UNIO - *EU Law Journal*. Vol. 4, No. 2, July 2018, pp 3-17.

School of Law – University of Minho

From the Internal Market to the citizenship of rights: the protection of personal data as the jus-fundamental identity question of our times

Alessandra Silveira & Pedro Froufe*

ABSTRACT: Bearing in mind the applicability of the General Data Protection Regulation as of May 25, 2018, the Authors use the teachings of computer engineers to explain the extent to which data (including personal data) is at the basis of the algorithmic revolution that is reconfiguring science, business, and politics. The Authors argue that, in the context of the European Union's assertion as a Union based on the rule of law, the importance and attention given to the effectiveness of the fundamental right to the protection of personal data is justified not only by the pressure of the technological times we are experiencing and by the gradual emergence of a homo digitalis. At the same time, the increasingly (outspokenly) political sense of deepening integration, as well as the priority placed on building European citizenship and reinforcing a dimension of extra-economic integration, all contribute to the development of a European fundamental rights culture. The referential paradigm of the Internal Market is, nowadays, a market where, first and foremost, citizens are moving and circulating, who are also circumstantially, economic agents and consumers. In this sense, the Authors seek to demonstrate why the protection of personal data has become the jus-fundamental identity issue of our times, basically so that the project of humanism does not become irrelevant.

KEYWORDS: protection of personal data – fundamental rights – learning algorithms – artificial intelligence – Digital Single Market.

* Professors at the School of Law of the University of Minho. Team members of the Jean Monnet Project "INTEROP - EU Digital Single Market as a political calling: interoperability as the way forward" funded by EACEA (Education, Culture and Audiovisual Executive Agency).

I. GDPR and the awakening of the sleeping princess: the question of data ownership

On May 25, 2018, the General Data Protection Regulation (GDPR)[1] became applicable – and since then, our email box has been filled with requests for consent to continue to receive newsletters and similar information. After all, the European citizen found himself/herself "owner" of his/her data on the Internet (which until now was doubtful, we hope it is no longer ...) and can no longer be pestered by undesirable emails. He/She realised that personal data is not only that which enables one to ascertain the identification of a person, but also that data which allows one reach this identification by association of concepts and contents, even if a direct reference to its holder is not made – as would be the case with the Internet Protocol (IP) address through which one accesses the Web or the registration of a vehicle. It was as if the European citizen, like the sleeping princess in the children's tale, had awakened from a deep sleep to discover that the value of the retribution he/she received, as well as the sound of his/her recorded voice to allow access to a bank account, or the registration of the purchases you make and the means of payment you use, but also your medical history, your debts and credits, your resume, etc. are all personal data, since being associated with a natural person, they allow you to identify it. Moreover, the European citizen has realised that such data is protected by EU law when subjected to an operation/treatment carried out with or without the use of automated means.

Still somewhat amazed, the European citizen now seeks to know why his/her data is so appealing (they had no idea!). That is, he/she seeks to understand the reason for the noise around rules that regulate not only the treatment of your personal data but also (soon) your privacy in the electronic communications area.[2] What is relevant in computerized personal data? To the point that the Court of Justice of the European Union (CJEU), since the judgment in *Lindqvist* - followed by *Scarlet*, *Digital Rights, Google*, *Shrems*, *Tele 2*[3], etc. – has fought a real battle, sometimes misunderstood, for the European legislator to adopt the GDPR. The reason is simple: the free movement of data is indispensable for the development of the so-called digital economy. Technological solutions that allow the smarter use of resources such as energy and water, the reduction of pesticides in agriculture, the competitiveness of manufacturing, as well as the reduction of road accidents, all depend on data processing.[4] The learning algorithms of Google, Facebook, Amazon, Apple, etc., learn from the data we give them. That is why it is said that data (including personal

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

[2] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 10 Jan. 2017, available on http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN.

[3] Judgment *Lindqvist*, 6 Nov. 2003, case C-101/01, ECLI:EU:C:2003:596; Judgment *Scarlet*, 24 Nov. 2011, case C-70/10, ECLI:EU:C:2011:771; Judgment *Digital Rights Ireland,* 8 April 2014, joint cases C-293/12 and C-594/12, ECLI:EU:C:2014:238; Judgment *Google*, 13 May 2014, case C-131/12, ECLI:EU:C:2014:317; Judgment *Schrems*, 6 Oct. 2015, case C- 362/14, ECLI:EU:C:2015:650; Judgment *Tele 2*, 21 Dec. 2016, joint cases C-203/15 and C-698/15, ECLI:EU:C:2016:970.

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the mid-term review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All [COM(2017) 228 final], Brussels, 10 May 2017, available on http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0228&from=PT.

data) are at the basis of the algorithmic revolution that is changing the world.

But private life is not (it should not be) a marketable product (especially against the will of the interested ones). We know that the privacy breach that increasingly accompanies the universal use of the Internet ensures the monitoring of every human gesture and idea. There is even vigilance for sale, by high profits, by the hand of a series of technological companies.[5] There must definitely be limits, since respect for privacy and protection of personal data is a prerequisite for stable, secure and competitive global trade flows.[6] That is why there is a need for a set of rules governing, in particular, liability, transparency and accountability in the digital age - and to translate the intrinsically European and humanistic universal values that characterize Europe's contribution to society. Norms that do not jeopardize the process of research, innovation, and the development of digitalisation[7], but shape the technological revolution so that the advantages of robotics and learning algorithms are widely shared, avoiding as much as possible their potential dangers.

Of course, we cannot go back to the pastoral age, especially since society is reorienting its interests, from a specific connectivity (computers, smart phones, etc.) to ubiquitous connectivity (articles for domestic use, industrial products, etc.). It is estimated that by 2020 about 6 billion household devices (televisions, refrigerators, washing machines, etc.) will be connected to the Internet in the European Union.[8] This poses a significant threat to privacy, due to the positioning of connected devices in traditionally protected and intimate spaces, with the ability to extract and transmit information about sensitive personal data.[9] An intensely connected market and society is more vulnerable to cyberattacks – which harms businesses of all sizes and compromises confidence in the digital economy and democratic institutions.

In any case, the premise to face it must always be the one where nothing is inevitable concerning the impact of digital technologies. Everything depends to a large extent on how citizens, businesses and public authorities decide to use them and how their regulatory framework is defined.[10] Moreover, as revealed by the *General Report* presented under the FIDE Congress 2018[11], the biggest problem of digital is perhaps the risk of overregulation in a highly variable and unpredictable sector. In the opinion of the European Data Protection Supervisor on the proposal for a Regulation on privacy and electronic communications (e-privacy Regulation), the complexity of the rules is criticized – which creates a potentially involuntary risk of protection gaps.[12]

---

[5] António Damásio, *A estranha ordem das coisas – a vida, os sentimentos e as culturas humanas*, Círculo de Leitores, 2017, Lisboa (*The strange order of thimgs – life, feeling and the making of cultures*).

[6] *Communication from the Commission on the mid-term review on the implementation of the Digital Single Market Strategy...*

[7] Digitisation is conceived here as "*the way in which many domains of social life are restructured around digital communication and media infrastructures or the way in which these media structure, shape, and influence the contemporary world*", see Corien Prins *et al.* (ed.), *Digital democracy in a globalized world* (UK/USA: Edward Elgar Publishing, 2017), 6.

[8] *Communication from the Commission on the mid-term review on the implementation of the Digital Single Market Strategy...*

[9] Resolution of the European Parliament with recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL), 16 Feb. 2017, available on http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//EN.

[10] *Communication from the Commission on the mid-term review on the implementation of the Digital Single Market Strategy...*

[11] *General Report - XXVIII FIDE Congress - Vol. I* (The internal market and the digital economy), ed. José Luís da Cruz Vilaça *et al* (Lisboa: Almedina, 2018).

[12] Opinion of the European Data Protection Supervisor on the Proposal for a Regulation on

In this text, we will try to demonstrate why the protection of personal data has become the fundamental identity issue of our times. The protection of personal data acquired legal-constitutional centrality not only because the Digital Single Market[13] has become a primary public interest to pursue – and the desired movement of people, goods, services, and capital implies an increase in the cross-border flow of data. Nor has it been only because the finalization of the Digital Single Market requires a stable legal environment that stimulates innovation, combats market fragmentation, and allows competitiveness on fair and balanced terms. This legal-constitutional role is also not just a matter of the certainly impressive estimate that the value of the data economy will rise to EUR 739 billion by 2020, corresponding to 4% of total EU GDP (i.e. more than twice the current value) and the number of professionals in the data sector will increase from 6 million in 2016 to more than 10 million by 2020.[14] Then why?

Well, the protection of personal data has become the fundamental identity issue of our times so that the project of humanism does not become irrelevant.

II. The Internal Market and the teleology of fundamental rights: the issue of citizenship

Homo digitalis[15] is increasingly more present in all of us. It surrounds us, it captures us. Our daily life is digitalising rapidly. It imposes on us a reorganization of the habitual pattern of life – or the digitisation of our life processes. We live, factually and considerably, a virtual existence…but very real! The real and the virtual merge in our normal life, the frontiers between these dimensions of our existence are blurring. Yet, this high-tech life of ours does not seem to be easily framed by law. Law has its own time – for now barely compatible with the speed of technologic developments. It is a time-deferred time – not a real time. Besides, in the face of new realities, it naturally hesitates in the pursuit of the value path (therefore, normative) to follow. We must give (its) time to law, without disregarding the obstacles and challenges of *homo digitalis*.

That is why, in the context of European integration, the importance of an effective uniform regime for the protection of personal data – able to debate technological advances and, at the same time, concretizing the fundamental right enshrined, directly and autonomously, in Article 8 of the Charter of Fundamental Rights of the European Union (CFREU) – must be observed and understood in the light of the meaning and objectives which have, in the recent past, been directed towards deepening integration.

As the goal of building a solid Internal Market was achieved, the "engine" of deepening integration began to gradually focus on building effective European citizenship. In a way, the Union, this kind of 'unidentified political object', according to the expression of Jacques Delors, no longer has prejudices regarding the assumption

---

Privacy and Electronic Communications (ePrivacy Regulation), Official Journal of the European Union (2017/C 234/03), available on http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017XX0720(01)&from=PT.

[13] A Digital Single Market Strategy for Europe [COM (2015) 192].

[14] *Communication from the Commission on the mid-term review on the implementation of the Digital Single Market Strategy...*

[15] The expression is used regularly as a synonym for literacy/knowledge and dependence on the new information and communication technologies (ICT) that have invaded our daily lives. See Natasha Saxberg, *Homo digitalis: How the human needs support digital behavior for people, organizations and societies* (Copenhagen: Dansk Psykologisk Forlag, 2015).

of its nature and its political yardstick (political Union). To a certain extent, the priority focus of the institutions is no longer the construction of the Internal Market (basically achieved), to concentrate on the citizen, regardless of his or her quality or "clothing" as an economic or consumer agent.

Freedom of movement was affirmed and guaranteed, initially through the case law of the CJEU, as a freedom of personal movement, irrespective of or in addition to freedom of movement. Social intervention, inherent in the affirmation of European citizenship (being still and above all a "citizenship of rights"), has become one of the concerns of the action of the Institutions. A certain return to some ordoliberal views was reaffirmed to mitigate the hardship of a construction focused solely on the market and economic competition: with the Lisbon reform, the Treaty on the European Union (TEU) expressly associates the Internal Market with a *"highly competitive social market economy, aiming at full employment and social progress"* – Article 3(3) TEU. We want, with this note, to affirm that today and in the context of the EU's affirmation as a Union based on the rule of law, the importance and attention given to the effectiveness of this fundamental right to the protection of personal data, is not justified only by the pressure of the technological times that we live in and by the progressive emergence of a *homo digitalis*. Upstream, the increasingly (more or less) political sense of deepening integration, the priority placed on the construction of European citizenship [Articles 20 and 21 of the Treaty on the Functioning of the European Union (TFEU)] and the reinforcement of an extra-economic integration dimension have favoured the development of a European culture of fundamental rights.

Unequivocally, the Internal Market and the application of economic freedoms initially served as a pretext for the jurisprudential construction of a dogmatic and European personalist culture of Fundamental Rights; but nowadays, more and more, the strengthening and deepening of the Internal Market (of economic integration) develop themselves according to a teleology of protection of fundamental rights, inseparable from the densification of European citizenship. We can reasonably say that the referential paradigm of the Internal Market is, nowadays, a market where, firstly, citizens are moving and circulating who are also, circumstantially, economic agents and consumers.

At the stage where the immediate objective of the European institutions' action was the realization and/or deepening, in certain areas of activity, of the Internal Market, it was essential to guarantee the free circulation of personal information. Increased cross-border movement of people, goods, capital, and the provision of services has led to an increase in the collection and circulation of personal data - and this increase in the flow of (and economic use) of data has made it necessary to establish, in the European area, an equivalent level of protection in all Member States. That is, the protection of data arose from the need to circulate personal information in the Internal Market in a secure condition for the data owners. This equivalent level of protection should result, as a minimum, from harmonized legislation. It is in this context that Directive 95/46/EC arises (i) imposing on Member States the obligation to adopt domestic legislation offering similar safeguards throughout the European area, and (ii) stipulating procedures and behaviour in relation to the flow of personal data to be transferred to third countries (which were classified by the European Commission in a differentiated way, depending on whether or not they offered an "adequate level of protection" with regard to personal data).

However, this phase of regulatory harmonization has proved to be inadequate in the face of the astonishing circulation of computerized data, with the introduction of a uniform application system in the Union, with a view to giving back control of personal data to its holders. Since January 2012, the Union institutions have

announced the need to undertake a revision/reform of the data protection legal regime then in force. The fragmentation of national systems resulting from the various transpositions of Directive 95/46 was one of the reasons for the need for reform, technically and from the point of view of legal certainty and uniformity. Therefore, it was always clear that the intention was to move forward with a Regulation (henceforth standardizing) repealing and replacing Directive 95/46. Moreover, this unifying trend has made its way in the digital field.[16]

The development of the technical information society and the advances in the digital economy have accelerated the need to develop a system capable of ensuring the effectiveness of the fundamental right to protection in the current circumstances and in the context of the technological/digital development in which we live, of personal data in (progressing) uniform terms by means of a Regulation. The Internal Market increasingly requires the circulation of data; and the increasingly sophisticated processing of such data urgently requires a standardized system for monitoring technical and digital behaviour in order to prevent abuse.

The GDPR is at the heart of a real reform of the regime for the protection of personal data, reflecting the (now added) concerns of the need to reconcile the necessary competitiveness and flexibility of European businesses with effective protection of fundamental rights. A conciliation that is difficult and necessarily dependent on casuistic circumstances – an equation that seeks to optimize a culture of citizenship rights (by reserving privacy and proficiency of each one's data), without impeding the growing deployment of the digital economy. To some extent, a real revolution, with a view to placing Europe at the forefront of technological development, economic growth and competitiveness provided by the wave of the digital economy - but at the same time, with the strong certainty that the European citizen, their dignity, and their fundamental rights are Europe's and integration's "watermark".

III. Learning algorithms as market intermediaries: the issue of unlimited choice

In a study dedicated to explaining why data (including personal data) is at the basis of the Machine-Learning Revolution – and to what extent artificial intelligence is reconfiguring science, business, and politics –, Portuguese scientist Pedro Domingos[17], Professor in the Department of Computer Science and Engineering at the University of Washington, explains that the problem that defines the digital age is the following: how do we find each other? This applies to both producers and consumers – who need to establish a connection before any transaction happens –, but also to anyone looking for a job or a romantic partner. Computers allowed the existence of the Internet – and the Internet created a flood of data and the problem of limitless choice. Now, machine learning uses this infinity of data to help solve the limitless choice problem. Netflix may have 100,000 DVD titles in stock, but if customers cannot find the ones they like, they will end up choosing the hits; so, Netflix uses a learning algorithm that identifies customer tastes and recommends DVDs. Simple as that, explains the Author.

Computer engineers explain that machine learning is a technology that builds itself. What differs machine learning from normal programming is that in the latter, it

[16] *General Report - XXVIII FIDE Congress - Vol. I* (The internal market and the digital economy)...

[17] Pedro Domingos, *A revolução do algoritmo mestre. Como a aprendizagem automática está a mudar o mundo* (Lisboa: Letras & Diálogos, 2017).

is necessary to explain to the computer what it has to do – step by step. If I want the computer to play chess or make a medical diagnosis I must explain to it how to play chess or how to make a diagnosis. But a learning algorithm can learn from the data it is given: if it is given a video of a car to be driven, of a road, and of what a person does at the wheel, the learning algorithm learns how to drive. Computers learn by simulating reasoning by analogy.[18] No wonder, then, that machine learning – this method of transforming data into knowledge – is revolutionizing science, business, and politics. With the development of e-commerce, automated customization has become mandatory. That is why the success or failure of a business – and ultimately an entire market or economy – increasingly depends on the quality of its learning algorithms. And these, in turn, depend on our data: the more data they have, the more they learn.

As learning algorithms become market intermediaries, more power is concentrated in them.[19] Hence, Google's algorithms determine what information is found, Amazons's algorithms determine what products to buy, Match.com's algorithms suggest the ideal match for those looking for it. The decisive step in choosing remains ours, but 99% of the selection is done by algorithms – explains Pedro Domingos. A new type of network effect emerges: whoever has the more customers – accumulates more data – obtains the best algorithmic models – and wins the most new customers…[20] Therefore, a virtuous circle (or a vicious circle, in the perspective of competition, for how to deal with digital monopoly).

In any case, machine learning is just a technology – and therefore what matters is what we decide to do with it and how to regulate its use. What data should we give to the computer so that it can achieve the model we want and that serves us? With whom should we share our data? More than a billion users have decided to share their personal data with Facebook – and Facebook's main use of the knowledge generated by such data is the targeting of ads. In return, the company provides the infrastructure for sharing – that is the bargain of using Facebook. As Facebook's learning algorithms learn more and better from users' data, the company gains more value from it. There are no free services on the Internet ... we are always paying in some way. Google knows about our searches, Amazon knows our literary preferences, Apple knows about the songs we download. These companies collect and sell information about us.[21]

There is no problem in marketing our data as long as it is done in a free and clear way. It is very easy to communicate with WhatsApp or Skype, especially for professional reasons, and it is difficult for us to relinquish such services. The problem is that some companies use our data for what is not of our interest - and until the GDPR was implemented, we had no way to stop it. However, most people are unaware of the amount of data they collect on their daily lives - and the potential costs and benefits involved. In the meantime, big companies act without transparency.

All this is part of a business model through which Internet users pay with their personal data for a service - with no (seemingly) damaging consequences until the Russians came to use fake news as a military strategy. In the case of a business, the solution would be simple: if Facebook and its counterparts exercise a digital monopoly on which there is no taxation, it is important to focus European taxation on digital platforms of this nature, by paying taxes for the targeted advertising

[18] Pedro Domingos, *A revolução do algoritmo mestre*...
[19] *Ibidem*.
[20] *Ibidem*.
[21] *Ibidem*.

business. Moreover, to hold companies accountable for the irregularities committed from the scope of the business they offer to those in the European Union. The GDPR imposes fines of up to EUR 20 000 000 or up to 4% of the company's annual turnover (whichever is higher) in case of breach of its provisions [Article 83 (5)]. However, it is important to know how the European and national authorities will now use the new tools that the GDPR gives them.

It is, therefore, urgent to discuss such questions without reservations. It is important to make people aware of what they want to share (and how and where) and what they do not want to share because learning algorithms increasingly decide who gets credit, who buys what, who gets what job, who gets what increase, what actions go up and down, how much insurance costs, where the police officers are, who has romantic encounters and with whom, etc. ...[22]

For this reason, the Portuguese MEP João Ferreira recently questioned the European Commission about the measures to be taken to face the so-called "algorithmic discrimination" (based on sex, age, ethnic origin, sexual orientation, etc.) caused by risk management algorithms. In other words, what measures are being considered to extend existing provisions for certain sectors (e.g. granting of bank credit), ensuring a more global scope? The GDPR extends the right to object (Article 21) and non-subjection to individual automated decisions (Article 22), including definition of profiles. That is, the holder has the right not to be subject to any decision taken solely based on the automated processing of his data (objecting to profiling, in order to assess and typify individuals on the basis of their data) or significantly affect it. This is because there must be i) human intervention on the part of the controller, and ii) a contradictory statement to expose the owner's arguments and challenge the decision.

But perhaps, the question is even deeper: how do we prevent learning algorithms from perpetuating the discrimination underlying the data from which they learn and develop? The scandal involving Facebook and Cambridge Analytica (a private company for data analysis and strategic communication) raises, among others, the problem of regulating learning algorithms. The problem lies, above all, in the fact that there is no necessary connection between intelligence and free will. Unlike human beings, algorithms do not have a will of their own, they serve the goals that are set for them.[23] Though spectacular, artificial intelligence bears little resemblance to the mental processes of humans – as the Portuguese neuroscientist António Damásio, Professor at the University of Southern California, brilliantly explains.[24] To this extent, not all impacts of artificial intelligence are easily regulated or translated into legislation[25] – and so traditional regulation might not work.

The example of fake news is elucidating. Facebook's algorithms aim to maximize the users' involvement – they intend for people to read fake news because that is how they can show them more ads. It does not matter to the algorithm whether the news is true or false, good or bad. Moreover, since fake news is the most scandalous, it tends to be the one that attracts the attention of Internet users. Ultimately, learning algorithms are stupid – as Pedro Domingos explains – because they lack, at least for

[22] *Ibidem*.

[23] *Ibidem*.

[24] António Damásio, *A estranha ordem das coisas – a vida, os sentimentos e as culturas humanas*...

[25] On this matter, see European Parliament, Scientific Foresight study "*Ethical Aspects of Cyber-Physical Systems*", Science and Technology Options Assessment Panel (STOA), 2016, available on http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2016)563501.

now, common sense and ethics, which are human characteristics, as well as empathy and creativity.[26]

In a recent study, the European Union Agency for Fundamental Rights sought to explain how algorithmic discrimination may occur, suggesting possible solutions to move towards fundamental rights compliance in this field. The study gives an account of the following examples: *i*) checking the quality of data as it remains a challenge to assess the quality of all data collected and used for building algorithms given the amount of data generated and used; *ii*) promoting transparency, opening up for scrutiny how algorithms were built, allowing others to detect, and where necessary rectify, any erroneous applications; *iii*) conducting fundamental rights impact assessments (including the assessment of the potential for discrimination in relation to different grounds) in order to identify potential biases and abuses in the application of and output from algorithms; and *iv*) making sure that the way the algorithm was built and operates may be *meaningfully* explained – most notably, which data was used to create the algorithm.[27]

Therefore, the GDPR does not allow lawyers to rest with the digital and technological revolution. The complex systems of artificial intelligence that are being forged are not just machines, they learn to recognize patterns and to adopt strategies that are beyond human comprehension. In addition, it may be humans themselves to give them control voluntarily, because they have great facility to take orders and be dazzled by what they do not know.[28] Here, the lessons of the young philosopher Étienne de la Boétie on the subject of voluntary servitude are relevant.[29] The lessons of the young philosopher about voluntary servitude and the reasons for which we abdicate our ability to decide are still valid here - something not only explained by the use of force. To capture this "something more" that explains the domination, Étienne de la Boétie already concluded, in the middle of the 16th century, that those who give up freedom gain bondage - which, moreover, can be a more comfortable place than freedom. What supports this delivery, according to Étienne de la Boétie? The fear of freedom - explains the Brazilian historian Leandro Karnal.[30] For, as we well know, it is easier and more convenient to be a subject than to be a citizen.

It was for no other reason that the European Parliament called on the European Commission, on the basis of Article 114 TFEU, to present a legislative proposal on legal issues related to the development and use of robotics and predictable artificial intelligence for the next 10 to 15 years - a proposal that contemplates the hypothesis of recognition of electronic people, in addition to the usual natural and legal persons.[31] In other words, to create a specific legal status for robots, so that at least the most sophisticated autonomous robots will have the status of electronic people responsible for remedying any damages they may cause – and eventually apply the electronic personality to cases in which that robots make autonomous decisions or interact in any way with third parties independently. At the request of the European Parliament, the European Commission adopted the Communication "*Artificial*

[26] Pedro Domingos, *A revolução do algoritmo mestre*...

[27] European Union Agency for Fundamental Rights (FRA), *#BigData: discrimination in data-supported decision making*, available on http://fra.europa.eu/en/publication/2018/big-data-discrimination.

[28] Pedro Domingos, *A revolução do algoritmo mestre*...

[29] Étienne de la Boétie, *Discurso da servidão voluntária* (São Paulo: Editora Brasiliense, 1982).

[30] Leandro Karnal, *O medo à liberdade e a servidão voluntária* (Café Filosófico), available on https://www.youtube.com/watch?v=zR8QzE_goCs.

[31] Resolution of the European Parliament with recommendations to the Commission on Civil Law Rules on Robotics...

Intelligence for Europe" in April 2018 – and foresees by the end of this year the adoption of a coordinated plan in that domain, under the principle that "*new technologies are based on values*".[32] Herein lies the idea that the development of robotics, artificial intelligence, and digitization (in a broad sense) requires that all those involved in the development and commercialization of such applications assume legal responsibility for the quality of the technology they produce at all stages of the process. That is, sustainable technologies – or a fairly secure, equitable, open digital environment.

IV. Data processing and decision making: the issue of democracy

Some time ago, the most vigilant jus-publicists realized that power was de-territorialised. As Gustavo Zagrabelsky explains, political and constitutional power is no longer exercised in the same way, because power does not have a territorial framework (or only partially), configuring what has been called "de-territorisation of power". Faced with this process, there is a growing gap between the free expression of political preferences and the real capacity of this expression to have repercussions on the decision-making processes that affect the daily life of voters. The right to vote expressed in a given electoral district ceases to be effective because the representatives elected in this way have no influence over the decisions that have been made in such circumscription.[33] In this context, governments change but policies do not. The margin for change is greatly reduced because the structures of the State are aging, thought of for another time, and unable to manage transnational dynamics they do not control.[34]

This mismatch translates into an unprecedented divorce between power and politics, as Zygmunt Bauman explained: power understood here as the ability to carry things out and politics perceived as the ability to decide what things should be carried out. This produces the effect of a national political system reduced to the management of routine administration and a system of global power without political representation and without any control. Finances, investment capital, the circulation of goods and capital, the labour market, etc., are beyond the responsibility and reach of the only political agencies still available to fulfil the task of regulation and supervision - the States. The European Union was the only more or less successful (because incomplete) attempt to regulate global flows and mitigate their effects. Thus, under conditions of global and digital interdependence, more important than the answer to the question "What to do?" would be the answer to the question: "Who is going to do it?"[35]

And here we go back to the data. Among the controversial statements of Yuval Harari in *Homo Deus*, one stands: as data-processing conditions change in the 21st century, democracy might decline or disappear.[36] Trying to decipher where power went in the digital age, the Author explains that as both the volume and speed of

[32] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions "Artificial Intelligence for Europe", Brussels, 25 April 2018, COM(2018) 237 final, p. 4, available on https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe.

[33] Paulo Castro Rangel, *O estado do Estado. Ensaios de política constitucional sobre justiça e democracia* (Alfragide: Dom Quixote, 2009).

[34] Gustavo Zagrebelsky, *Il diritto mite* (Torino: Einaudi, 1992).

[35] Zygmunt Bauman and Carlo Bordoni, *Estado de crise* (Lisboa: Relógio D'Água Editores, 2016).

[36] Yuval Noah Harari, *Homo Deus: história breve do amanhã* (Amadora: Elsinore, 2017).

data increase, respectable institutions such as the electoral system, political parties and Parliaments might become obsolete because they are unable to process data with the necessary efficiency. These institutions evolved in a time when politics was advancing faster than technology and were able to regulate and control its course. According to Harari, democracy and free market gained the upper hand because, under the unique conditions of the late 20th century, they were able to improve the global data-processing system through distributed processing methods rather than centralised processing methods. However, in the 21st century, traditional political structures cannot process data fast enough to produce meaningful visions of the future.

Hence, voters sense that democratic mechanisms no longer empower them – power is shifting away from them and they don't know where it has gone. In the UK, voters sense that power has shifted to the EU and they vote for Brexit. In the US, voters sense that power is monopolised by the "system" and they vote for Trump. They are mistaken in both cases, Harari explains, because power will not return to ordinary voters. But this does not entail the return to dictatorships identical to those of the 20th century, as authoritarian regimes are equally overwhelmed with the speed and volume of dataflow. Democracies and dictatorships are similarly overpowered and the "art of governing" has become the mere management of current affairs.

As power gaps do not last long, it is important to know who will build and control the new (political?) structures that will replace the traditional ones.[37] Perhaps a new, more efficient, omniscient, and omnipotent data-processing system, a kind of Internet-of-All-Things?[38] It's true that Google is quicker to detect an epidemic than traditional health organizations, but only if we allow its full access to the information we generate. Free-flowing data can also reduce pollution and waste by rationalising transport systems. It may allow for an intelligent car-sharing system, controlled by learning algorithms, that would always know where we are and where we want to go according to our daily habits.[39] Provided, however, we increasingly give up our privacy, autonomy, individuality.

But what harm or risk is there in this? – would ask our European citizen, still getting used to the GDPR, like a newly awakened princess. If not properly regulated, this civilizing choice entails the loss of what is most genuine in mankind, as human experiences would be reduced to data patterns. We believed that the experiences took place within us and that was where we sought the reason for everything that happened to us. But, when we connect our experience with the great dataflow and let algorithms discover the meaning of what is happening to us[40], we cease to make free choices based on rational judgments and lose human dignity. "Value" no longer lies in everyday experiences, but in turning these experiences into free-flowing data.

And that is why, increasingly, the intimate discourse exposed on the Internet as a shared political fact no longer needs to correspond to the truth to succeed, if it is accepted as close, possible, credible - that is, something that could happen - me or my neighbour. What results in the Internet is shared space, the projection of close, intimate perception and here, it is not so much what is said, but what people hear[41]. Some of the disinformation that runs on the Internet - the most sophisticated and fraudulent - has the power to shape the way people see the world because it meets what

[37] Yuval Noah Harari, *Homo Deus: história breve do amanhã…*

[38] *Ibidem.*

[39] *Ibidem.*

[40] *Ibidem.*

[41] On that point, see Yanko Moyano Diaz, "Understanding political beliefs: advantages and conditions of a culturalist notion of event", *UNIO – EU Law Journal*, vol. 4, nº. 1 (2018).

they want to hear, legitimizing their prejudices. The mechanism for reporting false news (on Facebook, for example) is not enough to change the user' perception.[42] That is why it has become increasingly difficult in the digital age to convince citizens that they are wrong.[43] If social media outlets are today the gateway to content, should they not be subject to the same editorial rules and certification of regulated media contents in order to combat disinformation?[44]

Overall, what is the use of democratic elections if learning algorithms anticipate who we will vote on?[45] The scandal involving Facebook and Cambridge Analytica reveals the extent to which it is possible, in democracy, to promote manipulation of the electorate by reliance on illegitimately obtained data (87 million Internet users had their data negotiated, unaware of the use of electoral manipulation). As we know, from the collection of information of 300,000 Internet users (through an inquiry/game), Facebook allowed the misappropriation of personal data of millions of people. In the United Kingdom, as far as we know, 1.1 million citizens have been targeted. If the difference between Remain and Exit was 1.3 million votes, it is legitimate to assume that the manipulation carried out may have been decisive in the results of the British referendum.

It is not a given, therefore, that a technological revolution leads to the effective empowerment of citizens and the perfection of democratic institutions. Citizens can be increasingly marginalized or manipulated in decision-making processes. This is not to weaken efforts to develop a digital democracy[46] – whose concept implies the use of electronic means of communication to empower and broaden the action of citizens and (tendentially) control of government and public institutions[47]. The problem is that this demands a change in civic culture - and this is the most difficult to change in politics. Hence, it is said that digital democracy is a cultural change. Digital began as a revolution for industry 4.0 - and then for commerce, tourism, etc. – but will it be for politics as well? Here, the time lag does not help, since digital causes expectations for the immediate, and citizens do not perceive the slow (proceduralised) response of democratic institutions to the rule of law, which leads to growing discontent.[48]

In theory, through the Internet, it seems possible to create a global public sphere that allows political dialogue between citizens and their concerns beyond artificial boundaries. The question is how to optimize the potential of the Internet to ensure democratic legitimacy based on the value of the rule of law[49] – this is the great challenge facing the Western legal-political culture in defence of its most recognized and precious heritage. The rule of law resumes today in a global scenario (marked by fragmentation, financialization, digitisation) that is not properly favourable to it. Positioning for the

---

[42] Dora Santos Silva *et al* (coord.), Enquadramento dos temas para a conferência *Democracia 4.0 – O futuro da democracia na era digital*, Session IV: A vertigem da desinformação, Representação da Comissão Europeia em Portugal, Reitoria da Universidade Nova de Lisboa, 8 May 2018.

[43] Yanko Moyano Diaz, *Understanding political beliefs*…

[44] Dora Santos Silva *et al.* (coord.), *Enquadramento dos temas para a conferência Democracia 4.0 – O futuro da democracia na era digital*...

[45] Yuval Noah Harari, *Homo Deus: história breve do amanhã*...

[46] See Corien Prins *et al.* (ed.), *Digital democracy in a globalized world*...

[47] Marco Lisi (coord.), *Enquadramento dos temas para a conferência Democracia 4.0 – O futuro da democracia na era digital*, Session II: A nova vaga da democracia digital, Representação da Comissão Europeia em Portugal, Reitoria da Universidade Nova de Lisboa, 8 May 2018.

[48] This idea was proposed by His Excellency the President of the Portuguese Republic, Marcelo Rebelo de Sousa, during the closing session of the conference *Democracia 4.0 – O futuro da democracia na era digital*...

[49] Ingolf Pernice, "E-democracy, the global citizen and multilevel constitutionalism", *Digital democracy in a globalized world*...

rule of law means that political institutions - or that power, wherever they now reside – strictly aim to guarantee the fundamental rights of individuals.[50]

In the ideal world, digital democracy could implement techniques to increase the transparency of political processes, encourage direct involvement and citizen participation, as well as improve the quality of information and opinions, by opening new spaces for communication and deliberation. In this sense, the digital revolution could transform democratic representation by changing the spaces and times of political action.[51] Digital tools could enable other ways of involving citizens in the life of their street, city, or country. However, the extent to which public entities are genuinely interested in increasing and improving the level of civic participation and whether citizens are genuinely interested in actively participating in democratic decision-making processes that affect their daily lives, remains to be seen.[52]

Digital can effectively revolutionize democracy, but it will no longer be the "physical" democracy we know. We cannot anticipate whether it will be better or worse, just different. This implies a civilizational option for the wide availability of data – which again confronts us with the regulatory challenge. At the "Democracy 4.0" conference organised in Lisbon by the European Commission Representation in Portugal, European Commissioner Carlos Moedas (responsible for Research, Science, and Innovation) showed great enthusiasm for blockchain technology applied to democracy because it would prevent intermediation (State, banking, etc.) and avoid upstream inequality by spreading recognition. If a dictator wanted to nationalize land in a given country, as exemplified by the Commissioner, he/she would have to erase property registration on millions of computers that recognized it - which would be impossible. At a particularly difficult time in European integration, permanently provoked by nationalist and xenophobic populism and its manifestations of collective bestiality, it may not be a bad idea ...

V. Protection of personal data and universality: the jus-fundamental identity issue

Since May 25, 2018, the GDPR has been the subject of much criticism - especially the one according to which the consent we are granting would be fallacious, since it only deceives internet users in the sense that they would be more protected. The complexity of the GDPR and its applicability to non-European companies operating in the Union, especially US companies, is also criticized. Posts claiming that few companies would be fully complying with it, including about 60% of technology companies, circulate online. That is, no one would still be ready for the GDPR. It is anticipated that regulators would initially be more lenient towards business as long as they do not gauge how GDPR really works.[53]

Firstly, it should be remembered (that is the purpose of this text) that the GDPR fulfils the essential dimensions of a fundamental right laid down in Article 8 CFREU which applies universally to those within the Union. Only from this

[50] Danilo Zolo, "Teoria e crítica do Estado de direito", in *O Estado de direito – história, teoria, crítica*, coord. Pietro Costa and Danilo Zolo (São Paulo: Martins Fontes, 2006).

[51] Marco Lisi, *Enquadramento dos temas para a conferência Democracia 4.0 – O futuro da democracia na era digital*...

[52] Ana Neves *et al* (coords.), Enquadramento dos temas para a conferência *Democracia 4.0 – O futuro da democracia na era digital*, Session III: Democracia participativa – criar pontes, defender interesses e protestar, Representação da Comissão Europeia em Portugal, Reitoria da Universidade Nova de Lisboa, 8 May 2018.

[53] Sarah Jeong, No one's ready for GDPR, in *The Verge*, 22 May 2018, https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu.

fundamental point of view can the GDPR be fully understood: *"Everyone has the right to the protection of personal data concerning him / her"* (highlighted). This means all persons who are in the territory of the Union (and not only the residents) are holders of that fundamental right by virtue of the principle of universality. In good time, the European legislator has "corrected the navigation" by amending the wording of the GDPR in this sense.[54] Thus, there is no denying that the GDPR strengthens and broadens the rights of personal data holders - and it does so from conception (proactive approach to ensure protection throughout the development process of a new product) and by (ensuring that only the necessary amount of personal data will be collected, used and maintained) introducing new transparency requirements.

The territorial scope of the GDPR is primarily related to the location of the data controller or subcontractor's establishment - if it is in the Union, the treatment is subject to the GDPR regardless of whether the processing takes place within or outside the Union The establishment presupposes the effective exercise of an activity based on a stable installation, and the legal form of such establishment is not relevant for that purpose (branch, office, etc.). But even if the establishment is located outside the Union, the GDPR will apply whenever the data subject is in the Union and the treatment is related to i) the supply of goods and services to the owner or; ii) the control of his/her behaviour.[55] In addition, the GDPR applies to the processing of personal data by an official established not in the Union, but in a place where the law of a Member State applies under public international law [Article 3(3)].

This must be the case because the Internet knows no territorial boundaries - and data protection only results if it is carried out in a universal way. It may seem exaggerated - but this is the Europe we want. As Angela Merkel would have said in her official greetings to the then President elected Donald Trump, we have here some principles that we like to respect. No one is obliged to offer goods and services to data subjects in the European Union - but if they intend to do so, benefiting from the European market, they have to adapt to their standards. This allows for a level playing field for all companies operating in the European market. The GDPR requires companies based outside the Union to apply the same rules as companies based in the Union if they offer goods and services related to personal data or monitor the behaviour of individuals within the Union.[56] This occurs when they are followed on the Internet for the potential use of profiling techniques, tending to make decisions about them or analysing/predicting their preferences and attitudes.

The GDPR, therefore, does not introduce an illusion. Silence and inactivity cease to be considered valid consents, and clear affirmative action is required to express consent to data processing. As we live in democratic societies, it is incumbent upon the data subject to attribute to that consent the relevance (or, on the contrary, lightness) that he/she deems compatible with the exercise of their fundamental rights. In any case, it cannot be denied that the GDPR establishes a comprehensive set of rules on personal data breaches. It also introduces an obligation to notify the supervisory

[54] Corrigendum to 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), published in the Official Journal of the European Union, L 127/2, 23 May 2018.

[55] Communication from the Commission to the European Parliament and the Council "Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018" [COM(2018) 43 final], Brussels, 24 Jan.2018, available on https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52018DC0043&qid=1517578296944&from=EN.

[56] *Ibidem.*

authority, within 72 hours at the latest, of where the breach of data is liable to entail a risk to individual rights and freedoms by requiring the holder of the data to be informed about of the violation. This greatly enhances protection compared to the previous regime, since only electronic communications service providers, essential service operators and digital service providers were obliged to report data breaches under the existing Directives.[57/58]

Of course, much remains to be done by public authorities - national and European. The Portuguese State, for example, has not yet acted to produce legislation to make the GDPR enforceable. Although the Regulation enjoys direct applicability, without the action of the national legislature, it is impaired, for example, the application of fines set forth in Article 83(5) GDPR, under penalty of violation of the sanctioning legality is well-nigh impossible without incorporation into the national laws of Member States. In addition, the GDPR provides for limitations on its application, with a view to ensuring judicial independence and judicial proceedings, as well as the enforcement of civil actions - and here, Member States enjoy some discretion in legislative action that should not be delayed. But the process has had some amateur outrages – moreover, already identified by an overwhelming opinion from the National Data Protection Commission on the legislative proposal.

In any case, as long as the Privacy Regulation for electronic communications does not enter into force, the effectiveness of the GDPR is, to some extent, undermined. In the opinion of the European Data Protection Supervisor on the proposal for an e-privacy Regulation, the European legislator is called upon to address the issue of the processing of electronic communications data by controllers other than providers of electronic communications services. The additional protections offered to the communications data would be unsuccessful if they could be easily circumvented by, for example, the transfer of data to third parties. It should also be ensured that the rules on privacy and electronic communications do not allow for a level of protection lower than that established in the GDPR. In this sense, consent must be genuine, offering free choice to users, in compliance with the GDPR. In addition, the new rules must also define solid requirements for privacy from design to default - as GDPR does.[59]

In view of the foregoing, we can conclude that the GDPR concretises the solution adopted by the CFREU when it empowered the right to protection of personal data (Article 8) regarding the right to privacy protection (Article 7). For European Union law, not all personal data is likely, by its nature, to hinder the privacy of the data subject – but it must also be protected. That is, not all data is of the same nature - and this justifies the autonomy conferred on the protection of personal data in relation to the protection of privacy in the Union's order. In this area, the CFREU goes a step further in relation to several Member States and in relation to the European Convention on Human Rights, in so far as it enshrines a fundamental right protecting data that do not have to be private/intimate. It is sufficient that they are personal. It is a civilizational advance that the GDPR now densifies - and that, by the impact of its territorial application, benefits (potentially) the rest of the world.

---

[57] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[58] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[59] *Opinion of the European Data Protection Supervisor on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)…*