated decision-making process. Paragraph 4 provides for further safeguards in case of processing of particular categories of data, formerly known as sensitive data.

Interestingly, the *loi informatique et libertés*, as amended after the entry into force of the GDPR, still maintains a specific regime for judicial decisions. In 2004, the traditional distinction between judicial, administrative and private decisions was replaced in order to narrow the distance between the domestic law and the Directive. The then Article 10 of the *loi informatique et libertés*, as amended in 2004, differentiated between judicial decisions and other decisions having legal effects.[40] Today, after the last amendments entered into force in June 2019, Article 47 establishes two different regimes according to the presence of a judicial decision or a decision having legal or significant effects on the individual.[41] Although the last version of the statute is closer to the text of the GDPR, French law still resolutely prohibits that judicial decision be based – fully or partially – on automated data processing aiming to define the personality of an individual.

4. Exploring the Constitutional Message of the GDPR

In the previous sections, we have reconstructed the genealogy of the GDPR framework on automated decision-making and traced back its origin to a single national law: the French *Loi informatique et libertés*. Despite the unicity of the French approach in the European legislative panorama, we consider that the incorporation of norms restricting automated decision-making in the Data Protection Directive – and today in the GDPR – can be justified by the fact that their underlying principles and objectives were deeply rooted in a series of European shared constitutional values. Even if the Data Protection Directive was introduced before the adoption of the Charter of Fundamental Rights of the European Union (Charter),[42] we observe that a series of common constitutional principles have influenced the economic-oriented approach of the Data Protection Directive, whose primary aim was to ensure a harmonised framework for the free-flow of personal data in the internal market. The GDPR – we will argue – has further consolidated this constitutional role of EU data protection law.

Article 1 of the GDPR explicitly states that the aim of the Regulation is 'in particular', to safeguard the right to the protection of personal data of natural persons. However, the same provision recognises that the GDPR generally seeks to protect the fundamental rights and freedoms of the individuals since this right is not absolute. In any case, as stressed by Recital 4, 'the processing of personal data should be designed to serve mankind'. This is not a

---

the Rights and Freedoms of Individuals, Groups and Society as a Whole' (2019) <https://www.bertelsmann-stiftung.de/doi/10.11586/2018018> accessed 27 January 2020.

[40] Loi N° 78-17 Du 6 Janvier 1978 Relative à l'informatique, Aux Fichiers et Aux Libertés | Legifrance (Version Consolidée 2004) <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20041124> accessed 10 March 2020.

[41] Loi N° 78-17 Du 6 Janvier 1978 Relative à l'informatique, Aux Fichiers et Aux Libertés | Legifrance (Version Consolidée Juin 2019) <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20190926> accessed 10 March 2020.

[42] Charter of Fundamental Rights of the European Union (2012) OJ C 326, 391–407.

redundant statement, but the result of a complex process of constitutionalisation that has occurred in Europe in the last few decades. While EU data protection law was introduced at the end of last century to harmonize national laws and to ensure a smooth flow of data between member states, this economic aim has progressively been flanked and then – one can argue – supplanted by the need to protect a series of fundamental rights of the individual. Over the past few years, the principles of data protection law have been gradually constitutionalised as necessary safeguards to guarantee the respect of other fundamental rights.[43] Today, an autonomous right to data protection is enshrined in Article 8 of the Charter,[44] and Article 6 of the Treaty on the Functioning of the European Union.[45] In particular, the role of the European Court of Justice has been fundamental in the process of consolidation and emancipation of this right. On the one hand, the Court has recognised its relevance in the *Promusicae* case, linking data protection to the safeguard of private life.[46] On the other hand, the Court has vigorously striven to ensure the 'effective protection' of this fundamental right. This approach is particularly apparent in the decisions following the entry into force of the Lisbon Treaty, especially, in *Digital Rights Ireland*,[47] *Google Spain*,[48] and *Schrems*.[49] These decisions by the European Court of Justice have stressed how automation can be identified as one of the primary factors of risk, requiring higher safeguards to be implemented. In the words of the Court, the need for safeguards is 'all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data'.[50]

This shift from a predominantly economic and functional perspective to a fundamental rights-based approach as promoted by the judicial activism of the Court is reflected in several provisions of the GDPR. The general principles driven by the data controller's accountability or the principles of privacy by design and by default are just two examples showing the GDPR's intention to ensure that data protection is not treated only as a matter of compliance, but it is embedded in data controllers' activities to assess the challenge that the processing

---

[43] Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Gutwirth and others (eds.), *supra* n. 11.

[44] Charter, *supra* n. 42 Art 8.

[45] Consolidated version of the Treaty on the Functioning of the European Union (2012) OJ C 326, 47–390.

[46] Case C-275/06 *Productores de Música de España (Promusicae)* v *Telefónica de España SAU* [2008] ECR I-00271. See Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).

[47] Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12)* [2014] OJ C 175. See Edoardo Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (2019) 15 *EuConst* 134.

[48] Case C-131/12, *Google Spain SL and Google Inc.* v *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] OJ C 212. See Orla Lynskey, 'Control over personal data in a digital age: *Google Spain v AEPD* and Mario Costeja Gonzalez' (2015) 78 *Modern Law Review* 522.

[49] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* [2015] OJ C 351. See Oreste Pollicino and Marco Bassini, 'Bridge Is Down, Data Truck Can't Get Through... A Critical View of the Schrems Judgment in the Context of European Constitutionalism' (2017) 16 *The Global Community Yearbook of International Law and Jurisprudence* 245.

[50] *Digital Rights Ireland*, *supra* n. 47, paras. 54 and 55 and *Schrems*, *supra* n. 49, para. 91. See, also, *S. and Marper v. United Kingdom* App. no. 30562/04 and 30566/04 (ECtHR, 4 December 2008) para. 103; *M. K.* v *France* App. no. 19522/09 (ECtHR, 18 April 2013), para. 35.

presents for data subjects.[51] In other words, these principles have allowed the whole system to move from a reactive (or ex-post) approach to a proactive (or ex-ante) strategy of risk assessment. Furthermore, one can mention the obligation to carry out the Data Protection Impact Assessment, which explicitly aims to address the risks deriving from automated processing 'on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person'.[52]

The prohibition to subject an individual to a decision based solely on automated processing complements this legal framework. Dreyer and Schulz even talk of a 'shift of the focus of protection' in this norm.[53] The primary purpose of data protection law would be converted to defend a series of values that automated decision-making puts under threat. The analysis of these values is quintessential. The existing scholarship highlighted a significant number of doubts in relation to the interpretation of this norm.[54] A potential method to address them could therefore be to embrace a theological interpretation, elaborating on the specific constitutional values underlying the GDPR's provisions on automated decision-making. In this way, a constitutional reading of the GDPR would aim to provide the basic principles which should guide the interpretation and future development of norms regulating automated decision-making systems.

In this context, one could speak of 'constitutional values' because the GDPR, and more broadly European data protection legislation, ultimately plays a para-constitutional role.[55] Although not having any formal primary value, its norms convey a constitutional message. In contrast to the OECD Guidelines of 1980, the Convention no. 108/1981 of the Council of Europe was the first pan-European text to consider the protection of fundamental rights as an equally important objective besides preserving transnational trade. The Data Protection Directive followed this model, mentioning in its first article both the safeguard of personal freedoms and the need to maintain a free flow of information among member states. Originally created also to safeguard commercial freedoms, data protection law is currently playing a key role in the process of evolution of contemporary constitutionalism vis-à-vis the challenges of the digital age. The GDPR implements a series of principles which are direct corollaries of a series of fundamental values. It perpetuates core elements of contemporary constitutionalism in the context of the digital society. One could argue that it is a direct expression of what has been called 'digital constitutionalism'.[56]

---

[51] GDPR, Art. 25.

[52] Ibid Art. 35(3)(a).

[53] Dreyer and Schulz, *supra* n. 39, 17.

[54] See, in particular, Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 *Columbia Business Law Review* 1; see also notes 8-11.

[55] This expression was first used by Giorgio Resta, 'Il Diritto Alla Protezione dei Dati Personali', in Francesco Cardarelli, Salvatore Sica and Vincenzo Zeno-Zencovich (eds), *Il Codice dei Dati Personali. Temi e Problemi* (Giuffrè 2004). On the constitutionalising role of EU data protection legislation, see also Paul De Hert and Serge Gutwirth, *supra* n. 11, 13.

[56] See Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33(1) *International Review of Law, Computers & Technology* 76 <https://doi.org/10.1080/13600869.2019.1562604> accessed 10 March 2020; Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2019) <https://papers.ssrn.com/abstract=3506692> accessed 10 March 2020.

EU data protection legislation does not represent a Copernican revolution of the constitutional paradigm. It re-specifies the values of contemporary constitutionalism in light of the needs of the present society, translating them into operational norms. By doing so however, it unavoidably shapes a series of principles that work as the links of the chain connecting fundamental constitutional values with data protection rules. These principles are often implied, even unconscious. Yet, they are key to understand how to interpret and further develop data protection law in a way that perpetuates our core constitutional values in the future digital society. The digital revolution, and especially data processing techniques, are transforming our daily life at an unprecedented speed. Now more than ever the legal system needs long-term reference points to orient its action: constitutional principles that could act as 'lighthouses' shining in the dark.[57] Constitutional law does not pretend to know what the future transformations of our society will be. It has, however, the duty to clearly outline where we want to go.

For this reason, we now delve into an investigation of the constitutional message of the GDPR to show that its aim to protect core foundational principles of our democratic traditions provides a rationale for its approach taken vis-à-vis automated decision-making. In the following sections, we reconstruct the constitutional values and principles which underline the GDPR's normative framework on automated decision making. In particular, we identify three main focal points of the GDPR's constitutional message: human dignity, the rule of law and due process.

4.1 Human Dignity

Let us start this task of constitutional archaeology by analysing the core principle of Article 22. Paragraph 1 establishes a general prohibition of all decisions which a) are exclusively based on a form of automated processing of personal data, and b) generate legal, or at least, significant effects on the data subject. In reality, the letter of Article 22 establishes the right of the individual not to be subject to similar kinds of decisions ('The data subject shall have the right not to be subject to a decision […]'). However, the norm has been consistently interpreted as a general prohibition, with, as we will see later, a limited number of exceptions.[58] Article 22, as well as Recital 71, are silent on the constitutional values that inform this rule. By simply reading the GDPR, one cannot understand the values which this general prohibition seeks to protect. In a similar case, one could hypothesise that this norm shares the overall objective of the GDPR. However, as stated before, the scholarship recognised that the guarantee of the right to the protection of personal data does not represent the primary target of this norm.[59] Article 22(1) would rather aim to protect the constitutional value of human dignity.[60] Let us explore why.

Machines are supposed to be more efficient than human beings. They can perform more complex calculations; they can take into considerations multiple factors at the same time, and

[57] Lawrence Lessig, *Code: and Other Laws of Cyberspace, Version 2.0* (Basic Books 2006); Stefano Rodotà, *Il diritto di avere diritti* (Laterza 2012).

[58] See Veale and Edwards, *supra* n. 30.

[59] See Dreyer and Schulz, *supra* n. 39.

[60] Meg Leta Jones, 'The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 *Social Studies of Science* 216.

they can even be more neutral than human beings.[61] However, machines too can err. They can fail to appreciate all the elements that compose a complex situation, and they can perseverate in that error for a longer time than a human being would do. Machines are ultimately more consistent and neutral than us in erring. At first glance, algorithms could be considered as neutral and independent technologies capable of producing useful information to deal with social changes and market dynamics. From a technical perspective, algorithms are merely methods expressing results within a finite amount of space and time, and in a defined formal language. However, algorithms consist of encoded procedures which transform inputs – made up of data – into outputs on the basis of a specified calculating process.[62] Algorithmic processes are, therefore, value-laden, since ultimately individuals develop such technologies.[63] The human contribution in the development of algorithms unavoidably leads to the translation of personal interests and values into technological processes.[64]

In this way, the use of algorithms can lead to troubling discriminatory effects.[65] The right to non-discrimination is one of the fundamental principles enshrined in member states' constitutions and in the Charter of Fundamental Rights of the European Union. It is based on the general principle of equality according to which similar situations must be treated in the same way and different situations differently. In the case of algorithms, discriminatory results originate from biased evidences and inflexible decision-making processes. This point is shown, for example, by profiling algorithms that produce discriminatory results against marginalised populations, as in the case of delivery of online advertisements according to perceived ethnicity.[66]

After all, a positive characteristic of humans would be to learn from our mistakes. According to the tradition, Seneca would have said: *errare humanum est, perseverare autem diabolicum.* The prohibition introduced by the GDPR concerning automated decision-making processes would, therefore, recognise that machines can err and cannot be fully trusted. However, not in general terms: automated decision making would generate significant advantages from the point of view of economic efficiency. Article 22, in fact, operates a balancing: it does not ban in an outright way the possibility to rely on automated decision making, but it establishes such a prohibition only when something extremely important is at stake. Only when automated decision-making affects the legal status of the individual or produces significant consequences for her, the economic advantage of relying on the choice of a machine would be to sacrifice. In particular, the Article 29 Working Party, the caucus that regrouped the representatives of member states' data protection authorities under the Data

---

[61] Ibid.

[62] Tarleton Gillespsie, 'The Relevance of Algorithms', in Tarleton Gillespie, Pablo J. Boczkowski and Kirsten A. Foot (eds.), *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014) 167.

[63] Philip Brey and Johnny Hartz Soraker, *Philosophy of Computing and Information Technology* (Elsevier 2009); Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society* (Da Capo Press 1988).

[64] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, (Harvard University Press 2015).

[65] Andrea Romei and Salvatore Ruggieri, 'A Multidisciplinary Survey on Discrimination Analysis' (2014) 29 *The Knowledge Engineering Review* 582; Bart Custers et al. (eds.), *Discrimination and Privacy in the Information Society* (Springer 2013); Kevin Macnish, 'Unblinking Eyes: The Ethics of Automating Surveillance' (2012) 14 *Ethics and Information Technology* 151.

[66] Solon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671.

Protection Directive, specified that Article 22 applies to cases of 'serious impactful effects' and when the automated decision could 'significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals'.[67] In these particular situations, the machine has to take into account factors related to an individual, and there is, therefore, a higher risk of error due to the complexity of human life.

Article 22(1), therefore, implicitly provides that, when a decision affects important aspects of human life, machines, alone, do not suffice, and human intervention is needed. In other words, this norm establishes that human life is more important than economic efficiency. Human life requires an anti-economic effort to safeguard its unicity and unrepeatability. Human beings are so unforeseeable and complex that, as a matter of principle, no machine, even the most advanced, could never fully understand them. Humans are unique creatures, *hapax legomena*, as Floridi explained: rare words that are recorded only once in the text of the universe.[68] Montaigne described our life as 'an uneven, irregular, and multiform movement'.[69] Attempting to reduce it to a series of machine-readable data would be impossible. It would imply an objectification, a radical de-humanisation of the individual. Maybe, in the future, the most powerful machine will understand human nature at 99.9%. It is, however, to preserve that potential 0.1% of incomprehensible human existence that Article 22 does not tolerate that a machine alone determines significant aspects of our life. Otherwise, one would deny the uniqueness of the human being, her being versatile and multi-faceted, *polytropos,* as Homer used to say.[70] This characteristic deserves to be respected. The human being is *dignus*, worthy.[71] Reducing their life to mere digits would mean to violate their *dignity*.

This is a lesson that we have learnt from the past. The horrors of Nazism nullified the human person. In concentration camps, people were fully deprived of their humanity, being reduced to serial numbers.[72] Human dignity, therefore, became the mantra of post-war constitutionalism. Article 1 of the Universal Declaration of Human Rights of 1948 affirmed that 'All human beings are born free and equal in dignity and rights'.[73] Article 3 of the Italian Constitution of 1947 recognised that 'All citizens shall have equal social dignity'.[74] The first article of the Basic Law for the Federal Republic of Germany of 1949 guaranteed that 'Human dignity shall be inviolable',[75] a provision which has been used in the aforementioned 'census decision' by the German Federal Constitutional Court to recognise a right to informational self-

[67] WP29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (2018).

[68] See Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 *Philosophy & Technology* 307.

[69] Michel de Montaigne, *The Complete Essays of Montaigne*, trans. Donald M. Frame (Stanford University Press 1957) 621; see Jean Starobinski, *Montaigne in Motion* (University of Chicago Press 1985).

[70] See Floridi, *supra* n. 68.

[71] Rodotà, *supra* n. 57, ch. VI, 'Homo dignus'.

[72] Primo Levi, *If This Is A Man*, trans. Stuart Woolf (Abacus 2014).

[73] Universal Declaration of Human Rights (1948).

[74] Constitution of the Italian Republic (1947).

[75] Basic Law for the Federal Republic of Germany (1949).

determination,[76] and literally reiterated half a century later in the Charter of Fundamental Rights of the European Union.[77]

Today, the human being cannot be reduced to mere digits once again. The prohibition of automated decision-making enshrined in Article 22 reflects the right to escape from the blind determinism of machines and their programmers, ultimately at the service of private and public dominant actors.[78] This provision does not only aim to protect the dignity of single human beings, but that of the whole humanity.[79] In 1995, the Data Protection Directive stated that 'data-processing systems are designed to serve man […] and contribute to economic and social progress, trade expansion and the well-being of individuals'.[80] Today, the GDPR underlines that 'the processing of personal data should be designed to serve mankind'.[81] Moreover, it is not by chance that, recently, the High-Level Expert Group on Artificial Intelligence proposed a human-centric approach.[82] Not a long time ago, the European Data Protection Supervisor also stressed that: '[The] respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual. It should be at the heart of a new digital ethics'.[83]

In conclusion, the GDPR is guaranteeing the existence of a diverse, irrational, and less schematised society. Article 22 not only finds its conceptual roots in the protection of human dignity, but it also translates this value in the context of artificial intelligence. The GDPR, by crafting a norm implementing human dignity in the present social reality, unavoidably shapes a new constitutional principle according to which human life is worthier than economic efficiency. The value of human dignity in the age of artificial intelligence means that women and men are more important than machines. The diversity of human life cannot be sacrificed on the altar of economic efficiency. The Constitution of the German city-state of Bremen was a pioneer in establishing this principle in relation to the right to data protection. Its Article 12 foresightedly stated: 'Der Mensch steht höher als Technik und Maschine', the human being outranks technology and machines.[84] This principle represents the key connection between the value of human dignity and the prohibition of automated decision making established in Article 22. So far, it is only implicit in the GDPR, but it is now time to adopt it as a guideline for the interpretation of existing norms and the development of further legislation.

---

[76] *Volkszählung*, *supra* n. 16.

[77] Charter, *supra* n. 42 Art. 1.

[78] Antoinette Rouvroy, 'Technology, Virtuality and Utopia: Governmentality in an Age of Autonomic Computing' in Mireille Hildebrandt and Antoinette Rouvroy, *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology* (Routledge 2011) 119, who talks of a 'statistical governance of the real'.

[79] See Floridi, *supra* n. 68; Rodotà, *supra* n. 57, ch. V.

[80] Data Protection Directive, *supra* 25, Recital 2.

[81] GDPR, 1–88, Recital 4.

[82] High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (8 April 2019) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419> accessed 15 February 2020.

[83] European Data Protection Supervisor, 'Opinion 4/2015, Towards a New Digital Ethics' 11 September 2015 <https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf> accessed 28 January 2020.

[84] Landesverfassung der freien Hansestadt Bremen (1947).

4.2 Rule of law

Article 22 does not establish an absolute prohibition in relation to automated decision-making. Even in circumstances where a decision exclusively based on automated processing has legal or similarly significant consequences on the data subject, the GDPR establishes a series of exceptions. They are three in total, and they are specified in Article 22(2).[85]

At first sight, their presence seems to be absolutely justified. A peculiarity of European constitutionalism is that fundamental rights do not enjoy absolute protection. In the EU framework, fundamental rights are subject to limitations according to the test established by Article 52 of the Charter.[86] Interferences with fundamental rights are limited to what is strictly necessary to genuinely meet the objectives of general interest pursued, subject to the principle of proportionality. There is no case in which the protection of fundamental rights can lead to the 'destruction of any of the rights and freedoms recognised in this Charter or at their limitation to a greater extent than is provided for herein'.[87] As underlined by the ECJ, the right to the protection of personal data, too, is not an absolute right, but must be balanced against other societal interests.[88]

However, although these exceptions could find sound grounds, one could also argue that their existence manifestly contradicts the need to protect human dignity in the algorithmic society. How is it possible to establish exceptions to the principle of respect for human dignity? How could one tolerate episodes of human objectification and, consequently, dehumanisation? In this paragraph, we explore a series of further guarantees that the GDPR offers in those circumstances in which automated decision-making is exceptionally admitted. We understand that these safeguards ultimately preserve human dignity by establishing the right of the data subject to ask a re-humanisation of the decision.

From a chronological perspective, we can distinguish two kinds of additional guarantees: ex-ante and ex-post.[89] The former category identifies a series of safeguards that the data controller is obliged to provide before the start of the decision-making process. The latter conversely characterises those duties that have to be guaranteed once a decision has already been taken. Starting from the ex-ante guarantees, Article 13 of the GDPR establishes the duty of the data controller to inform the data subject, at the moment of the collection of data, about the existence of a process of automated decision-making, its logic, significance and consequences. Furthermore, Article 15 confers on the data subject the right to ask the data controller to access her personal data.

These norms implement two constitutional values. Firstly, they aim to safeguard the ability of the data subject to freely develop her personality and fully exercise her personal freedom in the digital environment. By ensuring a transparent use of automated decision-making processes, the GDPR enables the data subject to autonomously and consciously manage her

---

[85] GDPR, Art. 23. This provision allows member states to restrict Art. 22 provided that such restrictions respect the essence of the fundamental rights and freedoms and are necessary and proportionate measures in a democratic society to safeguard legitimate interest listed in Art. 23.

[86] See also European Convention on Human Rights (1950), Art. 8(2).

[87] Charter, *supra* n.42 Art. 54.

[88] Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert* [2010] ECR I-11063; GDPR, Recital 4.

[89] Dreyer and Schulz, *supra* n. 39.

digital persona.[90] The individual becomes aware of the existence of a process of automated decision-making and can consequently direct her behaviour in light of this information. Therefore, freedom to develop one's personality and personal freedom, as translated in the GDPR, imply the recognition of the principle of informational self-determination of the data subject.[91]

It is not a coincidence that transparency is at the core of the debate about algorithms.[92] The risks for fundamental rights are strictly linked with the lack of transparency about the functioning of automated decision-making processes.[93] Ensuring transparency could be complex for reasons relating to the protection of other interests, such as trade secrets.[94] Since algorithms are becoming always more pervasive in everyday life, individuals will increasingly expect to be aware of the implications deriving from the use of these technologies. Nowadays, social awareness of automated decision-making is still very limited. Often individuals are not conscious of the ethical (and legal) implications that the use of algorithms has on their life. Individuals are increasingly surrounded by technical systems influencing their decisions without the possibility to understand or control this phenomenon, and, as a result, to participate consciously in this society.

Secondly, Articles 13 and 15 represent an essential instrument to rebalance power asymmetries among the actors involved.[95] This constitutional reading of these provisions is generally neglected by the existing scholarship. The data subject undoubtedly embodies the weak actor in the relationship with the data controller. However, the GDPR re-equilibrates natural informational asymmetries by providing the individual with a series of information about the processing of her personal data. In this way, automated decision-making ceases to be an inscrutable phenomenon for the data subject.[96] The data controller has the duty to disclose the presence of automated decision-making and explain the logic underlying such process, an obligation which requires to show the existence of a series of predetermined, logical and non-arbitrary criteria. Automated decision-making cannot be tolerated if it is entirely subject to the opaque discretion of the machine.

We could argue that, in this way, the GDPR is translating the value of the rule of law in the context of automated decision-making. As the state is not subject to the free will of the ruler, but should respect predetermined laws, the GDPR bans indiscriminate processes of automated

---

[90] See Rodotà, *supra* n. 57.

[91] See *Volkszählung*, *supra* n. 16.

[92] See, in particular, Daniel Neyland, 'Bearing accountable witness to the ethical algorithmic system' (2016) 41 *Science, Technology & Human Values* 50; Mariarosario Taddeo, 'Modelling Trust in Artificial Agents, a First Step Toward the Analysis of E-Trust' (2010) 20 *Minds and Machines* 243; Matteo Turilli and Luciano Floridi, 'The Ethics of Information Transparency' (2009) 11 *Ethics and Information Technology* 105.

[93] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 *Big Data & Society*; Christopher Kuner et al., 'Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?' (2017) 6 *International Data Privacy Law* 167; Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', in Jacques Bus and others (eds.), *Digital Enlightenment Yearbook* (IOS Press 2012).

[94] Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press 2014).

[95] Rodotà, *supra* n. 57, who in similar terms talks about the rebalancing function of national data protection authorities.

[96] See Veale and Edwards, *supra* n. 30.

decision-making. EU data protection law, therefore, translates (and fosters) the constitutional principle of the rule of law to the private arena. Non-state actors are generally not required to explain the logic of their actions and decisions. However, in the context of the digital society, the scenario has mutated. Powerful private companies creating, managing and selling digital products and services emerge as new dominant actors besides the State. The data subject is a particularly vulnerable actor and her electronic body requires further protection. Articles 13 and 15, therefore, enshrine the principle of the rule of law in the context of automated decision-making: an additional guarantee to balance powers in the digital environment.

From this observation, we can thus derive a further finding from a wider perspective. The GDPR is a legislation that reflects a new societal context. Its norms are sensitive to a reality which is no longer dominated by states, but witnesses a plurality of dominant actors, both public and private, rivalling in a context that has definitively become transnational, not to say global. The sense of constraining the constitutional value of balancing of powers within the boundaries of the relationship citizens-state unavoidably fades. The individual finds herself in a weak position with regard to a variety of actors, including private companies. The GDPR, therefore, by implementing a plurality of constitutional values in the context of private actors, spurs an evolution of contemporary constitutionalism. This legislation is highlighting the need to extend the personal scope of application of constitutional values: not only citizens, but all individuals should be protected against the arbitrary use of automated decision-making; not only states, but all dominant actors, in particular, powerful private companies, should be subject to constitutional constraints.

4.3 Due process

Simply enabling data subjects to be aware of the existence of an automated decision-making process and its characteristic, however, could not suffice to rebalance the asymmetry of power between individuals and data controllers. The scholarship talked of 'transparency fallacy' in this context.[97] Moreover, the ex-ante guarantees presented above do not solve the problem of potential violations of human dignity. For this reason, the GDPR also prescribes an important safeguard that acts ex-post, i.e. once a decision exclusively based on automated processing has already been taken.

Article 22(3) provides the right of the data subject to require human intervention, to express her point of view and to contest the decision.[98] Such a right confirms the general approach of the GDPR contrasting exclusively automated decision-making processes. Decisions solely based on machines are prohibited or, if admitted, the individual can always urge human intervention. Theoretically, one may think that a right to express one's own point of view and to contest the decision could be exercised with a machine. However, the GDPR

[97] Ibid.

[98] This right is explicitly provided in two (letter (a) and (c)) of the three exceptional circumstances in which a decision solely based on automated processing of data and producing legal or similarly significant effects is admitted according to Article 22(2). However, it can be considered as implicit in the third case too (letter (b)). See Ben Wagner, 'Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems' (2019) 11(1) *Policy & Internet* 104; Fabio Massimo Zanzotto, 'Viewpoint: Human-in-the-loop Artificial Intelligence' (2019) 64 *Journal of Artificial Intelligence Research* 243; Jones, *supra* n. 60.

clarifies that the data controller should guarantee, as a minimal condition, the right of the data subject to require human intervention.[99]

This series of rights implements in the context of algorithmic decision-making the constitutional value of due process.[100] This concept too originated and developed with reference to the power of the state. The GDPR, however, horizontally claims the application of this constitutional safeguard in relation to private actors too. Article 22 deals with decisions that are so relevant for the individual that, although they are not pronounced in a courtroom, deserve the respect of a series of procedural principles, such as the adversarial principle and the right to appeal. Interestingly, however, the GDPR goes beyond a mere reiteration of these constitutional principles in the context of automated decision-making. Article 22(3) introduces a new principle, or better, a principle which is taken for granted in the analogue context: the judge of our actions must be human.[101] It cannot be a machine: there should be a human in the loop. As stressed by the European Commission in 1992, data processing can be useful to decision-making processes but 'human judgment must have its place'.[102]

Therefore, such a principle complements the general prohibition of automated decision-making established in Article 22(1). Both provisions ultimately aim to preserve human dignity. Human life is so diverse and unpredictable that it cannot be fully understood by a machine. The data subject has the right to require a human decision. In a certain sense, this principle is paradoxical: one prefers the fallacy of human judges rather than the efficiency of machines. There is no doubt: human beings will never be as efficient as machines; however, for this very reason, we will never be able to design a machine that understands fully our inefficiency and irrationality. Paradoxically, the human being, although inefficient, irrational, limited, unpredictable, is the only creature that can fully understand the nature of her peers.

It is worth observing that the principle of human in the loop is not a universal panacea. While enhancing due process safeguards, it can potentially disregard other interests requiring protection. First of all, it can affect the principle to conduct business or to perform a public task, due to additional human resources required. Secondly, and most importantly, the risks associated with biased decision-making are not mitigated per se by the presence of a human being.

However, these drawbacks are largely compensated by the utility of this principle as a guarantee against the non-accountable development of artificial intelligence technologies and the rise of private powers in the algorithmic society. The development of automated systems is based on the choice of programmers who, by setting the rules of technologies, transform human language in technical norms. They contribute to define transnational standards of

---

[99] GDPR, Recital 71.

[100] Several scholars underlined the need of guaranteeing minimal due process rights as an answer to the issue of asymmetry of power between individuals and data controllers in the context of automated decision-making. See Danielle Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington University Law Review* 1; Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 *Boston College Law Review* 93; Dannielle Citron, 'Technological Due Process' (2008) 85 *Washington University Law Review* 1249.

[101] See Article 2 of the *Loi informatique et liberté*. *Cf*. Bruno Romano, *Scienza giuridica senza giurista: Il nischilismo «perfetto»* (Giappichelli 2006); Rodotà, *supra* n. 57, 398.

[102] EU Commission, 'Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' COM(92) 422 final, 26-27.

automated systems whose processes escape from any form of scrutiny or control. The result of this situation affects not only the principle of transparency under data protection law, but even, more importantly, the principle of the rule of law. Legal norms are potentially replaced by technological standards. Within this framework, the principle of human-in-the-loop plays a crucial role not only as a due process guarantee, but also to protect democratic values.

5. Conclusion

Nowadays, data are fundamental assets for the digital economy, regardless of their nature, thanks to their capacity to generate value. Data can be regarded as simple pieces of information, but, if analysed for specific purposes and put together, can acquire huge importance. It is not a case that the GDPR ranks the concepts of privacy by design and by default among its principles, introducing an ex-ante approach in order to ensure that data protection is taken seriously into consideration, not only when running the business, but also in the previous phase of product design.[103] The ex-ante approach protects data subjects who cannot perceive the value of those small pieces of data, apparently meaningless information which acquire huge value through their processing.[104]

Artificial intelligence systems have contributed to introducing new ways to process large amounts of data, leading to positive effects for the entire society, including for fundamental freedoms, by increasing the capacity of individuals to exercise certain rights, such as freedom of business. However, this positive scenario firmly clashes with the troubling opacity of the present 'algocracy', the domain of inscrutable algorithms which characterizes contemporary societies.[105] Individuals are increasingly surrounded by ubiquitous systems that do not always ensure the possibility to understand and control their underlying technologies. Leaving algorithms without any safeguards would mean to open the way to a form of techno-authoritarianism, allowing the actors who govern these automated systems to arbitrarily determine the standard of protection of rights and freedoms at transnational level. The implications deriving from the implementation of automated technologies may have consequences not only on individuals' fundamental rights, such as the right of self-determination, freedom of expression and privacy, but also at a collective level.[106]

In this context, data protection law plays a crucial role in preventing disproportionate interferences with individuals' personal data. It emerges as a counterbalance against the potential marginalisation of weak societal actors, enabling data subjects to control how their personal data are processed. In this sense, we have seen how the GDPR plays a significant role from a constitutional law perspective. The new pan-European legislation, formally speaking,

---

[103] GDPR, Art. 25.

[104] Mireille Hildebrandt, 'Who Needs Stories if you can Get the Data? ISPs in the Era of Big Number Crunching' (2011) 24 *Philosophy & Technology* 371; Lita Van Wel and Lamber Royakkers, 'Ethical Issues in Web Data Mining' (2003) 6 *Ethics and Information Technology* 129.

[105] John Danaher, 'The Threat of Algocracy: Reality, Resistance and Accommodation' (2016) 29 *Philosophy & Technology* 245.

[106] Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 *Northwestern Journal of Technology and Intellectual Property* 239; Sue Newell and Marco Marabelli, 'Strategic Opportunities (and Challenges) of Algorithmic Decision-making: A Call for Action on the Long-term Societal Effects of "Datification' (2015) 24 *The Journal of Strategic Information Systems* 3.

does not have a constitutional character. Yet, it can be said to play a constitutional function, by translating and implementing core values of our constitutional tradition.

Specifically, our analysis of the constitutional message of the GDPR's framework on automated decision-making has highlighted how it is deeply rooted in the constitutional values of human dignity, due process and the rule of law. In this way, we have examined why the GDPR aims to restrict the possibility to resort to automated decision-making systems, notwithstanding their undoubted efficiency. We have explained how early data protection law in Europe, although emerging in response to an increased level of automation of data processing, did not include specific rules related to automated decision-making. Only the French data protection legislation, adopted in 1978, foresightedly restricted the possibility to resort to automatic decisional processes. In the paper, we have therefore argued that one can explain the decision of the European legislator to regulate automated decision-making, following the French impulse, because such an intervention appeared to be perfectly in line with the European constitutional tradition, which privileges the human dimension over profit and economic efficiency. If also the most important decisions related to our life were left in the hands of algorithms, our dignity as human beings, as well as the fundamental principles of the rule of law and due process, would be inexorably affected. By restricting the possibility to resort to automated decision-making, EU data protection law reinterprets and substantiates these constitutional values in light of the challenges of the digital society. In this way, the GDPR, as before it the Data Protection Directive, seeks to contrast the rise of an absolute techno-determinism in the algorithmic society. It expresses a new form of humanism – digital humanism, we could say – which advocates a vision where the data subject's free development, the protection of her digital identity, and, more broadly, her life outrank technology and economic efficiency.

The GDPR carries an old constitutional message, timely adapted to address the challenges of a society that risks to completely entrust human judgment in the hands of algorithms. Technology should not order society, but should be functional to ensure the evolution of mankind. Humanity is still not a fully explored invention. Only other human beings should take the responsibility to judge it, and affect its course of action.