

©2019 Centre of Studies in European Union Law  
School of Law – University of Minho



## Artificial intelligence, Digital Single Market and the proposal of a right to fair and reasonable inferences: a legal issue between ethics and techniques

Alexandre Veronese\*

Alessandra Silveira\*\*

Amanda Nunes Lopes Espiñeira Lemos\*\*\*

*ABSTRACT: The article discusses the ethical and technical consequences of Artificial intelligence (hereinafter, AI) applications and their usage of the European Union data protection legal framework to enable citizens to defend themselves against them. This goal is under the larger European Union Digital Single Market policy, which has concerns about how this subject correlates with personal data protection. The article has four sections. The first one introduces the main issue by describing the importance of AI applications in the contemporary world scenario. The second one describes some fundamental concepts about AI. The third section has an analysis of the ongoing policies for AI in the European Union and the Council of Europe proposal about ethics applicable to AI in the judicial systems. The fourth section is the conclusion, which debates the current legal mechanisms for citizens protection against fully automated decisions, based on European Union Law and in particular the General Data Protection Regulation. The conclusion will be that European Union Law is still under construction when it comes to providing effective protection to its citizens against automated inferences that are unfair or unreasonable.*

*KEYWORDS: Digital Single Market – General Data Protection Regulation – artificial intelligence – ethics.*

---

\* Professor of Social and Legal Theory at University of Brasília and coordinator of the Telecommunications Law Research Team of the University of Brasília (GETEL/UnB).

\*\* Professor at the School of Law of the University of Minho and Jean Monnet Chair holder in European Union Law.

\*\*\* Ph.D. candidate in Law at University of Brasília (UnB) and researcher of the Telecommunications Law Research Team of the University of Brasília (GETEL/UnB).

## I. Introduction: the fourth industrial revolution and the digital economic development<sup>1</sup>

Currently, one of the most exciting discussions in the field of digital technology field is the potential use of AI among various social and economic processes.<sup>2</sup> The concept of Fourth Industrial Revolution encompasses the debate and one can understand it as describing the expansion of automation.<sup>3</sup> In the legal domain, there are several researches on the subject and the term “artificial intelligence” is been heard more often, not only on the specialized mass media, but also in prospective studies by governments.<sup>4</sup> The International Data Corporation (IDC), a consulting firm that specializes in information technology in the United States, estimates that the global expenditures on cognitive systems and AI will annually reach around US\$ 78 billion by 2020.<sup>5</sup> This article contributes to this debate by offering an analysis of the European Union’s policies on the subject, as well as by highlighting that the issues about AI have a direct relation to the protection of personal data.

The Fourth Industrial Revolution draws its power from the automation of production processes. However, the current stage of automation has a new quality: the ability to learn from programs to improve their own performance. The traditional automation processes and labor is widespread in both the mass industry production as in the offer of services. Several factories already deploy their products – cars, for example – with the intensive use of robotic labor. The same occurs in banking and other services. The main difference in the automation of the Fourth Industrial Revolution is the effort to create computer programs that are capable of self-learning. The AlphaGo program is a usual example.<sup>6</sup> This program won a row of games against a human competitor in that old Chinese board game. The developers created a training routine in which the computer program played many matches against itself. Thus, because of the many repetitions, it was possible to create an evolution of its playing skills by the means of an algorithmic model. Therefore, the developers of computer programs in the new paradigm of the Fourth Industrial Revolution are focusing their

<sup>1</sup> This article is a result from the research of the first two authors in the scope of cooperation between the Telecommunications Law Research Team of the University of Brasília (GETEL/UnB) and the Centre of Studies in European Union Law of the University of Minho (CEDU/UMinho). The research received grants from the Foundation for Research Support of the Brazilian Federal District (FAPDF) and from the Jean Monnet project “INTEROP - EU Digital Single Market as a political calling: interoperability as the way forward”. This article was published in Portuguese as a chapter in the following book: Ana Frazão and Caitlin Mulholland (eds.), *Inteligência artificial: ética, regulação e responsabilidade* (São Paulo: Revista dos Tribunais / Thomson Reuters, 2019), 233-264. This article was translated by Sâmella Bonfim. It was presented during the Fourth France- Brazil Colloquium of Internet Law, held at the University of Brasília on 18th and 19th November of 2019. The authors also thank to FAPDF - Foundation for Research Support of the Brazilian Federal District, which granted resources for the translation.

<sup>2</sup> Klaus Schwab, *The Fourth Industrial Revolution* (Geneva: World Economic Forum, 2016); Klaus Schwab and Nicolas Davis, *Shaping the Fourth Industrial Revolution* (Geneva: World Economic Forum, 2018).

<sup>3</sup> Jon-Arild Johannessen, *Automation, innovation and economic crises: surviving the Fourth Industrial Revolution* (London: Routledge, 2018).

<sup>4</sup> Dietmar Harhoff, Stefan Heumann, Nicola Jentsch and Philippe Lorenz, *Outline for a German Strategy for Artificial Intelligence* (Berlin: Think Tank für die Gesellschaft im technologischen Wandel, July 2018); France, Le gouvernement, *Rapport de synthèse: France intelligence artificielle* (Paris: La Documentation Française, 2017), 36.

<sup>5</sup> International Data Corporation, *Worldwide Spending on Cognitive and Artificial Intelligence Systems Forecast to Reach \$77.6 Billion in 2022, According to New IDC Spending Guide* (Framingham, MA: IDC, 2018), <https://www.idc.com/getdoc.jsp?containerId=prUS44291818>.

<sup>6</sup> Deepmind, *AlphaGo* (London: DeepMind, 2019), <https://deepmind.com/research/alphago>.

building on machine learning to allow the improvement of its skills when it comes to performing specialized tasks. Those new computers have a set of skills that only apply to the restricted activities for which they were designed. The main point is that these programs would be specialized, not restricted. Soon, AlphaGo would be very effective for modeling and playing the game Go. By contrast, it would not have the same ability to model and play chess. This concept is relevant to understanding the automation of the Fourth Industrial Revolution. The past machines specialized tools. The future machines will be super specialized.

Why is this subject, which seemingly comes out from science fiction, begun to set the agenda of the economists and the governments all around the world? It does so because of one simple fact. The continuous increases in profit margins of productive processes are crucial for a good future of the economic situation in the countries. Using highly specialized systems for agricultural, industrial or services activities will be imperative in order to compete in the global market. Countries that are not investing in these new super-specialized machines will become more dependent on those that are doing it. Therefore, the diagnosis of the centrality of these investments is becoming hegemonic and the issue is under debate in national and in the international fora. That is why the European Commission and the European Parliament draw their policies from Articles 4(2)(a), 26, 27, 114, 115 of the Treaty on the Functioning of the European Union (TFEU).<sup>7</sup> They are developing specific policies for the Digital Single Market and, at the core of it; they are debating a plan for development in the AI sector.<sup>8</sup>

This paper will discuss how AI – in the narrow sense – can also cause negative consequences for citizens and not only economic benefits. The article illustrates the usage of the European Union legal framework for personal data protection – General Data Protection Regulation, or Regulation (EU) 2016/679,<sup>9</sup> henceforth GDPR – to enable citizens to defend themselves against some AI applications. The next section will expose some fundamental concepts about AI. The third section will describe the current documents on AI policies that are under debate in the European Union Digital Single Market. It will show how the subject correlates with the personal data protection issue. In the conclusion, the paper will describe the legal mechanisms for protecting citizens – based particularly on the GDPR – against fully automated decisions. The conclusion will be that the European Union Law is still in construction when it comes to protecting citizens against fully automated inferences that are unfair or unreasonable. Someone could consider that the Articles 21 and 22 of the GDPR (rights of opposition and explanation) would already provide enough protection. However, the definition of the limits of these legal provisions is, of course, an ongoing regulatory process, as Sandra Wachter warns:

Similar concerns [algorithmic discrimination] are reflected in the RGPD, especially in Article 21 (Right to Opposition) and Article 22 (Rules on Individual Automated

<sup>7</sup> Consolidated version of the Treaty on the Functioning of the European Union (EU). Brussels, Official Journal C 326, 26 October 2012, 1-390, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN>.

<sup>8</sup> Max Craglia et al., *Artificial intelligence: a European perspective* (Luxembourg: Publications Office, 2018), 140, <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/artificial-intelligence-european-perspective>.

<sup>9</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, concerning 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), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>.

Decisions, including Trimming). Article 21 introduces the right of holders of personal data to oppose data processing, including profiling, at any time. If the purpose of data processing is to conduct targeted marketing, the holder will have an absolute right of opposition. In all other cases, the processing of data must be interrupted unless the controller can show legitimate interests to override the interests of the data owners. Unfortunately, the regulatory framework does not provide a definition of what would be the compelling interests of the controllers, leaving them as well as the data subjects in an indeterminate legal situation. In addition to this legal uncertainty, the technical feasibility of ceasing data collection is also a challenge. The ways in which data controllers can manage one-off objections without ceasing all service provision remains unclear. As a result, users worried about their privacy – or with facilitated logging from Internet applications of things – may be faced with a binary “take it or leave it” choice. Article 22 introduces additional safeguards against automated decisions, including tillering, but only when the treatment is exclusively automated and has legal or significantly similar effects. The scope of applicability may be very limited, at least until two crucial concepts of Article 22 (1) are still unclear, which are “solely on the basis of automated processing” and “effect legal sphere or that significantly affects it in a similar way” (which produces legal effects concerning him or her or similarly significantly affects him or her).<sup>10</sup>

As a result, therefore, this diagnosis brings evidence about the limit of legal protection. A general problem pervades the legal debate in Cyberspace since its beginning. It also applies to the legal framework as explained by Sandra Wachter. The legal regulation tends to be more efficient in repressive mode (*ex post*) than in preventive mode (*ex ante*). Thus, the only way to achieve efficient preventative regulation when it comes to fully automated decisions refers to a conjoint use of ethical postulates and an increase of the prior technical auditing capability in such automated systems.

## II. Key concepts about AI

Before discussing the public policies proposed by the European Union, it is important to notice that many people use the term “artificial intelligence” usually without precise and accurate concepts. Meredith Broussard explains that there are two meanings for the same expression. In this way, she explains that there is a “general artificial intelligence” and a “narrow artificial intelligence”. The first concept comes from the common sense and from the fiction. It encompasses the kind of artificial intelligence that most people think we would like to have. The second concept refers to the computer programs currently available and in development. It embraces the AI that we have available nowadays.

Alan Turing’s paper “Computer Machinery and Intelligence”, published in 1950, states that there is no plausible meaning to the question: “Could a machine think?”<sup>11</sup> It would be too vague. He explains that the only way to satiate human understanding on the subject would be imagining how a machine could simulate a person. Then he proposes the well-known “Imitation Game”. At the same time, this paper brings other relevant information that needs further definition. In addition to the imitation game, he explains what would later be scientifically known as the Turing machine; or, the

<sup>10</sup> Sandra Wachter, “Normative challenges of identification in the Internet of things: privacy, profiling, discrimination, and the GDPR”, *Computer Law & Security Review*, No. 34 (2018): 436-449, 443.

<sup>11</sup> Alan M Turing, “Computer machinery and intelligence”, *Mind: a quarterly review in psychology and philosophy*, v. 59, No. 236 (1950): 433-460.

universal machine. By his diagnosis of the 1950, it would be possible, by the end of the century, to produce a machine that could win the imitation game. Consequently, the test is relevant for us to think that computer programmes – such as virtual assistants – are useful as good imitators of human beings. It is a pertinent test for measuring imitation from the point of view of natural language. In that way, it seeks to understand whether a computer program can mimic a human until we can induce a person to believe that the actual communication is happening with another human being, rather than with a computer program. A periodic international competition tests imitation programmes. Some computer programmes already have won this test since several programmes already managed to deceive human counterparts. One of them behaved like a schizophrenic person. Thus, when it received questions, it answered with the enunciation of its “neuroses”. Another programme answered questions like a thirteen-year-old foreigner. The Turing’s test turns out not to be an AI test.<sup>12</sup> It is an imitation test of human intelligence.

Then, the paper written by Alan Turing presents another interesting concept. It is the idea of a universal machine. This machine would be a digital computer capable of performing any calculations. The calculations are done by introducing data through a tape – which became, then, customary with tapes and punch cards – that would be read by the machine. The machine would only read “0” (zero) or “1” (one). After reading the zero or one, it could consult the list of commands – the computer programme – that would determine a subsequent command and then a new reading. We can understand the computation process like this:

Command 1 – reading space 1 – If it is “0”, go to space 25; if it is “1”, go to space 42.

Command 2 – reading space 25 – If it is “0”, go to space 89; if it is “1”, go to space 38.

Command 3 – reading space 42 – if it is “0”, go to space 110; if it is “1”, go to space 78.

These readings proceed indefinitely, until the end of the computational process. We should emphasize that the binary logic – if “yes”, do this; if “not”, do that – is the basis of all computational process. Therefore, the universal machine could execute any computational process. Everything would depend on the lists of commands we can provide for it. Nevertheless, computation is not an intelligence process, as we can observe. It is a logical process and it fits perfectly in dumb machines. There is nothing that can be said related to intelligence as a creative or as a self-created improvement. The machine will do exactly as programmed and will not better itself. Certainly, Alan Turing knew and showed that. The main point for the definition of intelligence, to the author, is the concept of learning. Therefore, for a machine to be considered intelligent, it must have the capacity to learn and, then, to evolve. It is valid to transcribing a part of the end of the paper:

The idea of a machine you learn may seem paradoxical to some readers. How would the machine’s operating rules change? They should fully describe how the machine will react whatever the future, whatever changes it may undergo. The rules would thus be impervious to chronological time. That’s true. The explanation for the paradox is that the rules to be changed in the learning process would be of a much less pretentious character, considering only their ephemeral validity.

<sup>12</sup> For an interesting overview of the literature on the Turing test: James Moor, *The Turing test: the elusive standard of artificial intelligence* (Berlin: Springer, 2003).



We may hope that machines will eventually compete with men in all purely intellectual fields. But which ones will be the most appropriate to start? Even this is a difficult decision. Many people may think that a very abstract activity, like chess games, would be the best.<sup>13</sup>

We can label several current and actual programs as AI machines. However, we had better exclude those that exist just in literature or in the cinema. Those are part of the “artificial intelligence in general”, as defined by Meredith Broussard. In the real science and technology field, “artificial intelligence in the narrow sense”, the computer programs that aim to produce predictions based on large volumes of data prevail. From a legal – and ethical – point of view, the discussion is about the control of these inferences and their transposition to the real application. Again, Meredith Broussard explains that humans create all the data and the entire computational process:

*“Although data can be generated in different ways, there is one thing that all examples have in common: all data is generated by people. This is true for all data. Ultimately, data is always reduced to people counting things numerically. If we do not think critically about it, we might imagine that the data springs into the world completely formed from the head of Zeus. We assume that, because there are data, they must be true. The first principle of this book: the data are socially constructed. Abandon any notion that data is produced by anything other than people”.*<sup>14</sup>

This concept is fully compatible to the Lawrence Lessig’s explanation about Cyberspace and Internet regulation based on the code. The main issue is the attribution of certain autonomy to processes carried out by automated systems. The automation generates action and interaction rules that furthermore demand high costs for their reformulation:

*“Thus, instead of thinking of the “enemy of freedom” in the abstract - as philosophers did - we should focus on a specific threat to the freedom that can exist at a specific time and place. And this is especially true when we think about freedom in cyberspace. I believe that cyberspace creates a new threat to freedom; absent from novelty because no theorist had conceived it before; but new in the sense of its innovative emergence. We are beginning to understand a powerful new regulator in cyberspace. Such a regulator could be a significant threat to a wide range of rights; and we still do not understand how best to control it. This regulator is what I call “code” - the instructions immersed in software or hardware that allow cyberspace to be what it is. This code is the “built environment” of social life in cyberspace. It is their “architecture”. And if, in the mid-nineteenth century, the threat to freedom were legal norms; and, at the beginning of the twentieth century, it was state power; and for much of the middle of the twentieth century it was the market; so my point is that we should tend to understand how at the beginning of the 21<sup>st</sup> century it is a new and different regulator - “code” - that should shape our present concern. However, the other relevant “regulators” should not be excluded. My argument does not mean that there is only a threat to freedom or that we should forget about the other traditional threats. Rather, it is that we must add yet another, increasingly relevant threat to the list”.*<sup>15</sup>

In 1997, Joel R. Reidenberg uses the term “*lex informatica*” to explain the creation and application of these rules in the digital environment when it comes to citizens and users.<sup>16</sup> The main point for him is that one can change these “*lex informatica*” rules.

<sup>13</sup> Alan M Turing, “Computer machinery and intelligence”, 458-460.

<sup>14</sup> Meredith Broussard, *Artificial unintelligence: how computers misunderstand the world* (Cambridge, MA: MIT Press, 2018), 18.

<sup>15</sup> Lawrence Lessig, *Code: version 2.0* (New York: Basic Book, 2006), 121.

<sup>16</sup> Joel R Reidenberg, “Lex informatica: the formulation of information policy rules through technology”, *Texas Law Review*, v. 76, No. 3, (1997): 553-593. The expression was also utilized by Aron Mefford, “Lex Informatica: Foundations of Law on the Internet”, *Indiana Journal of Global Legal Studies*, v. 5, No. 1, (1997): 211-237. And the creation of the expression was made by: Willem W. Van

However, this modification would require the expenditure of resources. Considering this allows us to place the AI regulation on another level, how could it be possible to modify or even suppress the application of AI technologies – always in the narrow sense – that could generate damaging diagnoses for citizens? The answer is close to the Manuel Castells' definition of power, to understand the network society:

*“I have gathered analytical elements necessary to address the question that is central to this book: where does power in global networking society radiate? To emphasize this, I must first differentiate four distinct forms of power: networking power; network power; networked power; and, network-making power. Networking power refers to the power of the actors and organizations included in the networks that constitute the core of the global network society about the groups or people that are not integrated into them. This form of power operates by inclusion/exclusion (...). In a network world, the ability to exercise control over others depends on two basic mechanisms: 1) the ability to build networks and to program/reprogram networks according to the objectives assigned to them (link and programming); and 2) the ability to connect different networks and ensure cooperation by sharing objectives and combining resources while avoiding competition from other networks by establishing strategic (switching)”*.<sup>17</sup>

Therefore, there are two ways of imagining the possible regulation of AI in the narrow sense. The first way refers to the regulation of the creation and the modification of computer programs. The second way refers to the regulation of part of the raw material used by computer programs: personal data protection. The first way of regulation is less likely to be effective. History is full of cases in which there was an attempt to limit human creativity. Therefore, banning and limiting the creation of computer programmes from previous and abstract bases would be almost impossible. Thus, the legal regulation of AI programming systems would tend to be innocuous. A derivation of the first control modality could be the attempt to regulate the use of these programmes or systems. In this way, if someone identifies a specific programme as a producer of abusive results, then some authority endowed with competence to do so could ban its use. Of course, this regulation will be very difficult to apply. The main difficulty is its kind of *ex post* regulation, which means that the ban will only be possible after the production and identification of damages. That is why the legal debate about the possible regulation of the production of computer programmes has been manifestly attached to the field of ethics.<sup>18</sup> Only an ethical discussion on the subject would allow effective *ex ante* regulation.

The second possible way of regulation refers to the protection of personal data in the processing systems. The attempt to build legal systems to protect citizens – in the European Union – dates back to the 1970s. France, for example, approved a national statute about this subject in 1978: Informatics and liberties act (*Loi de l'informatique et des libertés*).<sup>19</sup> This statute already provides legal protection of citizens against profiling, as well as other automated data processing. The debate in Europe about the subject, therefore, is much older. Therefore, the current legal provisions of the GDPR on the

---

Boom and J. H. M. Van Erp. (Sjef), “Electronic highways: on the road to liability - a case study of the Internet”, in *Emerging electronic highways: new challenges for politics and law*, eds. Victor Bekkers, Bert-Jaap Kopps and Sjaak Nouwt (The Hague: Kluwer, 1995).

<sup>17</sup> Manuel Castells, *The Communication Power* (Lisboa: Fundação Calouste Gulbenkian, 2013), 80-84.

<sup>18</sup> Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter and Luciano Floridi, “The ethics of algorithms: mapping the debate”, *Big Data & Society*, v. 3, No. 2 (july/december 2016): 1-21.

<sup>19</sup> France, Loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Statute No. 78-17 of 6 January 1978, about informatics, archives and liberties). *Journal Officiel de la République Française*, January 7, 1978, 227-231, [https://www.legifrance.gouv.fr/jo\\_pdf.do?id=JORFTEXT000000886460&pageCourante=00227](https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000886460&pageCourante=00227).

right of opposition and on the right of explanation are just the evolutionary landmarks of a long political and social process. In 1995, European Union Law prescribed in the Data Protection Directive,<sup>20</sup> the necessity to create national legal norms to protect citizens in the matter. In addition, in 2001 and before the GDPR, the Charter of Fundamental Rights of the European Union prescribed that the right to personal data protection – inserted in the Article 8.<sup>21</sup>

The two regulatory paths – ethics and data protection law – are not mutually exclusionary. Instead, they can converge and, thus, fortify an efficient legal regulation to control issues related to inferences based on statistical results, which is one of the greatest challenges of the combination between AI technologies and “Big Data”, among other possibilities. The next section will expose ongoing policies in the European Union for AI. The section will also highlight the attempts of regulation through ethical parameters.

### III. The European Union policies for artificial intelligence in the Digital Single Market, and the Council of Europe proposal

The term “artificial intelligence” describes software applications whether or not inscribed in hardware devices. The European Commission policy papers define the intelligence by the means of self-awareness and autonomy. Nevertheless, it describes systems that can gather external elements and then take different decision paths.<sup>22</sup> We can read the autonomy as indirectly dependent on the self-learning capability.<sup>23</sup> AI applications require regulation and discussion about the ethical elements that involve them, because they have a certain level of self-determination and have implications in many, and often sensitive, fields, such as human health, for example. It would be possible to think of several regulation modes, as expressed earlier. Nonetheless, the regulatory tendency has been to combine self-regulation tools (ethics, for example) with ways of coregulation (promotion and collaboration) and traditional regulation (supervision based on the protection of personal data). The regulatory panorama, however, is unclear. In the intent to move toward a normative field, the European Union has been producing several opportunities to debate and research the issue with the purpose of building policies – in the future – to regulate the subject. The current main objective is to search for a regulation scheme that does not harm innovation and creativity, which are inherent elements of this sector. The theme achieves special relevance in the context of the implementation of the GDPR. The Brazil-European Union Dialogues Report of May 2018 provides an overview of the theme in the European Union. The document seeks:

*“To identify trends and perspectives in the formulation of public policies regarding the current and future impacts of applications based on Artificial Intelligence (AI) technologies – mainly with regard to the regulation of algorithms, and their effects on guaranteeing the protection of fundamental*

<sup>20</sup> 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, *Official Journal L* 281, 23/11/1995 p. 0031 – 0050, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en>.

<sup>21</sup> European Union Charter of Fundamental Rights. Brussels, 18 december 2000, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>.

<sup>22</sup> European Commission, Communication from the Commission, Artificial Intelligence for Europe, COM(2018) 237 final, Brussels, 25.4.2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0237&from=PT>.

<sup>23</sup> Stuart Russel and Peter Norvig, *Artificial intelligence: a modern approach*. 2. ed. (Upper Saddle River, NJ: Prentice Hall, 1995).



*rights, correction of possible market failures and anti-competitive practices, as well as the establishment of mechanisms for scientific and technological stimulation in this field*".<sup>24</sup>

This section divides its subject in two parts. The first part deals with ongoing policies related to the European Union. The second part will describe a proposal being debated in the Council of Europe. It is always important to distinguish the Council of Europe from the European Union. The first is an international organization founded in 1949 by several European countries, which occurred right after the end of World War II. Currently, it has dozens of European countries in its composition, including the Russian Federation. This international organization has the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter, ECHR)<sup>25</sup> as its legal main norm and the European Court of Human Rights (ECtHR), which operates in Strasbourg, as its main judicial body. The European Union is a supranational entity, which brings together several Member States and has a governance structure that operates in an integrated way for the countries that comprise it. Thus, we can label the ECHR as international law in the narrow sense. EU Law is an integration legal framework that sets a very different and complex relation between the Member States and the European Union itself. The justification for exposing the Council of Europe's proposal for the subject comes from the fact that all the European Union Member States have also joined that international organization. Moreover, Article 6 (3) of the European Union Treaty prescribes that: "*the Union's law is compounded by fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and, as they result from the constitutional common traditions to the Member States, they shall constitute general principles*".<sup>26</sup>

#### ***a. The ongoing policies for artificial intelligence in the European Union***

This subsection exposes some of the current documents on the ongoing policies about AI that are under debate within the general Digital Single Market European Union working groups and policies. The first document is the European Parliament's Resolution of 16 February 2017. This document contains recommendations to the European Commission on civil law provisions about robotics (2015/2103, INL). It proposes definitions of "robot" and "artificial intelligence" that are flexible and do not create obstacles to innovation. The text considers that there has been an increase in investments in this area in the world – between 2010 and 2014 – and that:

*"(...) humanity lies at the threshold of an era in which increasingly sophisticated robots, bots, androids and other manifestations of artificial intelligence (AI) seem to be prepared to unleash a new industrial revolution, will leave no layer of society intact, it is extremely important for the legislator to weigh its implications and its legal and ethical effects without hindering innovation"*.<sup>27</sup>

This Resolution brings out the importance of ethical principles for the use of intelligence applications in face of the risks they could bring to "*the security, the health,*

<sup>24</sup> Paulo Novais and Pedro Miguel Freitas, *Inteligência artificial e regulação de algoritmos* (Brasília, Brussels: Governo Federal Brasileiro and European Commission, 2018), 16, <http://www.sectordialogues.org/publicacao/inteligencia-artificial-e-regulacao-de-algoritmos>.

<sup>25</sup> Council of Europe. European Convention on Human Rights. Strasbourg, 1950, [https://www.echr.coe.int/Documents/Convention\\_POR.pdf](https://www.echr.coe.int/Documents/Convention_POR.pdf).

<sup>26</sup> Treaty on European Union (Consolidated version 2016), 7 June 2016, C 202, 18, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016M/TXT&from=EN>.

<sup>27</sup> European Parliament, European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics [2015/2103(INL)], [http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051\\_EN.html](http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html).

*the freedom, the privacy, the integrity, the dignity, the self-determination, the non-discrimination, and the protection of personal data*". In that way, the document not only proposes a constant updating of the legal scope of the European Union for the subject, but it also advocates something that would become the Charter of 4 December 2018, of the European Commission for the Efficiency of Justice (ECEJ). The influence of the former document on the latter comes in the form of *"an annex to the resolution, a framework in the form of a consistent charter in a code of conduct for robotics engineers, in a code for ethics research committees when analyzing robotics protocols and model licenses for creators and users"*. The provisions of the Resolution also present the importance of AI for many fields, such as health, transport, education, employment and environmental impacts.

There is also a Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe, released in April 2018.<sup>28</sup> In the aforementioned document, the European Commission states that the concept of AI *"is applied to systems which present a smart behavior, analyzing their environment and how they make decisions, with a certain level of autonomy, to achieve specific objectives"*. It also emphasizes that AI is applicable in software, such as voice assistants, image analysis programs, facial recognition systems, as well as in physical devices (hardware) like advanced robots, autonomous automobiles, unmanned aerial vehicles, or Internet of Things applications. The document presents three pillars for AI, namely:

- (1) *Reinforce the European Union's technological and industrial capacity and the acceptance of artificial intelligence throughout the economy, both by the private sector and the public;*
- (2) *Prepare socioeconomic changes arising from artificial intelligence;*
- (3) *Ensure an appropriate ethical and legal framework based on the values of the Union and in line with the Charter of Fundamental Rights of the European Union.*

Among the series of proposals presented by the European Commission in the document, it emphasizes the importance of strengthening the Digital Single Market. In this context, the document advocates the development of uniform and adequate legal standards for future applications of AI. The objective is to ensure the possibility – by means of regulation – of the free movement of non-personal data within the European Union freedom area. In order to achieve this intent, legal norms are indicated, which will potentially strengthen online trust, such as the proposal for a regulation on respect for privacy and protection of personal data in electronic communications<sup>29</sup> and the Proposal for a Regulation on the "European Union Agency for Cybersecurity" and the certification of information and communication technologies cybersecurity.<sup>30</sup>

A few months after the presentation of this Communication, in December 2018, the European Commission published an Annex that outlines the Coordinated Plan

<sup>28</sup> European Commission, Communication from the Commission, Artificial Intelligence for Europe.

<sup>29</sup> European Commission, 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, Brussels, 10.1.2017, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=PT>.

<sup>30</sup> Directorate-General for Communications Networks, Content and Technology (European Commission), European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM/2017/0477 final/2 - 2017/0225, <https://publications.europa.eu/en/publication-detail/-/publication/0ae19c15-ae6f-11e7-837e-01aa75ed71a1/language-en>.

for Artificial Intelligence.<sup>31</sup> This Plan puts AI as an element that will contribute to the sustainability and viability of the industrial base of the European Union countries. The Plan highlights the potential of AI to improve services by: (1) increasing the quality and consistency of services provided; (2) improving the conception and implementation of policy measures; (3) enabling more efficient and targeted interventions; (4) enhancing the efficiency and effectiveness of public contracts; and (5) strengthening security, identity management, improving health services and employment. The document also points out that is expected that “*Europe becomes the region in the global leadership of the development and implementation of cutting-edge, ethical and secure artificial intelligence, promoting a human-centered approach in a global context*”. To this end, the Plan considers the necessity of investing a few million euros in technologies geared to AI between 2018 and 2020. The Plan emphasizes that the projection is not only about the need for investments of public funds, but also about the need to adopt partnerships with the private sector. The European Union’s usual role in similar issues has been to coordinate the economic and technological development efforts of the Member States. In this way, the Plan proposes joint actions not only from the Member States; it postulates the coordination of industries and academia on a common agenda for research and innovation in AI. Therefore, in addition to the investment directed to the industries, there is a forecast of educational and research programs, with scholarships and incentives, for the strengthening of excellent research centers in the field of AI by 2020. Matthias Schäfer presents the roles of each of these actors in the proposal to build the Fourth Industrial Revolution within the framework of the European Union:

*“EU policy for the fourth industrial revolution should focus on strengthening the capacity of Member States to improve the potential for innovation in the private sector rather than on the choice of winners and the creation of EU industry advocates. The private sector creates technologies that meet customers’ needs efficiently and effectively. The role of governments should be to support a wide range of technological applications in different sectors. Governments should be reluctant to support technology in which investments can be made more appropriately by companies. Removing all obstacles in the way of cooperation between government and the private sector would support this approach. Universities would play a crucial role. They would carry the fruits of pure science into applied science. They would also provide laboratories and workspaces to develop entrepreneurial skills and foster demand for new products, services and applications”*.<sup>32</sup>

The Plan also presents relevant information that the implementation of AI strategies at local level in the Member States would contribute to their growth. It states that by December 2018, France, Finland, Sweden, the United Kingdom and Germany would have already implemented AI oriented strategies. Some Member States, including Denmark, Luxembourg, the Netherlands, Ireland and Norway, would include actions related to AI in a wide national digitalization strategy. In addition, Austria, Belgium, the Czech Republic, Denmark, Estonia, Germany, Italy, Latvia, Poland, Portugal, Slovenia, Slovakia and Spain would be in the development phase of their national strategies.

<sup>31</sup> 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. Coordinated Plan on Artificial Intelligence, COM 2018 795 final, Brussels, 7.12.2018, <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-795-F1-EN-MAIN-PART-1.PDF>.

<sup>32</sup> Matthias Schäfer, “The fourth industrial revolution: how the EU can lead it”, *European View*, v. 17, No. 1, (2018): 5-12, 5, <https://journals.sagepub.com/doi/pdf/10.1177/1781685818762890>.

Besides the mentioned documents, the European Commission has set up an Artificial Intelligence High Level Expert Group (AIHLEG).<sup>33</sup> The Group's overall objective is to support the implementation of the European Union strategy for AI. This will include the elaboration of future recommendations on the development of related policies, as well as propositions on ethical and legal issues related to AI, including social and economic challenges.<sup>34</sup> These guidelines cover subjects such as equity, security, transparency, the future of work, democracy and, more broadly, the relationship between the dissemination of these technologies and the application of the Charter of Fundamental Rights of the European Union, including privacy, protection of personal data, dignity, consumer protection and non-discrimination.

Nevertheless, the European Union has other forums and groups. The European Group on Ethics in Science and New Technologies published a statement on March 2018 entitled "*Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*".<sup>35</sup> There is also a public forum, engaged in a broad and open discussion of all aspects about the development of AI and its impacts: the European Alliance of AI.<sup>36</sup> Alliance members can interact with experts from the Group of Experts AIHLEG. The various debates contribute directly to the elaboration of comprehensive policies to the European Union in this area.

Another worth mentioning issue is the creation of a common European data space since the "*current expansion of artificial intelligence is driven by the availability of large datasets combined with increases in processing capacity and connectivity*". This excerpt is contained in the aforementioned Communication of the European Commission about AI.<sup>37</sup> Based on it, it is possible to visualize the evident overlapping of policies in favor of AI with data protection. Thus, the debate of the topic of AI relates to the discussion on the application of the GDPR. This is because the European Union organizes its initiatives towards the Digital Single Market in an integrated way. In that sense, all the efforts of multiple instances of the European Union are engaged in drawing principles and converging guidelines. In this way, in the 537<sup>th</sup> European Economic and Social Committee of September 2018, an Opinion was stated about "*Artificial intelligence: anticipating its impact on work to ensure a fair transition*" (own-initiative opinion) (2018 / C 440/01). This Opinion contains recommendations that revolve around the strengthening of ethical principles in the elaboration of new technologies based on AI and their strengthening in the productive and labor environment, such as:

*"(...) recommends that engineers and intelligent machine builders be trained in the field of ethics in order to avoid the emergence of new forms of digital taylorism in which the human being is relegated to the execution of machine instructions. The dissemination of good practices and the partition of experience in this field should be promoted".*<sup>38</sup>

<sup>33</sup> "Digital Single Market policy: High-Level Expert Group on Artificial Intelligence", last modified July 3, 2019, <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>.

<sup>34</sup> High-Level Expert Group on Artificial Intelligence, *Draft ethics guidelines for trustworthy AI* (Brussels: European Commission, 2018), <https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai>.

<sup>35</sup> European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and "Autonomous" Systems* (Brussels: European Commission, 2018), [http://ec.europa.eu/research/ege/pdf/ege\\_ai\\_statement\\_2018.pdf](http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf).

<sup>36</sup> "Single Market policy: the European AI Alliance", last modified August 21, 2019, <https://ec.europa.eu/digital-single-market/en/european-ai-alliance>.

<sup>37</sup> European Commission, Coordinated Plan on Artificial Intelligence, COM 2018 795 final.

<sup>38</sup> Opinion of the European Economic and Social Committee on "Artificial intelligence: anticipating its impact on work to ensure a just transition" (own-initiative opinion), 2018/C440/01, OJ C 440, 6.12.2018,



The Opinion also addresses another topic of great relevance when it comes to AI and employment. The liability for damages:

*“The Industrial robots or service robots collaborate more and more with the human being. Artificial intelligence allows robots to “get out of their cages”, what can cause accidents. As such, the liability of autonomous systems if an accident occurs must be clearly established and the health and safety risks to which workers are susceptible must be covered. The European Commission is launching a reflection on these emerging risks within the chart of the Directive when it comes to the responsibility due to the products. This approach should be more ambitious with regard to safety at work”.*

Therefore, it is possible to see a synergy between specific policy themes – such as AI and the Internet of Things – and the debates that are occurring within the European Union about the protection of personal data. The same meeting of the European Economic and Social Committee, which produced the Opinion about AI, adopted another Opinion about *“Trust, privacy and safety for consumers and companies on Internet of Things”*.<sup>39</sup> Those courses of actions come in a comprehensive project. They reflect the necessary uniformity needed for data subjects in the Digital Single Market and its expansion in several strands. After that description of this set of actions in the context of the European Union, we should describe the proposal of the Council of Europe about AI in judicial systems.

### ***b. The Council of Europe proposal about ethics to the artificial intelligence in the judicial systems***

The proposal refers to the ethical principles related to the use of AI in judicial systems, published on 4 December 2018<sup>40</sup> and was adopted by the European Commission for the Efficiency of Justice (ECEJ), operating within the framework of the Council of Europe. The ECEJ brings together experts from the 47 Member States of the Council of Europe and tries to improve the quality and efficiency of European judicial systems as well as to strengthen the confidence of court users in such systems. The document that approves the proposal is the *“European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment”*. The Charter is directed towards the stakeholders – public or private –, who are responsible for designing or applying AI tools and services related to the processing of court rulings and judicial data (whether by machine learning or by any other method derived from data science). In addition, the Charter is addressed to those responsible for establishing a legal framework on the national level. It lists five principles: (i) principle of respect for fundamental rights; (ii) principle of non-discrimination; (iii) principle of quality and security; (iv) principle of transparency, impartiality and fairness; and, (v) under user control principle.

When it comes to processing judicial data and decisions, the judicial-related systems must use certified sources and data developed in multidisciplinary models, in a safe technological environment. Another concern about the use of AI is the necessary special care when processing directly or indirectly “sensitive” data. This data may include a wide range of elements. They might refer to a possible racial or ethnic origin, as well as socio-economic background, political opinions, religious or philosophical

<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:C:2018:440:FULL&from=EN>, 5-12.

<sup>39</sup> Opinion of the European Economic and Social Committee on “Artificial intelligence: anticipating its impact on work to ensure a just transition” (own-initiative opinion), 2018/C440/01.

<sup>40</sup> European Commission for the Efficiency of Justice (CEPEJ), European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment (Brussels: Council of Europe, 2019), <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

beliefs, trade union membership, genetic, biometric data or health-related data or data related to sexual aspects or sexual orientation. The Charter states that, when someone identifies potentially discriminatory data, some remedial measures must come into force to limit or, if it is possible, to counteract such risks and to raise awareness among the ones involved. The main objective is to create safeguards in order to avoid discrimination, in accordance with the guarantees to a fair trial.

After the principles, the Charter has four Appendices. The first – and largest – is entitled “In-depth study on the use of AI in judicial systems, notably AI applications processing judicial decisions and data”. Different European countries researchers author this appendix. It brings many examples of good and bad uses of AI in judicial systems. In brief, to the ECJ, the application of AI in the field of justice can contribute to improving the efficiency and quality of the public service. Nevertheless, these new technologies must be applied in a responsible manner, respecting fundamental rights, in particular those assured in the European Convention on Human Rights,<sup>41</sup> as well as the ones assured in the Convention 108+ (Convention for the protection of individuals with regard to the processing of personal data).<sup>42</sup> This initiative of the Council of Europe is an example on how it is possible to fulfil a desired correlation between human rights protection, personal data protection, and protection against new and potentially harmful technologies. AI remains at the crucible of all these protection policies and they can receive legal force from the Council of Europe’s ECtHR. As a matter of fact, that legal and institutional framework can be an example for other countries and regions.

#### **IV. Conclusion: the idea of the right to fair and reasonable inferences**

The increase in capacity of processing information– and its cost reduction – was a crucial step in the development of computer programmes capable of analyzing a very large amount of data. The cost reduction was useful for making technology more accessible for the automation of decision-making in courts. In the 1970s, when France passed the Informatics and liberties act (*Loi de l’informatique et des libertés*) into law, there were few devices capable of producing high-performance computing, which is a necessary condition for creating massive potential damages. Nowadays, the facts are entirely different. In the past, the production of information for further processing was very complicated. Nowadays, data gathering methods have also become more accessible. We can characterize Big Data by the use of a large volume of data, in great variety, through a high-speed data processing system. This data processing is capable of generating information that would not be intuitively available. It can also provide dense information to justify complex and risky decisions, such as granting a bank loan or hiring people to perform specialized services. The joining of Big Data with AI refers to the possibility of creating computer programs that can learn from errors that they make when performing data processing in order to provide useful information. The system will improve in their capacity to offer prodigious data processing.

<sup>41</sup> Council of Europe, European Convention on Human Rights, Strasbourg, 1950, [https://www.echr.coe.int/Documents/Convention\\_POR.pdf](https://www.echr.coe.int/Documents/Convention_POR.pdf).

<sup>42</sup> Convention 108+: Convention for the protection of individuals with regard to the processing of personal data. Strasbourg, Council of Europe, June 2018, 33, <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>.

This article demonstrates the attempt to construct legal frameworks – whether in the European Union, National Law or International Law – in order to provide protection for citizens against the result of fully automated decisions. The French statute, at some sense, foresaw the right of explanation and opposition of the GDPR under its 1<sup>st</sup> to 5<sup>th</sup> Articles.<sup>43</sup> Under European Union Law, the Directive 95/46/CE also provided protection provisions – the right of explanation and opposition – against automated decisions in its Articles 14 and 15. In addition, the Directive explains the special protective needs in its Recitals 15, 27 and 41. The GDPR overcame the Directive but it continues to list the rights of explanation and opposition in its Articles 21 and 22. It also mentions the issue in Recitals 15, 35 and 71. The GDPR also reinforces the need to comply the Conventions 108 and 108+ of the Council of Europe. Lastly, it reinforces Article 8 of the Charter of Fundamental Rights of the European Union, which provides the right of personal data protection.

One may think that the legal framework is complete. On the other hand, is it not? For Sandra Wachter and Brent Mittelstadt, researchers at the Oxford Internet Institute of Oxford University and at the Alan Turing Institute of the British Library, the answer would be negative. They postulate the need to construct a right to reasonable inferences.<sup>44</sup> The first step to analyze the subject would be to determine whether the inferences – results produced from possible data processing – could receive protection from the GDPR. They examine this subject through the point of view of an amalgamate array of rights: the right of access, the right of information, the right of rectification, the right of erasure, the right of opposition and the right of explanation. In the paper, they test the applicability of the GDPR provisions with regard to the interpretation of pragmatic cases judged by the Court of Justice of the European Union (Hereinafter, CJEU)<sup>45</sup> and by the ECtHR<sup>46</sup> as well as by the definition model of personal data,<sup>47</sup> produced by the Data Protection Working Party Article 29.<sup>48</sup>

Their conclusion is that there must be an expansion of the legal protection based on a jurisprudential innovation by the CJEU. At the end of the article, they expose five recommendations. The first one is to expand the concept of protection beyond personal data. They emphasize that personal data compound the right of privacy, which would include the right to identity, reputation, self-image and autonomy.<sup>49</sup> The second

<sup>43</sup> France, Loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 227-231.

<sup>44</sup> Sandra Wachter and Mittelstadt, "A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI", *Columbia Business Law Review* (2019).

<sup>45</sup> Court of Justice (Second Section), *Peter Nowak contra Data Protection Commissioner*, 20 december 2017, C-434/16, <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62016CJ0434>. Court of Justice (Third Section), *YS contra Minister voor Immigratie, Integratie en Asiel*, 17 july 2014, C-141/12 and C-372/12, <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CJ0141>. Court of Justice (Main Section), *Comissão Europeia contra The Bavarian Lager Co. Ltd.*, 29 june 2010, C-28/08 P, <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62008CJ0028>. The paper also appreciates other judgments; however, these are the paradigms we selected as the most relevant.

<sup>46</sup> Directorate General Human Rights and Rule of Law, *Case Law of the European Court of Human Rights concerning the protection of personal data* (Strasbourg: Council of Europe, june 2018), <https://rm.coe.int/t-pd-2018-15-case-law-on-data-protection-may2018-en/16808b2d36>.

<sup>47</sup> According to the report in question and with the authors: "the content, purpose and outcome of the data (treatment) must relate to an identifiable person, either directly or indirectly. *Ibidem*, p. 15-16.

<sup>48</sup> European Commission, *Article 29 Data Protection Working Party. Opinion 4/2007 on the Concept of Personal Data (01248/07/EN WP 136)* (Brussels, Belgium: Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, june 2007), [https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf).

<sup>49</sup> Sandra Wachter and Mittelstadt, "A right to reasonable inferences", 81.

recommendation would be that the protective means should – based on the GDPR – focus more on the process of analyzing the personal data than on the methods of collection. The GDPR system defines categories of personal data to set different levels of protection. However, the authors consider, taking into account the Opinion of the Article 29 Data Protection Working Party, that that should be a categorization of protection based on the objectives and impact of the data processing. The third recommendation seems to be a logical consequence of the second one. They state that there should be an evaluation of risks not only on personal data, which gains its definition from the direct relationship it has with the holder of that data. Alternatively, there should be an evaluation of the data processing in a wider range. According to the authors, profiling from databases made anonymous may also create risks for the data subjects in data processing. In a certain way, the authors affirm the extension of personal data protection to cases in which it would not be possible to identify the holders. It would be possible to describe the proposal as a protection of the diffuse rights regarding personal data, which at first may sound contradictory. The fourth recommendation would be to expand the technical protection of the data processing, requiring a prior analysis of potential data sources before proceeding with large-scale analyses. This suggestion intends to cover even new data sources, such as mouse movements on computer screens.<sup>50</sup> The GDPR has already provided previous risks evaluations (impacts assessments) in Articles 35 and 36. This suggestion relates to the procedural and substantive coherence that is determined by the GDPR in Articles 63 and 64. The national data protection authorities, in line with the European Data Protection Board, must carry out these tasks.

Finally, the last recommendation refers to the legal construction of the right to oppose unreasonable inferences. Their idea is to create a right from a legal interpretation of the other data protection rights already inscribed in the GDPR. However, the authors themselves are aware of the limits of this proposal:

*“The intention to recognize the ex-post right to challenge unreasonable inferences is not, however, a guarantee that the data controller should modify his inference or assessment from the claim of a holder of personal data. Rather, it aims to establish a dialogue between data controllers and incumbents in which the former share details and justifications for the proposed inferential treatment, which will be open to comments and questions by the latter, under the terms of Article 22 (3) of the RGPD. This will be positive for both parties, just as an accurate assessment is taking place in the interests of all.”*<sup>51</sup>

As Sandra Wachter and Brent Mittelstadt know the limits of protection in the cyberspace and in the Internet have always been related to a structural dilemma, diagnosed by the first researches who dealt on the subject: the legal protection is applicable *ex post*, whereas the technical rules – fixed by the programs and network architecture – are applicable *ex ante*. As indicated in the text, the concepts of Code (Lawrence Lessig) and *Lex Informatica* (Joel R. Reidenberg and others) are enough to highlight the problem. The solution exposed by these two authors consist of a construction of legal, economic, social or ethical mechanisms, which can influence the production of computer programs and standards tuned with a progressive paradigm in a matter of rights. The solution is, therefore, indirectly legal. However, it will be directly technical or ethical. Their long-time conclusion enlightens the importance

<sup>50</sup> Fast Company, “Facebook confirms it tracks your mouse movement on the screen”, 13 June 2018. <https://www.fastcompany.com/40584539/facebook-confirms-it-tracks-your-mouse-movements-on-the-screen>.

<sup>51</sup> Sandra Wachter and Mittelstadt, “A right to reasonable inferences”, 84-85.



of the fora – such as those created within the European Union – and the political decisions – such as the ones taken by the European Parliament and the Council of Europe. They are effective actions to consolidate an ethical paradigm and a positive influence in the establishment of technical rules tuned with respect of the rights of the citizens paradigm. Many years ago, François Ost and Michel van de Kerchove had already diagnosed the emergence of new legal sources that showed the emergence of a new type of legal system. The traditional concept of a legal system – hierarchical, linear and arborescent – no longer serves to understand the complex construction of the contemporary law:

*“The collapse of the network pyramid is an evolution that is accompanied by two other major transformations of the juridical-political universe: the transition from regulation to regulation and the potential escalation of the governance in place of government (gouvernement). Network, regulation and governance thus form a new device by which it will undoubtedly be excessive to say that it replaces the classical triad-regulation-government pyramid; however, such a dawning is certain and subverts the modes of operation. A few words, especially, about regulation, by which we can say that it has come to be the new mode of production of the right, of means to the right in network. The unilateral command of authority, centralized - sovereign, in a word - gives way to a multipolar, decentralized, adaptive and subsequently negotiated order. The concept of regulation seems to be able to adequately account for this context. Regulating, it could be said, is for normative production, just as the treatment of texts is for the production of information: a flexible and evolving mode of management of an indefinite set of data in the search for an at least provisional balance”.*<sup>52</sup>

It is possible to conclude that the Articles 21 and 22 of the GDPR have limitations and that they should be subject to a future evolution of data protection law, in dialogue with ethical and technical debates. However, it is necessary to emphasize that the problem is even deeper: how can learning algorithms avoid perpetuating discrimination – unjust and unreasonable inferences – underlying the data from which they learn and develop? Law itself cannot solve such a problem. We can clearly see the need for a “multipolar, decentralized, adaptive and negotiated ordination”, as pointed out by François Ost and Michel van de Kerchove. In this way, as exposed by Felipe Debasa, it was necessary, in the past, to comprehend the study of law as a scientific discipline; nowadays, in contrast, it is imperative to analyze it also as a tool.<sup>53</sup> In addition, according to him, we can consider the European Union as a great laboratory to visualize the construction of a new legal and regulatory regime to provide protection to citizens in terms of this new information age.<sup>54</sup> The European Union legal system represents, to a certain extent, a clear example of network integration law, once its protective standards come from a complex dialogue between the national jurisdictions within the Union and international bodies, such as the Council of Europe.

<sup>52</sup> François Ost and Michel Van de Kerchove, *De la pyramide au réseau: pour une théorie dialectique du droit* (Brussels: Université Saint-Louis, 2002), 25-26.

<sup>53</sup> Felipe Debasa, “Fourth industrial revolution social challenges: the Law – from discipline to tool? Reflections about the European Union”, *UNIO – EU Law Journal The Official Blog*, February 5, 2019, <https://officialblogofunio.com/2019/02/05/editorial-of-february-2019>.

<sup>54</sup> Alexandre Veronese, “Revisitando o conceito de direito em rede: uma crítica sociológica à teoria normativista do direito”, *Confluências*, v. 15, (2013): 82-95.