
ARTIFICIAL INTELLIGENCE: REGULATORY CHALLENGES AND RISKIFICATION

INTELIGÊNCIA ARTIFICIAL: DESAFIOS REGULATÓRIOS E RISQUIFICAÇÃO

PAOLA CANTARINI

PhD in Law and Philosophy from PUCSP/Brazil, and from the Università del Salento (It.). Post-doctor degree at EGS/Switzerland, University of Coimbra/Portuga., USP and PUCSP-TIDD. Visiting fellow at the European University Institute/It. University of Miami and Florida International University. Director of Ethikai Institute (ethikai.com.br). ORCID: 0000-0002-9610-8440.

ABSTRACT

Objectives: The article sought to elaborate an approach in the light of interdisciplinarity and the theory of fundamental rights, as an important theoretical reference even when it involves risk analysis.

Methodology: The methodology and research techniques will combine theoretical research on a national and international level, promoting dialogue between the various fields of knowledge, in an interdisciplinary vision.

Results: it was pointed out in the Brazilian's Bill of AI the importance of a more ostensive regulation about procedural obligations, making effective the adoption of good practices and compliance practices in AI, pointing to the need of making the algorithmic impact report mandatory.

Contributions: In this sense, it was pointed out the importance of balancing fundamental rights, applying the proportionality principle. The article aims to point out the importance of an interdisciplinary study as well as an important theoretical reference to the fundamental rights theory, relating to the risky approach, involving protection not only at an individual level, but also at a collective and social level when



talking about artificial intelligence and data protection, correlated with the perspective of the multidimensionality of fundamental rights.

Keywords: Artificial intelligence; Fundamental rights; Riskification; "Brussels effect".

RESUMO

Objetivos: O artigo procurou elaborar uma abordagem à luz da interdisciplinaridade e da teoria dos direitos fundamentais, como uma referência teórica importante, mesmo quando envolve uma análise de risco.

Metodologia: A metodologia e as técnicas de investigação combinarão a investigação teórica a nível nacional e internacional, promovendo o diálogo entre os vários campos do conhecimento, em uma visão interdisciplinar.

Resultados: foi salientada acerca do projeto de lei brasileiro de regulação da IA (PL20/21) a importância de uma regulamentação mais ostensiva sobre obrigações processuais, tornando eficaz a adoção de boas práticas e práticas de compliance na IA, apontando para a necessidade de se tornar obrigatório o relatório de impacto algorítmico.

Contribuições: Neste sentido, foi salientada a importância de equilibrar os direitos fundamentais, aplicando o princípio da proporcionalidade. O artigo pretendeu salientar a importância de um estudo interdisciplinar, bem como uma importante referência teórica à luz da teoria dos direitos fundamentais, relacionada com a abordagem via risquificação, envolvendo proteção dos direitos fundamentais não só a nível individual, mas também a nível coletivo e social, essencial quando se fala de inteligência artificial e proteção de dados, correlacionando-se com a perspectiva da multidimensionalidade dos direitos fundamentais.

Palavras-Chave: Inteligência artificial; Direitos fundamentais; Risquificação; "Efeito Bruxelas".

1 INTRODUCTION

Given the rapid technological development of AI, reaching all social sectors, with such technologies having the greatest impact on the ongoing digital revolution, and with large public and private resources being invested in the field, so far there



generally is an absence of regulations by most countries, including by EU countries. The exception is for specific cases for certain sectors of AI application, such as some sparse regulations on facial recognition and autonomous cars. Given this regulatory vacuum and aiming to fill it whilst also avoiding fragmentation and antinomies due to isolated initiatives, the European Commission (executive arm of the European Union) pointed out the need for global regulation for all EU countries, in order to promote the development of AI while simultaneously addressing the potentially high risks to safety and fundamental and human rights.

One of the main goals to be highlighted is the possibility of the EU becoming economically competitive in this sector, competing in a market currently dominated mainly by the U.S. and China, competing head to head with such countries, having presented on 21.04.2021 a proposal for regulating the use of artificial intelligence in the European Union, in addition to the forecast of investments and funding in the sector of approximately 20 billion euros per year in the next decade seeking the development of technologies that use Artificial Intelligence. The article aims to bring the main issues surrounding this theme, particularly to analyze the so-called "Brussels effect" of the EU regulations in the digital area.

The recent proposal for regulation of AI by the European Commission reflects the analysis among several regulatory possibilities in the sector as well as articulation with the already existing European sectoral legislation, focusing on the "GDPR - General Data Protection Regulation of the EU", the "Digital Services Act", the "Digital Markets Act", the "White Paper on AI" and the "Regulation on liability for the use of AI", in preparation. In summary, the European Commission believes that the new regulation is essential to enable technological innovation and scientific progress, ensuring the necessary competitive advantage and technological leadership of the EU, in a context of strong global competition. All the while, leaving the preservation of fundamental and human rights and basic values enshrined by the EU, placing technology at the service of European citizens. The proposed AI regulation follows the European AI strategy presented in 04/2018 called "Artificial Intelligence for



Europe" (COM/2018/237), with a focus on European values as a means to address the new AI challenges.

In a recent press conference, the President of the European Commission, Ursula von der Leyen, stated the EU's desire to support the development of technology with Artificial Intelligence within the bloc "we want to encourage our businesses, researchers, innovators and entrepreneurs to develop AI, and we want to encourage our citizens to feel confident in using it."

The Commission's understanding is based on the need for heterogenic regulation of AI technology to provide a balance between innovation and protection of rights, preservation of ethical principles, as well as the democratic values enshrined by the EU, as a kind of axiological center of gravity. Both self-regulation, which could draw a first set of parameters ("benchmarks"), and only ethical principles, difficult to be implemented in tangible practices can be considered insufficient. It is a sustainable approach focused on creating a competitive advantage by reaffirming the values consensually agreed upon by the member countries likely to set a direction for technological change.

Other important proposals of regulations for Big Techs in related areas have already been presented on 12.2020 by the European Commission, namely by the DSA (Digital Services Act) and the DMA (Digital Market Act) aiming at a strong regulation of the sector. This limits the market stronghold of the Big Techs, as well as increasing transparency, since there is a huge commercial advantage for such companies, due to the behavioral surplus generated by the wide collection of personal data.

The new regulation follows the optics already outlined by the GDPR, by bringing a strong regulation, in comparison with the only moderate regulation in the USA or weak regulation in Brazil, according to part of the doctrine which follows the perspective of "human rights by design", "beneficial AI", "AI for good" and "Human-Centered AI". This optic aims to bring a balance between technological development, so as not to hinder innovation in one hand, and on the other hand to protect democratic values, human and fundamental rights. It starts from the "human-



centered" approach, bringing the value axis of the human person and human dignity, respecting the stimulus and development of innovation and technology, but providing that there is also respect for fundamental and human rights.

The proposal, therefore, follows the trajectory started with the approval in 02.2017 by the European Parliament Recommendations to the Commission on Civil Law Provisions on Robotics, being the first proposal for AI regulation by the European Union. *Verbis*:

[...] it is extremely important that the legislature considers its legal and ethical implications and effects, without putting obstacles in the way of innovation. Whereas it is necessary to create a generally accepted definition of robot and AI that is flexible and does not hinder innovation [...].

The above mentioned document points to concerns about human-centeredness, or human control of technology, highlighting the danger of a virtual "emotional bond between humans and robots," especially when it comes to vulnerable groups. Much like the proposal of a "code of conduct for robotics engineers" (also applicable to other players in the AI field), bringing the application of the transparency principle, through the creation of "black boxes" for advanced AI applications, preserving an intangible "log" of data related to all operations performed, including the steps of the logic that involved the production of the automated decision.

Another important initiative in the same direction is the so-called "White paper On Artificial Intelligence - An European approach to excellence and trust", of 19.02.2020, focusing on the promotion of scientific innovation, the preservation of the EU's technological leadership, bringing the forecast of large financial investment in the sector, but at the same time bringing the guarantee of protection of fundamental rights, and risk mitigation, migrating to a risk analysis approach when it comes to AI applications.

Therefore, such proposals are linked to the risk-based approach much in line with the practice of compliance, foreseen as fundamental in the field of data



protection, oriented to the probability and severity of the risk, in a proactive, systematic, and continuous process. The new regulation follows this trend already present in several regulations, bringing the prediction of different risk levels for AI applications: unacceptable, high, moderate and minimum. One of the central elements of this approach is the increase in "ex ante" regulations based on the precautionary principle, following the viewpoint of regulatory law.

This approach reflects a true paradigm shift in the field of personal data protection, already present in the GDPR and in AI, as noted in the "White Paper on AI", focusing on a more complex prism of regulatory law, involving techniques for preventing and mitigating risks to fundamental rights and freedoms, as well as pointing to a concern with protection not only for the individual, but also for collective and social protection.

The "risk regulation", typical of environmental law, poses a risk as its central element, linked to processes of information gathering and risk cognition, and creation of "ex ante" regulation instruments, such as codes of conduct, certifications, independent audits, preparation of documents like DPIA - Data Protection Impact Assessment Report and LIA - Legitimate Interest Assessment.

According to the "White Paper on AI", it is considered high risk when the use involves significant risks, in particular with regards to the protection of security, consumer rights, and fundamental rights. An AI application should be considered high risk if it meets the two cumulative criteria: the AI application is used in a sector where significant risks can be expected to occur given the characteristics of the activities typically performed and the assessment of the risk level of a particular use may be based on the impact on affected parties.

Applications of AI for recruitment processes, situations affecting workers' rights, as well as for remote biometric identification and other intrusive surveillance technologies are considered high risk. As a provision for "ex ante" regulation, this document requires that systems must be technically robust and accurate, and developed in a responsible manner through prior risk analysis. In the case of low-risk applications, there is provision for a voluntary labeling regime, opting to be bound to



legal or similar requirements especially created in this area. This would be a condition for receiving a quality seal for AI applications, confirming that a given company would be compliant with certain objective standards.

In turn, unacceptable risks according to the new regulatory proposal are seen in the case of a possible clear threat to European citizens in the form of applications that can manipulate human behavior, opinions, and emotions, especially in view of vulnerable sectors of the population, as is the case with toys with voice assistants. These can more easily manipulate children and teenagers. Another factor is the use of social scoring systems by governments, such as China, seen as an unacceptable risk. In such cases there is an express ban on the use of the AI application. Also considered as high risk is the use of algorithms in the field of selection and recruitment, creditworthiness assessments, distribution of social security benefits or asylum and visa applications and helping judges to make decisions.

There is an express prohibition on the use of surveillance technology except when used by government agencies for the investigation of serious crimes, such as the use of facial recognition in the fight against terrorism. When it comes to high risk, such as AI applications in the areas of transportation, education, security products, recruitment and access to employment, essential or public services, law enforcement or in situations of migration, asylum granting or border control, this use is possible but subject to compliance with strict rules and obligations. Facial recognition and biometric identification systems are considered high risk, prohibiting their use in public space as a rule, with "strictly defined and regulated" exceptions, subject to prior judicial authorization, limiting the time, location and data used. The proposal also aims to combat discriminatory practices, so-called biases, by proposing that datasets should not "incorporate any intentional or unintentional biases" that could lead to discrimination.

As examples of AI applications with minimal and limited risk, we have the use of chatbots as well as the free use of games or spam filters with artificial intelligence

The approach aims at strong state regulation, unlike in the US without regulation on a federal level, and at the same time it would distance itself from the



form of regulation by China, which created a true social surveillance state, contrary to the democratic values of the European Union.

Following the risk-based approach, there is a definition of obligations linked to an adequate risk assessment and mitigation of the systems, greater control over the quality of the data sets that feed the systems, registration of the activities in order to guarantee the traceability of the results, detailed documentation, and human supervision always as a mandatory condition.

With this landmark regulation, the EU is leading the way in developing new global standards to ensure trustworthy artificial intelligence". By setting the standards, it is possible to pave the way for ethical technology around the world while ensuring that the EU remains competitive. Future-proof and innovation-friendly, our rules will be applied when strictly necessary: when it comes to the security and fundamental rights of EU citizens.

In turn, the Bill 21/20 in Brazil, that creates the legal framework for the development and use of Artificial Intelligence (AI) is an important initiative for the regulation of AI in Brazil, alongside the Brazilian AI Strategy in Brazil, Instituted by MCTI Ordinance No. 4,617, dated April 6, 2021, despite some flaws and omissions, technical inaccuracies, absence of substantive and procedural obligations, absence of minimum procedural parameters, and lack of algorithmic governance instruments, especially when compared to international regulations. There is also a flaw to be highlighted regarding the democratic process of deliberation, since there was a short period of time for contributions from civil society, unlike, for example, the Marco Civil da Internet, Bill 12.965/2014, which had a much more extensive period of democratic and inclusive discussion.

A broad period of debate involving diverse civil society groups is essential and is related to the concept of intercultural digital ethics, bringing vulnerable groups and all sectors of society into the dialogue. Precisely intercultural digital ethics and the establishment of concrete frameworks for the translation of abstract ethical principles into concrete practices are points to be developed, and should rely on the



contribution of an interdisciplinary and multistakeholder, and above all independent, team.

The Bill 21/20 that creates the Legal Framework of AI in Brazil is an important initiative towards the regulation of AI, since more and more people are talking about the end of the era of codes of conduct (self-regulation), as pointed out by Luciano Floridi, in his recent article "The end of an era: from self-regulation to hard law for the digital industry". (FLORIDI, 2021)

This document also is based on the precautionary principle, which is considered a benchmark to measure and catalog the safeguards needed for high-risk and moderate-risk AI applications. This is an important framework for AI applications, along with the Impact Assessments on Human/Fundamental Rights, involving a shift in focus: from ethics in AI to a discourse with the framework and vocabulary of Human/Fundamental Rights, as well as focusing on collective, not just individual, protection. There should be broad public scrutiny, and involve a process of public deliberation, with review by independent external organizations or consultants with expertise in fundamental rights.

In this aspect, it is worth pointing out a flaw in the PL by providing only one article mentioning in a generic way the AI Impact Report and the adoption of standards and good practices (art. 13), without further details, as well as by providing that such document may be requested by the State, not making it mandatory in all cases of AI applications involving high or moderate risk, nor making its elaboration mandatory in a preventive way, i.e., before the beginning of the application, during the development of the product or service. There is in the PL a very vague and generic expression related to the elaboration of the impact report, conditioning its requirement to "the justification of its necessity", without further comments or specifications, contributing to legal uncertainty and to a weak level of protection regarding the fundamental rights involved.

There is also no provision in the PL about levels of potential damage of AI applications, contrary to several EU regulations in this sense, which would contribute to the risk-based approach.



3 THE BRUSSELS EFFECT OF THE NEW AI REGULATION

The impact of the new European Union regulations go far beyond the borders of the member countries, which is already the case with the GDPR, a model that has inspired other legislative initiatives in other countries, such as the General Law for the Protection of Personal Data in Brazil (LGPD), Law 13,709/18, as well as the Digital Services Act (DSA), the Digital Markets Act (DMA) and the regulation of hate speech and fake news, with the establishment of the voluntary Code of Conduct of the Commission on Combating Illegal Hate Speech Online. This is the so-called "Brussels effect",¹ in the sense of the extraterritorial effectiveness of European law and the worldwide influence and impact of its regulation. The GDPR has a broad territorial scope since it applies to all companies that process personal data of EU residents, regardless of where the data is processed or the companies are headquartered.

The Brussels Effect would be a manifestation of the European-centric mindset of the global regulatory environment; a theme analyzed by Anu Bradford, Professor of International Law and Organization at Columbia Law School and Senior Research Fellow at the Jerome A. Chazen Institute for Global Business. Bradford, in her book "The Brussels Effect",² points to the global market power of EU regulations, which has increased significantly in the last two decades, particularly in the field of the digital economy, directly impacting global digital businesses, as companies around the world are forced to adapt quickly to its regulations.

Such far-reaching effects of EU regulations can be seen in the famous court case of "Google Spain" (Google Spain S.L, Google Inc. and Agencia Española de Protección de Datos - AEPD, Mario Costeja González - C-131/12), with a broad scope of the right to be forgotten, forcing search engines to eliminate search results in all domains, including those accessible outside the EU. Due to a 2014 decision of

¹ Disponível em <https://valor.globo.com/opiniao/coluna/efeito-bruxelas-atinge-big-techs.ghtml>. Acesso em 05/04/2021.

² Bradford, Anu. The Brussels Effect. Oxford University Press, 2020.



the Court of Justice of the European Union providing for the right to be forgotten with respect to information available on Google, without there being a need or legitimate interest in maintaining the information, this company began to make available on its platform, within the tab "Transparency Report", requests for data removal from European citizens based on that court decision.

As the EU is one of the largest consumer markets in the world, most companies are forced to accept its conditions and regulations, while avoiding the cost of compliance with multiple regulatory regimes elsewhere, extending EU rules to their operations globally. Given the legislative vacuum in the sector on the part of the U.S. in betting on deregulation and techno-liberalism as a digital government strategy, in a regulatory isolationism, despite the Federal Trade Commission's initiatives to combat market domination practices, there was room for the EU to become a regulatory power in that theme, replacing globalization by Europeanization.

4 FINAL CONSIDERATIONS

Several authors point to a paradigm shift through the adoption of a risk management architecture, precautionary of damages, also called "risk-based policies", both for data protection and the use of AI, as pointed out by Serge Gutwirth & Yves Poullet, Claudia Quelle, Alessandro Spina and Rafael Zanata (2017), following the developments in the area of regulatory law, as well as involving a new dimension and re-signification of the concept of risk, approaching the concept of information security.

Such an approach also involves the consideration that the impact of AI systems is not limited to individual aspects but should involve a collective and social perspective. In this line of approach, the use of AI systems is recognized as a potential to play an important role in achieving the Sustainable Development Goals and preserving the democratic process and social rights.



Digital technologies such as AI are a key factor in achieving the goals of the Ecological Pact, calling for a common European approach to AI to achieve a sufficient level of protection and avoid fragmentation of the market. It has the same logic that was followed in the case of GDPR, aiming at a standardization of concepts, institutes and applications, which were previously treated differently by sectoral laws of EU countries.

This was necessary for the integration of the European market, harmonizing the various legislations often bringing conflicts or antinomies, contributing to the hindrance of trade in Europe. With the GDPR we see the creation of a digital single market, allowing an unhindered flow of data within the entire common market. Such fragmentation of the European internal market was already present, given some sparse regulatory initiatives, without a common European legal framework. This is the case of Germany's Data Ethics Commission with the creation of a five-tiered risk-based regulatory system, with no regulation for the most innocuous AI systems up to a total ban in the case of higher risks. Other cases include Denmark by launching the prototype of a data ethics seal and Malta by introducing a voluntary certification system for AI. The various national regulations could create obstacles for companies and investors in the field.

Therefore, the same reasoning is necessary in the field of AI regulation, and is one of the central goals of the new regulatory proposal presented by the European Commission, avoiding the fragmentation of the regulation of this subject by the various countries, which would bring about a consequent fragmentation of the internal market, without having enough strength at the individual level to compete with the main institutions at the global level, and would require a unified approach. Therefore, the new proposal contributes to the EU taking a prominent position in the field of AI and becoming competitive in the world market by bringing a forecast of a unified regulation, ensuring a common approach at the EU level.

We highlight the important remark by Claudia Quelle, from Tilburg University, when she states that data protection may be characterized as risk regulation, but that



the methodologies will be influenced by the theory of balancing fundamental rights, analyzing concrete cases (QUELLE, 2015).

In turn, Wolfgang Hoffmann-Riem³ points to the need for collective protection, including the treatment of power asymmetries, involving collective protection and discussion of ethical issues. It is not only the right to exercise freedom that must be ensured, but also protection against the consequences of the use of freedom by others.

REFERENCES

BEN-SHAHAR, Omri. Data Pollution, 2019: Volume 11, **Journal of Legal Analysis**, p. 133 e ss.

BIONI, Bruno Ricardo, LUCIANO, Maria. **O princípio da precaução na regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada?**, <https://brunobioni.com.br>.

BRADFORD, Anu. **The Brussels Effect**. Oxford University Press, 2020.

CANTARINI, Paola. **Teoria fundamental do direito digital: uma análise filosófico-constitucional**, Clube de autores, 2020.

CANTARINI, Paola. e GUERRA FILHO, Willis S. **Teoria inclusiva dos direitos fundamentais e direito digital**, Clube de autores, 2020.

FLORIDI, Luciano. **The Logic of Information: A Theory of Philosophy as Conceptual Design**, Oxford: OUP, 2019.

FLORIDI, Luciano. **The end of an era: from self-regulation to hard law for the digital industry** (November 9, 2021). Available at SSRN: <https://ssrn.com/abstract=3959766> or <http://dx.doi.org/10.2139/ssrn.3959766>

GELLERT, R. **Data protection: a risk regulation?** Between the risk management of everything and the precautionary alternative. *International Data Privacy Law*, 5, 3-20, 2015.

³ Hoffmann-Riem, Wolfgang, Big data e inteligência artificial: desafios para o direito.



GUTWIRTH, S., & POULLET, Y. Introduction. In S. Gutwirth, Y. Poulet, R. Leenes, & P. de Hert, **European Data Protection: coming of age** (pp. 1-10). Dordrecht: Springer, 2013.

HILDEBRANDT, Mireille. **Smart Regulation and the End(s) of Law**, Publisher: Edward Elgar, 2015.

HOFFMANN-RIEM, Wolfgang. *Big Data e Inteligência Artificial: Desafios Para O Direito*. Journal of Institutional Studies 2 (2020), **Revista Estudos Institucionais**, v. 6, n. 2, p. 431-506, maio/ago. 2020.

HOFFMANN-RIEM, Wolfgang *Autorregulação, autorregulamentação e autorregulamentação regulada no contexto digital*, **Revista da AJURIS** – Porto Alegre, v. 46, n. 146, Junho, 2019.

HOFFMANN-RIEM, Wolfgang **Teoria Geral do Direito Digital, Forense**, ed. kindle, 2021.

QUELLE, C. Does the risk-based approach to data protection conflict with the protection of fundamental rights on a conceptual level?, **Tilburg Law School Research Paper** 1-36, 2015.

PADOVANI, Claudia; SANTANIELLO, Mauro. Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system. **International Communication Gazette**, v. 80, n. 4, p. 295–301, 2018.

SPINA, A. A Regulatory Marriage de Figaro: risk regulation, data protection, and data ethics. **European Journal of Risk Regulation**, 8, 88-94, 2017.

SUZOR, Nicolas. The Role of the Rule of Law in Virtual Communities. Berkeley Technology **Law Journal**, v. 25, n. 4, p. 1817-1886. 2010.

ZANATTA, Rafael, REDE 2017, ***I Encontro da Rede de Pesquisa em Governança da Internet, Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?***

