

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

# Intelligence Artificial and Society Connected

coordination  
Sergio White  
Chiara of Teffe

publication  
January/2025



DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

# Intelligence Artificial and Society Connected

coordination  
Sergio White  
Chiara of Teffe

publication  
January/2025



**Coordination:**

Sergio Branco and Chiara de Teffé

**graphic design, cover and layout:**

Leandro Collares and Mariana Bertoluci

**Editorial production:**

Institute of Technology  
and Society -ITS

**Revision:**

Chiara de Teffé and Mariana Bertoluci

**International Cataloguing in Publication Data (CIP)  
(Brazilian Book Chamber, SP, Brazil)**

Artificial intelligence and connected society  
[electronic book] / coordination Sérgio Branco, Chiara de  
Teffé. -- 1st ed. -- Rio de Janeiro: ITS - Institute of  
Technology and Society, 2025. -- (Dialogues of the  
postgraduate course in digital law)

PDF

Various authors.  
Bibliography.  
ISBN 978-85-5596-010-9

1. Digital law 2. Artificial intelligence -  
Law 3. Protection of personal data 4. Data protection -  
Legislation - Brazil 5. Information society - Legal aspects I.  
Branco, Sérgio. II. Teffé, Chiara de. III. Series.

24-243711

CDU-34:004.8

**Indexes for systematic catalogue:**

1. Artificial intelligence and law 34:004.8

Aline Grazielle Benitez - Librarian - CRB-1/3129

**How to cite:**

BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Coords.). *Artificial intelligence and connected society*. Rio de Janeiro: Rio Institute of Technology and Society, 2025. 368p.

**Institute of Technology and Society:**

itsrio.org | @itsriodejaneiro | midias@itsrio.org



The work Artificial Intelligence and Connected Society is protected under the following license:

Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International



**You have the right to:**

**To share** -copy and redistribute the material in any medium or format.

The licensor cannot revoke these rights as long as you comply with the terms of the license.



**Under the following terms:**

**Assignment** —You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.



**Non-Commercial** —You may not use the material for commercial purposes.



**No Derivations** —If you remix, transform, or build upon the material, you may not distribute the modified material.

**No additional restrictions** —You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

[https://creativecommons.org/licenses/by-nc-nd/4.0/deed.pt\\_BR](https://creativecommons.org/licenses/by-nc-nd/4.0/deed.pt_BR)



---

## LIST OF AUTHORS

---

**Barbara Gomes D'Ascencao**

**Claudio Mendes da Silva**

**Daniel Santiago Diniz**

**Elmano Rodrigues Pinheiro Jr.**

**Giovana Sant'Anna**

**Henry Segolin Molina**

**Luisa Amelia**

**Maria Fernanda Longato**

**Maturana**

**Matheus Mantuani**

**Nina Ramalho Pinheiro**

**Rodrigo Santana dos Santos**

**Taís Bigarella Lemos**

**Victor Call Alvim**

**Vinicius Azevedo Coelho**

# PRESENTATION

---

In a scenario of accelerated innovation, in which Artificial Intelligence and digital technologies have been impacting human and institutional relationships, the book *Artificial Intelligence and Connected Society* aims to contribute to the legal, social and technological discussions of this new era.

Divided into three thematic axes, the work features analyses by several specialized authors, all postgraduate students *broad sense* in Digital Law from ITS Rio in partnership with UERJ and CEPED, which seek to unravel the complex aspects of regulating artificial intelligence, data protection and the structuring of smart cities. This book is essential reading for scholars, professionals and all those interested in the profound impacts of artificial intelligence on an increasingly connected society.

The first axis, dedicated to Artificial Intelligence, offers a broad approach to regulatory aspects applied to AI, especially in the Brazilian context. Issues such as the definition of a regulatory authority for AI, AI training via web scraping, and the originality of AI creations highlight the importance of defining limits and responsibilities for this technology. Important topics such as racism and algorithmic discrimination are given space in detailed discussions that address everything from social justice to the urgency of regulations that promote fair and responsible AI. Finally, the work explores the emerging field of neurorights and its implications, signaling the direct impact of AI on fundamental rights.

In the second axis, Smart Cities and New Technologies, the authors analyze the implications of technologies in so-called smart cities and the regulations that emerge to accompany them. Issues such as necropolitics and data protection in smart cities are addressed, providing a critical perspective on how these innovations affect fundamental rights. Discussions on the regulatory sandbox at the municipal level and the role of the Central Bank in regulating payment fintechs provide the reader with a practical view of the advances and complexities that technology imposes on legal security and public governance. In a look at blockchain technology, a gender perspective is introduced, stimulating a reflection on inclusion in a rapidly developing field.

# PRESENTATION

---

The third axis, Data Protection and Digital Security, offers a regulatory analysis aimed at strengthening cybersecurity and the protection of personal data in the face of threats that permeate the virtual environment. A highlight is the discussion on children's cybersecurity, which explores the need for specific policies to ensure the safety of children and adolescents on the internet, in an increasingly connected scenario. The axis ends with an analysis of the legal bases for data collection in the health area, emphasizing the importance of a system that respects privacy and values diversity, promoting an ethical and inclusive approach to protecting sensitive information.

*Artificial Intelligence and Connected Society* is a work that combines academic rigor with an innovative vision of the contemporary challenges of digital technologies. With reflections that transcend borders and disciplines, this book is a valuable resource for understanding how society can advance in an ethical, inclusive and informed way in the digital age.

ITS Rio believes in the importance of dissemination and access to knowledge. For this reason, this and other postgraduate publications are available free of charge, openly and with the license *Creative Commons Attribution-Non-Commercial-NoDerivatives 4.0 International* (CC BY-NC-ND 4.0).

In the coming years, we hope to expand partnerships and develop more actions focused on digital education that positively impact society and promote access to culture, innovation and information.

We note that the content presented here does not necessarily reflect the institutional opinion of ITS Rio, or its members, representing an academic reflection that is the exclusive responsibility of its author.

We thank everyone who contributed and showed interest in this project. We invite you to check out the other [publications](#) from ITS Rio. We are at your disposal and always open to dialogue.

Rio de Janeiro, December 2, 2024.

**the coordinators**

# THE COORDINATORS

---

## Chiara of Teffe

PhD and Master's Degree in Civil Law from the State University of Rio de Janeiro (UERJ), having been approved with distinction, praise and recommendation for publication. Graduated in Law from the Federal University of Rio de Janeiro (UFRJ), when she was a scientific initiation scholarship holder from CNPq and FAPERJ. Currently, she is the academic coordinator of the postgraduate course in Digital Law at the Rio Institute of Technology and Society (ITS Rio), in partnership with UERJ, and professor of Civil Law and Digital Law at the IBMEC Law School. She teaches specific postgraduate and extension courses at CEPED-UERJ, PUC-Rio, EMERJ and ITS Rio. Member of the Data Protection and Privacy Commission of the OAB/RJ. Member of the Civil Law Commission of the Rio de Janeiro Sectional Council of the OAB (2022/2024). Member of the Permanent Forum for Freedom of Expression, Fundamental Freedoms and Democracy of EMERJ. Member of the Permanent Forum for Technological Innovations in Law at EMERJ. She was a substitute professor of Civil Law at UFRJ. She is a member of the Brazilian Institute for Studies in Civil Liability (IBERC). She is a full member of the Municipal Council for the Protection of Personal Data and Privacy of Rio de Janeiro. She works as a lawyer in the areas of Civil Law and Digital Law and as a consultant in the protection of personal data. She is the author of the books "Sensitive personal data: qualification, treatment and good practices" and "Protection of the right to image on the Internet: from the identification of damage to its compensation".

## Sergio White

Co-founder and director of the Rio de Janeiro Institute of Technology and Society (ITS Rio). PhD and Master's degrees in Civil Law from the State University of Rio de Janeiro (Uerj). Guest researcher at the Centre de Recherche en Droit Publique of the University of Montreal. Visiting Research Fellow at Sciences Po between 2023 and 2024. Specialist in intellectual property from the Pontifical Catholic University of Rio de Janeiro – PUC-Rio. Postgraduate degree in documentary filmmaking from FGV. Graduated in Law from the State University of Rio de Janeiro (Uerj). Partner at the law firm Rennó Penteadó Sampaio.

# SUMMARY

---

AXIS 1

## ARTIFICIAL INTELLIGENCE

**13**

**Regulation of artificial intelligence: reflections on the definition of a competent authority in Brazil**

Elmano Rodrigues Pinheiro Jr.

**35**

**Artificial Intelligence and Personal Data Protection: reflections on the appropriate legal basis to support training via web scraping**

Matheus Mantuani

**56**

**Algorithmic Racism: The Challenges of Artificial Intelligence and Social Justice in the Digital Context**

Barbara Gomes D'Ascencao

**72**

**Personal Data Collection for Generative Artificial Intelligence Training: A Challenge for Data Protection and Privacy**

Rodrigo Santana dos Santos

**94**

**Classification of damages resulting from AI incidents**

Vinicius Azevedo Coelho

**113**

**PL 2.338/2023: a study on copyright provisions**

Nina Ramalho Pinheiro

**133**

**Algorithmic Originality: is there originality in the outputs of generative artificial intelligence?**

Taís Bigarella Lemos

# SUMMARY

---

**151**

**The challenges involved in the use and regulation of artificial intelligence in the face of algorithmic discrimination**

Maria Fernanda Longato Maturana

**169**

**A critical analysis of discriminatory algorithmization in criminal law**

Luisa Amelia Lino

**190**

**Between Brain and Computer: Dialogues on Neurorights and Artificial Intelligence**

Henry Segolin Molina

AXIS II

## SMART CITIES AND NEW TECHNOLOGIES

**212**

**Smart Cities and Necropolitics: Data Protection and Fundamental Rights in the Digital Age**

Claudio Mendes da Silva

**230**

**Implementation of smart cities and regulatory sandbox: Challenges and opportunities in Juiz de Fora's innovation law**

Daniel Santiago Diniz

**251**

**From Legal Security to Technical Security: Decoding Themes of Technological Advances in Electronic Real Estate Registration**

Louis Henry de Menezes Acioly

**273**

**The role of the Central Bank of Brazil in regulating payment fintechs**

Victor Call Alvim

# SUMMARY

---

**287**

**Blockchain as a feminine noun: a gender analysis of the rising use of blockchain technology**

Carolina Freitas

AXIS III

## DATA PROTECTION AND DIGITAL SECURITY

**304**

**Risk and Cybersecurity in Brazil: a regulatory analysis aimed at data protection**

Giovana Sant'Anna

**326**

**Cyberchildhood and social cybersecurity: seeking to improve the protection of children and adolescents on the internet**

Ligia Maria de Souza Lopes Reis

**346**

**The legal bases in the information collection system on diversity in Health and Digital Health**

Maira Lima de Souza

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

AXIS 1

# Intelligence Artificial

## AUTHORS

Barbara Gomes D'Ascencao

Luisa Amelia

Maria Fernanda Longato Maturana

Matheus Mantuani

Nina Ramalho Pinheiro

Rodrigo Santana dos  
Santos

Vinicius Azevedo Coelho

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

1

# Regulation of artificial intelligence: reflections on the definition of an authority competent in Brazil

Elmano Rodrigues Pinheiro Jr.

Summary: Introduction. 1. Regulation of emerging digital technologies. 2. Regulation of artificial intelligence. 2.1. Regulatory approaches in the European Union, the United States and the United Kingdom. 2.2. Proposals for state regulation of AI in Brazil. 3. Reflections on the definition of a competent authority for the regulation of artificial intelligence in Brazil. Final considerations. References.

## Introduction

Regulation is a central theme in many contemporary discussions about public policy. After the economic crisis of 2008 and the COVID-19 pandemic, few would disagree with the importance of regulation for the smooth functioning of modern market economies.<sup>2</sup> However, the role of regulation has not always been understood, recognized or desired, especially when it comes to emerging digital technologies, as was the case with the Internet.

In the “Declaration of the Independence of Cyberspace”, John Perry Barlow, renowned internet rights activist, defended the idea that the network should be treated as a new world, without rules, and free from the authoritarian abuses of governments.

Contrary to this utopian vision, the Internet is now seen as an extension of the “real world”. With the spread of networks in all areas of society – political, economic, social and cultural – discussions have begun to recognize regulation as essential, aiming to curb undesirable behaviors, such as the concentration of markets by digital platforms, and to promote positive uses, such as access to digital content with respect for copyright.

The debate on the regulation of emerging digital technologies, as happened with the Internet, has reached a new level in recent years, marking a kind of loss of innocence in relation to the discussions of the 1990s and 2000s. While in the previous period the argument predominated

1. Graduated in Electrical Engineering with an emphasis on Electronics from the São Paulo State University (Unesp), postgraduate degree in Telecommunications Regulation from the University of Brasília (UnB) and Master of Science in Electrical Engineering from the Military Institute of Engineering (IME). Postgraduate degree in Digital Law from the Rio Institute of Technology and Society (ITS), in partnership with the State University of Rio de Janeiro (UERJ) and the Center for Studies and Research in Legal Education (CEPED). He has held the position of Regulatory Specialist at the National Telecommunications Agency (Anatel) since 2005.

2. LODGE, Martin; WEGRICH, Kai. The Rooting of Quality Regulation: Asking the Hard Questions is the Answer. *In*: PROENCA, Jadir Dias; COSTA, Patricia Vieira da; MONTAGNER, Paula (Coord). *Regulatory challenges in Brazil*. Brasília: ENAP, 2009. p. 17.

tion against any form of regulation, with a utopian perspective of the benefits that uncontrolled technological innovation could bring, in the last twenty years a much more skeptical and pessimistic view on the subject has been observed<sup>3</sup>, recognizing the need to establish a specific legal framework that minimizes its potential harmful effects. Nevertheless, such regulation has been constructed from an adaptive perspective, based on experience and practice, so that it can be effective and relevant, as has already been thought of for the regulation of the Internet<sup>4</sup>.

The purpose of this paper is to explore one of the most significant emerging digital technologies: artificial intelligence. However, it is not intended to completely exhaust the topic, since, given the complexity of the subject, a detailed analysis of all the aspects involved would go beyond the limits established for the paper. The objective is to examine specific aspects of the regulation of artificial intelligence.

The general objective of this work is to evaluate different models of artificial intelligence regulation that have been implemented. Specifically, it seeks to: understand the specificities of the regulation of digital technologies and the possible impacts of its implementation; verify the different approaches and regulatory structures related to artificial intelligence in the European Union, the United States and the United Kingdom; evaluate the proposal for regulating artificial intelligence in Brazil; investigate how Bill No. 2,338, of 2023, deals with the issue of defining a competent authority for the regulation of artificial intelligence.

The relevance of this topic is due to the fact that emerging digital technologies, which transform personal and property relationships, creating and improving products, services and activities, procedures and practices, in various economic sectors and in relation to many aspects of society, also entail new risks and amplify existing ones. The use of artificial intelligence, for example, in the production or manipulation of content with the aim of disseminating notoriously false or decontextualized facts, can potentially harm the balance and integrity of electoral processes, thus justifying some form of regulation. For the analysis, the literature review methodology will be adopted.

3. BIANQUINI, Heloisa. Ex ante regulation, ex post regulation and responsive regulation: exploratory notes on the sanctioning process of the National Data Protection Authority. In: CAMPOS, Ricardo (org.). *The future of digital platform regulation: Digital Services Act (DAS), Digital Markets Act (DMA) and their impacts in Brazil*. 1st ed. New York: Oxford University Press, 2023. p. 266-267.

4. LESSIG, Lawrence. *The Law of the Horse: What Cyber Law Might Teach*. Harvard Law Review, Harvard, vol. 113, p. 501-546, Dec. 1999. Available at: <https://cyber.harvard.edu/works/lessig/finalhls.pdf>. Accessed on: October 1, 2024.

Therefore, this article will be divided into four chapters. Chapter 1 will present considerations on the theory of regulation and the challenges for regulating emerging digital technologies, such as artificial intelligence. Chapter 2, divided into two sections, will examine the evolution of the regulation of artificial intelligence in the world, presenting some approaches already taken, and the debate on the regulation of artificial intelligence in Brazil. Chapter 3 will reflect on the definition of a competent authority for the regulation of artificial intelligence in the country, presenting the advantages and disadvantages of adopting different models and under the coordination of different entities. Finally, the final considerations of the work will be presented, highlighting the main findings and providing suggestions for future research to be carried out.

## 1. Regulation of emerging digital technologies

Digital technologies are revolutionizing almost every sector of the economy, introducing innovative products and services, enabling new business models, and transforming the way countries promote and enjoy socioeconomic development. Digital technologies make it possible to connect citizens to services and opportunities, helping to build a more inclusive and prosperous future. However, to ensure that markets operate effectively and satisfactorily meet society's needs and expectations, it is essential that this transformation be accompanied by appropriate public policies and a regulatory environment that promotes fair competition, protects consumers, and encourages responsible innovation.<sup>5</sup>

The digitalization of societies and economies is generating unprecedented amounts of data, driven by the rapidly increasing connectivity between people and devices. Emerging technologies (such as 5G) are making it easier to engage in digital activities, while social media platforms and user-generated content are encouraging such interaction. At the same time, more devices are becoming "smart," connecting to the internet to exchange information. As a result of the explosive growth of data, new technologies have emerged that sift through and analyze large data sets, broadly described as artificial intelligence and *big data*.<sup>6</sup>

5. INTERNATIONAL TELECOMMUNICATIONS UNION; WORLD BANK. *Digital Regulation Handbook*. Geneva, 2020. Available at: <http://handle.itu.int/11.1002/pub/81630556-en> . Accessed on: July 22, 2024.

6. *Ibid.*, p. 142.

These technological innovations are challenging regulators to review their strategies to promote fair competition and protect consumers. In addition to the technical challenges, these technologies raise legal, ethical and macroeconomic issues. Central banks, consumer protection agencies, competition commissions and information and communications technology (ICT) sector regulators are working to assess the impact of these changes on their respective areas of responsibility. This may involve the need to redesign the roles of several regulators.<sup>7</sup>

With regard to regulators overseeing the ICT sector, and who are directly involved with emerging digital technologies, the *Digital Regulation Handbook*, published by the ITU and the World Bank, identifies three main models of institutional structure: sector-specific regulator, multi-sectoral regulator and convergent regulator. According to the study, traditionally, regulators with an exclusive focus were common for telecommunications regulation. However, nowadays, such regulators are less frequent compared to convergent or multi-sectoral regulators.

Thus, it can be said that the digital era has profoundly changed the roles of regulators and policymakers. While the traditional areas of responsibility and institutional structure of regulators may still remain relevant in the digital environment, regulation needs to become more flexible and adaptable. Regulators' remits may also need to be adjusted to accommodate the new digital realities.<sup>8</sup>

However, these new areas do not always fit neatly into existing regulatory frameworks, and many countries have been discussing whether their traditional regulators would have the necessary authority to deal with emerging digital technologies. While these discussions are at an early stage, the analysis generally involves assessing whether a new regulatory body dedicated exclusively to digital issues would be needed, whether an existing regulator would need to be expanded, or whether the most appropriate model would be an ICT regulator working alongside other government authorities responsible for areas such as consumer protection, privacy and cybersecurity.<sup>9</sup>

7. *Ibid.*, p. 142.

8. SCHOLZE, Simone Henriqueta Cossetin; VIEIRA, Vania Lucia Ribeiro; AGUIAR, Alexandre Kehrig Veronese. *Study on pro-innovation regulatory model*. 2024. p. 41.

9. INTERNATIONAL TELECOMMUNICATIONS UNION; WORLD BANK. *Digital Regulation Handbook*. Geneva, 2020. p. 8. Available at: <http://handle.itu.int/11.1002/pub/81630556-en> . Accessed on: July 22, 2024.

## 2. Regulation of artificial intelligence

In order to discuss the regulation of artificial intelligence, it is essential to clarify what is meant by artificial intelligence (AI). Definitions vary according to the area of knowledge used to explain it and take into account its transdisciplinarity and the complexity of its systems, algorithms and applications.<sup>10</sup> Given the rapid technological advancement, the concept of artificial intelligence has also been constantly updated and adjusted to reflect the latest changes.

In this context, recognizing that the concept is subject to revision, the Organization for Economic Cooperation and Development (OECD) defines artificial intelligence as a machine-based system that, for explicit or implicit purposes, infers from the data it receives how to generate results such as predictions, content, recommendations or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptability after implementation.<sup>11</sup>

As conceptualized, artificial intelligence is an emerging digital technology that has the potential to transform many aspects of life and society, including human well-being, inclusive economic growth, sustainable development, innovation, and the protection of human rights and fundamental freedoms. However, it also poses considerable risks to the population and society, and may threaten these essential rights and freedoms. One such risk is the spread of bias and discrimination, in which AI may make discriminatory decisions. Other risks commonly associated with the use of AI are: violation of privacy; cybersecurity; use for malicious purposes, such as fraud and illicit activities; obtaining information that may pose risks to the integrity of individuals; misinformation and manipulation of information; damage or harm caused by unintended consequences.<sup>12</sup>

These risks associated with technology have led to a growing demand for legal regulation of artificial intelligence. There are several approaches to such regulation, including the creation of specific laws for AI,

10. DE OLIVEIRA, Thaís Figueira. A regulatory authority for artificial intelligence in Brazil. In: CAMPOS, Ricardo (org.). *The future of digital platform regulation: Digital Services Act (DAS), Digital Markets Act (DMA) and their impacts in Brazil*. 1st ed. New York: Oxford University Press, 2023. p. 756-757.

11. ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. *Recommendation of the Council on Artificial Intelligence*. Paris, 2024. p. 7. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> . Accessed on: July 26, 2024.

12. BRAZIL. Federal Court of Auditors. *Ruling No. 616/2024*. Plenary. Rapporteur: Minister Aroldo Cedraz. Session of 04/03/2024. Brasília, TCU, 2024. p. 6. Available at: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233> . Accessed on: July 22, 2024.

the adoption of legislation that promotes innovation or even the decision not to regulate, with the justification that current regulations would already be sufficient<sup>13</sup>.

Given the dynamic and rapidly evolving nature of the area, regulation faces the challenge of anticipating future scenarios that may or may not materialize. Excessive regulation can inhibit technological advancement and reduce the international competitiveness of productive sectors. Thus, one of the main challenges is to find a balance between protecting individual and collective rights and enabling innovation and market development.<sup>14</sup> In this environment, the regulatory approaches being employed can be categorized into several types<sup>15</sup>, highlighting three main ones: regulation based on principles, based on risks and based on rights.

Principle-based regulation guides the development and use of artificial intelligence (AI) systems by establishing general premises and ethical guidelines, without the need to specify a rigid set of rights and obligations from the outset. These principles guide the development and use of AI systems through ethical, responsible, human-centered and human rights-respecting processes.<sup>16</sup>

In turn, risk-based regulation focuses on identifying and managing the risks associated with the development and use of artificial intelligence systems. This approach aims to adapt regulatory obligations or requirements based on the level of risk presented by different types of AI systems.<sup>17</sup> Unlike principle-based regulation, which is more flexible and guided by general values, risk-based regulation adopts a more structured and specific approach. It classifies AI systems according to their risk levels and sets strict governance standards based on the severity of the risks identified. This approach aims to ensure that control and regulatory measures are proportionate to the risk posed by each AI application.<sup>18</sup>

13. *Ibid.*, p. 7-8.

14. *Ibid.*, p. 8.

15. UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION. *Consultation Paper on AI Regulation: Emerging Approaches Across the World*. Paris, 2024. p. 20. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000390979>. Accessed on: October 1, 2024.

16. *Ibid.*, p. 21.

17. *Ibid.*, p. 35.

18. BRAZIL. Federal Court of Auditors. *Ruling No. 616/2024*. Plenary. Rapporteur: Minister Aroldo Cedraz. Session of 04/03/2024. Brasília, TCU, 2024, p. 8. Available at: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233>. Accessed on: July 22, 2024.

Finally, rights-based regulation emphasizes the protection of human and fundamental rights in the context of AI systems. This approach defines in advance a specific set of rights and obligations that must be respected in the development and use of AI, prioritizing the safeguarding of users' rights. While this approach offers a clear set of standards and protections, it can face significant challenges, especially due to its detailed and comprehensive nature, which may not keep pace with the speed and flexibility of the AI market. In contrast to other approaches, which may be more adaptive or guided by general principles, rights-based regulation can pose greater challenges to innovation and technological advancement, as it seeks to balance the protection of individual rights with the need for flexibility in technological development.<sup>19</sup>

From an internationalist perspective, normative and regulatory policies on artificial intelligence can also be systematized into three approaches to legal intervention: multilateral and regional dialogues (especially by international organizations such as the United Nations and the European Union); national strategies (with the adoption of government policies aimed at stimulating artificial intelligence in domestic environments); and transnational regulatory standards (such as principles, codes of conduct, guidelines and recommendations from non-state actors).<sup>20</sup>

For a more detailed analysis of these regulatory approaches, the next section will explore regulatory initiatives in the European Union (EU), the United States, the United Kingdom and, subsequently, the case of Brazil will be examined.

## 2.1 Regulatory approaches in the European Union, in United States and United Kingdom

Several countries are currently developing regulatory frameworks to integrate AI into their legal systems. Globally, there is a common trend in governmental and jurisdictional approaches that aims not only to harness the benefits of AI systems for society, industry and the public sector, but also to balance

19. *Ibid.*, p. 8.

20. POLIDO, Fabrício Bertini Pasquot. New perspectives for regulating artificial intelligence: dialogues between domestic policies and transnational legal processes. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord). *Artificial intelligence and law: ethics, regulation and responsibility*. 2nd ed. rev. updated. and increased. São Paulo: Thomson Reuters Brazil, 2020. p. 180.

these advantages with the ethical and legal concerns associated with their implementation<sup>21</sup>.

The European Union, based on its experience with personal data protection, which led to the publication of the General Data Protection Regulation (GDPR), regulatory model on the subject, has made, with regard to artificial intelligence, a continuous effort to develop a comprehensive system that guarantees safe and ethical technology. In 2018, the European Commission created a specific group to deal with the issue of AI, marking the beginning of regulatory work. In 2021, the proposal for a legal regulation on AI was published, which, after extensive discussions, received the negotiating position of the European Parliament in June 2023 and a final agreement in December of the same year, and which became known as *Artificial Intelligence Act (EU AI Act)*<sup>22</sup>.

THE *EU AI Act* adopts a risk-based approach, classifying AI systems into different risk categories, such as unacceptable, high, limited and minimal. This approach not only establishes strict legal requirements for high-risk systems, addressing aspects such as data governance, transparency and security, but also includes an experimental regulatory environment (*sandbox* regulatory<sup>23</sup>). This strategy aims to ensure that regulation is adaptable and balanced, encouraging innovation while protecting user rights and safety.<sup>24</sup>.

To implement the *EU AI Act*, each EU Member State must designate or establish a national authority responsible for assessing and monitoring compliance with the legislation. In addition, the draft provides for the creation of the *European Artificial Intelligence Board*, a committee designed to advise and assist national authorities in enforcing the rules. However, recent amendments suggest the need for a centralized agency with its own legal personality, funding and staff, to coordinate and harmonize actions among Member States and avoid market fragmentation. This proposal seeks to ensure more uniform and effective regulation by aligning

21. DE OLIVEIRA, Thaís Figueira. A regulatory authority for artificial intelligence in Brazil. In: CAMPOS, Ricardo (org.). *The future of digital platform regulation: Digital Services Act (DAS), Digital Markets Act (DMA) and their impacts in Brazil*. 1st ed. New York: Oxford University Press, 2023. p. 762.

22. BRAZIL. Federal Court of Auditors. *Ruling No. 616/2024*. Plenary. Rapporteur: Minister Aroldo Cedraz. Session of 04/03/2024. Brasília, TCU, 2024, p. 8. Available at: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233>. Accessed on: July 22, 2024.

23. The *sandbox* allows for more flexible experimentation with new products and services, while maintaining regulatory oversight. This strategy aims to ensure that regulation is adaptable and balanced, encouraging innovation while protecting user rights and safety.

24. *Ibid.*, p. 8.

national decisions and fostering a trusted and cohesive AI ecosystem across the European Union<sup>25</sup>.

In turn, AI regulation in the United States is in an early stage, reflecting a still-developing approach to dealing with the rapid evolution of this technology. In October 2022, the country launched the *Blueprint for AI Bill of Rights*, a technical document intended to guide the development of policies that protect civil rights and promote democratic values, but which does not yet constitute formal legislation<sup>26</sup>. This document serves as a guiding principle for the U.S. government, focusing on avoiding regulatory overload and maintaining U.S. leadership in the AI sector.<sup>27</sup> Recently, in October 2023, President Joe Biden issued an executive order<sup>28</sup> that sets new standards for safety and security, addressing concerns such as privacy and equity, and encouraging innovation and research in the sector<sup>29</sup>.

In the United States, the recent regulatory framework adopts a sectoral approach, characterized by co-regulation, conducted through the actions of federal regulatory agencies, state and local governments. In this structure, federal agencies are responsible for issuing principles-based guidelines and leave implementation to the private sector. *Federal Trade Commission (FTC)*, for example, has published guidelines that highlight the importance of AI systems being transparent, explainable, fair, and accountable. The *Department of Defense (DoD)* adopted ethical principles for AI applicable to both combat and non-combat functions, focusing on accountability, fairness, traceability, reliability, and governance. In addition, the *Food and Drug Administration (FDA)* introduced an action plan for AI software as a medical device, seeking to evaluate and monitor such software throughout its lifecycle<sup>30</sup>.

25. DE OLIVEIRA, Thaís Figueira. A regulatory authority for artificial intelligence in Brazil. In: CAMPOS, Ricardo (org.). *The future of digital platform regulation: Digital Services Act (DAS), Digital Markets Act (DMA) and their impacts in Brazil*. 1st ed. New York: Oxford University Press, 2023. p. 764.

26. MELO, Ana Karolina Acris; SOUZA, Jessica Cardoso; VASCO, Amanda Corrêa; REIS, Bruno Salomon. *Regulation of Artificial Intelligence: benchmarking of selected countries*. Brasília: National School of Public Administration, 2022. p. 18. Available at: <https://repositorio.enap.gov.br/handle/117419>. Accessed on: October 1, 2024.

27. The text does not introduce a new law or regulatory policy for the United States government. It is a statement of principles, based on five fundamental premises to protect the public in the age of artificial intelligence: 1. Automated systems must be safe and effective; 2. Users must be protected from algorithmic discrimination, ensuring equitable use; 3. People must have control over the use of their data, preventing abusive practices; 4. It is essential that users understand how and why an AI system made a certain decision; 5. People must have the option to object to AI decisions and request a human review in case of error or dispute.

28. *Executive Order*, equivalent to a Decree of the Presidency of the Republic in Brazil.

29. NAZARENO, Claudio. *Regulation of artificial intelligence: international experiences and challenges for Brazil*. Brasília: Chamber of Deputies, Legislative Consultancy, 2024. p. 15. Available at: <https://bd.camara.leg.br/bd/handle/bdcamara/41741>. Accessed on: October 1, 2024.

30. BELLI, Luca; CURZI, Yasmin; GASPAR, Walter B. *AI Regulation in Brazil: Advancements, flows, and need to learn from the data protection experience*. Computer Law & Security Review: The International Journal of Technology Law and Practice, vol. 48, p. 3-4.

In addition to executive directives and orders, several legislative proposals dealing with artificial intelligence have been approved in the United States. Among them, *Algorithmic Accountability Act* and the *Consumer Online Privacy Rights Act*, which aim to create specific regulations for automated decisions and online privacy. The *Good AI Act* of 2022 proposes the creation of a “Working Group on Artificial Intelligence Hygiene”, while the *Advancing American AI Act* seeks to regulate the use of AI by government agencies. However, to date, there has been no significant progress in adopting these proposals, and there is no comprehensive federal legislation on AI in the country<sup>31</sup>.

As regards the United Kingdom, in 2023, the government published the technical document *A pro-innovation approach to AI regulation*, reflecting a distinct strategy for regulating artificial intelligence. Through a flexible and iterative approach<sup>32</sup>, the UK seeks to balance fostering innovation with managing the risks associated with technology. Rather than establishing rigid and immediate regulation, the UK model is designed to evolve over time, allowing for continuous adjustments based on the progress of research and the maturity of the sector. This strategy is guided by principles and premises that adapt to the specific needs of different areas of the economy, preferring to regulate the use of AI rather than the technology itself.<sup>33</sup>.

In this way, the aim is to have a regulation that is predominantly sectoral and adjusted according to the rapid cycles of innovation and technological development. In this case, the central function of the regulatory authority is not to directly regulate all aspects of AI, but rather to manage the process through monitoring, evaluation and feedback. The authority is also responsible for supporting the implementation of regulatory principles, managing cross-sector risks, promoting innovation, and ensuring interoperability with international regulatory models.<sup>34</sup>.

In addition to its flexible regulatory approach, the UK government has also published an algorithmic transparency standard, accompanied by a framework and guidance to support the public sector in adopting this standard. This initiative reflects the UK’s commitment to establishing clear practices.

31. RADI, V. Gábor. *Comparative Analysis of the AI Regulation of the EU, US and China from a Privacy Perspective*. 2023 46th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2023, p. 1446.

32. In this approach, regulation is developed as studies progress, the sector matures and risks are identified, allowing for more effective adaptation in a field that requires rapid iteration and development cycles.

33. BRAZIL. Federal Court of Auditors. *Ruling No. 616/2024*. Plenary. Rapporteur: Minister Aroldo Cedraz. Session of 04/03/2024. Brasília, TCU, 2024, p. 9. Available at: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233> . Accessed on: July 22, 2024.

34. *Ibid.*, p. 9.

ras and those responsible for using algorithm-based systems, aiming to increase transparency and accountability in the public sector<sup>35</sup>.

In addition to the UK, several countries are adopting a sectoral approach to regulating artificial intelligence<sup>36, 37</sup>. These countries aim to integrate AI regulation into existing legal systems, ensuring that principles of accountability and trustworthiness are effectively enforced within the specific areas of activity of their respective authorities.<sup>38</sup>.

## 2.2 Proposals for state regulation of AI in Brazil

The trajectory of artificial intelligence in Brazil has been marked by significant strategic and legislative efforts, reflecting the growing importance of this technology for national development. The Brazilian Artificial Intelligence Strategy (EBIA), established by Ordinance MCTI No. 4,617/2021 and updated by Ordinance No. 4,979/2021, emerges as an important initial milestone<sup>39</sup>. Developed based on OECD guidelines, the EBIA aims to promote inclusive growth, transparency, and safety in the implementation of AI in the country.<sup>40</sup> However, the implementation of the EBIA has faced challenges, such as the lack of a detailed schedule and the definition of clear responsibilities, aspects that have been criticized by analysts and experts in the field.<sup>41</sup>.

The EBIA's objectives include promoting investment in research and innovation, training skilled professionals, and facilitating cooperation between the public and private sectors. Despite its key role, the strategy has been criticized for its lack of a detailed plan and the absence of a dedicated regulatory authority for AI. Implementation has been slow, exacerbated by the change of government in 2023, and the review of the

35. BELLI, Luca; CURZI, Yasmin; GASPAR, Walter B. *AI Regulation in Brazil: Advancements, flows, and need to learn from the data protection experience*. Computer Law & Security Review: The International Journal of Technology Law and Practice, vol. 48, p. 4.

36. IAPP. IAPP Research and Insights, 2023. *International Definitions of Artificial Intelligence*. Available at: <https://iapp.org/resources/article/international-definitions-of-ai/>. Accessed on: October 2, 2024.

37. WHITE & CASE. White & Case, 2024. *AI Watch: Global regulatory tracker*. Available at: <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker>. Accessed on: July 31, 2024.

38. DE OLIVEIRA, Thaís Figueira. A regulatory authority for artificial intelligence in Brazil. In: CAMPOS, Ricardo (org.). *The future of digital platform regulation: Digital Services Act (DAS), Digital Markets Act (DMA) and their impacts in Brazil*. 1st ed. New York: Oxford University Press, 2023, p. 766-767.

39. Information on advances in AI-enabling technologies, which enable analyses of their adoption and their main impacts on society, can be obtained from the Brazilian Observatory of Artificial Intelligence, accessible at: <https://obia.nic.br/s/home>.

40. BRAZIL. Ministry of Science, Technology, Innovation and Communications. *Brazilian Artificial Intelligence Strategy – EBIA*. Brasília, MCTIC, 2021, p. 17. Available at: [https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivointeligenciaartificial/ia\\_estrategia\\_diagramacao\\_4-979\\_2021.pdf](https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivointeligenciaartificial/ia_estrategia_diagramacao_4-979_2021.pdf). Accessed on: July 26, 2024.

41. DE OLIVEIRA, Thaís Figueira. A regulatory authority for artificial intelligence in Brazil. In: CAMPOS, Ricardo (org.). *The future of digital platform regulation: Digital Services Act (DAS), Digital Markets Act (DMA) and their impacts in Brazil*. 1st ed. New York: Oxford University Press, 2023. p. 759-760.

strategy can incorporate new axes and themes, such as cybersecurity and a more robust approach to public safety<sup>42</sup>.

In the National Congress, the debate on AI regulation has advanced through several Bills (PL). Bill No. 21, of 2020, approved by the Chamber of Deputies and currently being processed in the Senate, established the initial framework for AI regulation, but was criticized for its generic nature and lack of depth. This bill sought to create basic guidelines and principles for the use of AI, but did not sufficiently address issues such as privacy, ethics, and the creation of an authority<sup>43</sup>.

This bill was combined with others for joint processing. In order to draft a highly technical and advanced legislative text, a Committee of Jurists was created to support the drafting of a substitute bill. Based on all the material analyzed, the Committee of Jurists presented its final report, together with a draft bill to regulate artificial intelligence. In this context, Bill No. 2,338 of 2023 was drafted, which was based on the conclusions of the aforementioned Committee and sought to reconcile, in legislation, the protection of fundamental rights and freedoms, the appreciation of work and human dignity, and the promotion of technological innovation represented by artificial intelligence.<sup>44</sup>.

Bill No. 2,338/2023 represented a more structured attempt to regulate artificial intelligence in Brazil, adopting a risk-based approach, similar to the European Union's proposal, and establishing strict measures for high-risk systems. When providing for the oversight of artificial intelligence, the bill determined that the Executive Branch would designate an authority to ensure compliance with the established standards, without defining whether this body would be one already existing within the structure of the Federal Public Administration or a new body to be created later.

The substitute for Bill No. 2,338/2023, presented by Senator Eduardo Gomes in June 2024, reflects recent discussions on the topic of artificial intelligence, highlighting the need for multisectoral governance, emphasizing transparency, accountability, and the protection of rights.

42. BRAZIL. Federal Court of Auditors. *Ruling No. 616/2024*. Plenary. Rapporteur: Minister Aroldo Cedraz. Session of 04/03/2024. Brasília, TCU, 2024, p. 7. Available at: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233> . Accessed on: July 22, 2024.

43. DE OLIVEIRA, Thaís Figueira. A regulatory authority for artificial intelligence in Brazil. In: CAMPOS, Ricardo (org.). *The future of digital platform regulation: Digital Services Act (DAS), Digital Markets Act (DMA) and their impacts in Brazil*. 1st ed. New York: Oxford University Press, 2023. p. 761.

44. BRAZIL. Federal Senate. Bill No. 2338, of May 3, 2023. *Provides for the use of Artificial Intelligence*. Brasília: Federal Senate, 2023. Available at: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233> . Accessed on: July 22, 2024.

humans. The text provides for the creation of a public database on high-risk AI and the civil liability of AI agents, as well as mechanisms for reporting incidents and monitoring compliance. These aspects demonstrate progress in relation to previous proposals, seeking to balance the protection of rights with the promotion of innovation. Regarding the competent authority, the substitute for Bill No. 2,338/2023 provides for the designation of a monitoring and supervision system that includes:

- creation of the National System for Regulation and Governance of Artificial Intelligence (SIA), which enhances the regulatory skills of sectoral authorities;
- designation of the National Data Protection Authority (ANPD) as the competent authority to coordinate the SIA, which will also have the mission of reducing regulatory asymmetry in the face of the various intense uses of AI systems in unregulated sectors.

### 3. Reflections on the definition of an authority competent for the regulation of artificial intelligence in Brazil

Regulatory authorities have the purpose of regulating, organizing, controlling and supervising specific matters and may vary in structure, approach, objectives and scope. They may be established within the Direct or Indirect Public Administration, or they may operate as independent entities or private organizations with public interest responsibilities.<sup>45</sup> When reflecting on a competent authority for regulating artificial intelligence in Brazil, the issue can be assessed, fundamentally, from the perspective of defining an institutional structure model to be used and a body to be used as the central authority of this model.

As explained in previous sections, proposals for a competent authority to regulate emerging digital technologies, such as AI, have followed three different models: sector-specific regulator, multi-sectoral regulator and convergent regulator.

The specific regulatory model for artificial intelligence, used in Spain, for example, with the creation of *Spanish Supervision Agency*

45. DE OLIVEIRA, Thaís Figueira. A regulatory authority for artificial intelligence in Brazil. In: CAMPOS, Ricardo (org.). *The future of digital platform regulation: Digital Services Act (DAS), Digital Markets Act (DMA) and their impacts in Brazil*. 1st ed. New York: Oxford University Press, 2023. p. 770.

of *Artificial Intelligence (AESIA)*, has the advantage of being able to design an authority with the necessary characteristics to face ethical and human rights challenges raised by the development, implementation and use of AI. There are understandings that, given the complexity of the issue, a regulatory authority would need to integrate several *expertises* and multidisciplinary knowledge, including legal and technical, in addition to having a comprehensive regulatory and normative capacity<sup>46</sup>. On the other hand, the creation of a body with such competence and characteristics may require a high investment on the part of the Government. Furthermore, there is still not enough information on the effectiveness of applying this model in other parts of the world.

In turn, the multisectoral regulatory model, used, for example, in Jamaica (*Office of Utilities Regulation*, which oversees the telecommunications, energy, water and transportation sectors), has the advantage of taking advantage of the existing institutional structure to regulate a new sector, with administrative synergies and economies of scale in improving processes. However, in the Brazilian case, there are no bodies with this characteristic qualified to regulate AI, given that the existing ones, such as the Administrative Council for Economic Defense (CADE), deal with very specific aspects of regulation (in this case, the defense of competition).

The creation or merger of existing authorities into a convergent regulator, encompassing related ICT areas (such as telecommunications and data protection), presents the same advantages as the previous model, with the benefit of increasing the degree of specialization, which makes the authority more capable of responding in an agile and coordinated manner to emerging challenges in the area of artificial intelligence.<sup>47</sup> An example of this approach is China, with the Cyberspace Administration of China<sup>48</sup>. In Brazil, this approach is particularly delicate due to the necessary interventions of the Legislative Branch in the Executive Branch.<sup>49</sup>

46. DATA PRIVACY BRAZIL. Data Privacy Brasil, 2023. *AI in Brazil: who will be responsible for regulation?*. Available at: <https://www.dataprivacybr.org/documentos/ia-no-brasil-quem-sera-responsavel-pela-regulamentacao/?idProject=2331>. Accessed on: October 2, 2024.

47. BRAZIL. National Data Protection Authority. *Technical Note No. 16/2023/CGTP/ANPD*. Brasília, ANPD, 2023. Available at: [https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota\\_Tecnica\\_16ANPDIA.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf). Accessed on: July 30, 2024.

48. STANFORD UNIVERSITY. DigiChina, 2022. *Behind the Facade of China's Cyber Super-Regulator*. Available at <https://diqichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/>. Accessed on: October 2, 2024.

49. An example of controversy was the enactment of the General Law on the Protection of Personal Data (LGPD), in which the provisions proposed by the Legislature and which dealt with the structuring of the National Data Protection Authority (ANPD) were vetoed by the President of the Republic, as they allegedly constituted unconstitutionality of the legislative process, due to an affront to article 61, § 1º, II, 'e', in conjunction with article 37, XIX of the Constitution. Further information on the reservation of initiative in: REZEN-DE, RM de. *The Unbearable Uncertainty in the Should-Be: reserve of legislative initiative, oscillating jurisprudence and the creation of budgetary funds*. Brasília: Center for Studies and Research/CONLEG/Senate, April/2017 (Discussion Paper No. 231). Available at: <http://senado.leg.br/estudos>. Accessed on: October 3, 2024.

Considering the advantages and disadvantages of these three models, and considering the Brazilian legal system and the context in which it is inserted, in addition to the transdisciplinarity and complexity of AI systems, a hybrid approach seems to be the most appropriate for their regulation in Brazil, with the use of a convergent authority as coordinator of a regulatory system, associated with regulatory agencies of specific sectors already existing, as should be done in France with the National Commission for Informatics and Liberties (CNIL). This is justified by the fact that sectoral authorities, with their experience and specialization, are better positioned to deal with issues related to the development and application of AI systems in areas such as health, transportation and natural resources, for example.<sup>50</sup> This alternative is in line with what was proposed in the substitute for Bill No. 2,338/2023, presented by Senator Eduardo Gomes and currently under discussion in the National Congress.

From this perspective, the choice of the central regulatory body naturally falls on one of the two main agencies related to ICT regulation in Brazil: the National Telecommunications Agency (Anatel) and the National Data Protection Authority (ANPD).

Created by the General Telecommunications Law (Law No. 9,472, of July 16, 1997), Anatel was the first regulatory agency to be established in Brazil, on November 5, 1997. Anatel is an entity that is part of the indirect Federal Public Administration, subject to a special autonomous regime and linked to the Ministry of Communications. It is administratively independent and financially autonomous. The Agency's objective is to promote the development of telecommunications in the country in order to provide it with a modern and efficient telecommunications infrastructure, capable of offering society adequate, diversified and fairly priced services throughout the national territory.

Headquartered in Brasília, Anatel carries out inspection activities and maintains closer contact with society through units in all Brazilian capitals. Its staff, according to information from March 2024<sup>51</sup>, totals 1,343 (one thousand three hundred and forty-three) employees, of which 96.87% are from its own staff, 2.68% are requested from other agencies.

50. DE OLIVEIRA, Thaís Figueira. A regulatory authority for artificial intelligence in Brazil. In: CAMPOS, Ricardo (org.). *The future of digital platform regulation: Digital Services Act (DAS), Digital Markets Act (DMA) and their impacts in Brazil*. 1st ed. New York: Oxford University Press, 2023. p. 772.

51. BRAZIL. Ministry of Management and Innovation in Public Services. *Bulletin of the Direct, Autonomous and Foundational Administration*. Brasília, MGI, 2024, p. 165. Available at: <https://www.gov.br/gestao/pt-br/central-de-conteudo/publicacoes/boletins/boletins-da-administracao-direta>. Accessed on: July 30, 2024.

public administration bodies and 0.45% have no link with the public service, occupying positions of free appointment and dismissal.

In turn, the ANPD was created by Provisional Measure No. 869 of 2018, converted into Law No. 13,853 of July 8, 2019, which amended the General Data Protection Law (Law No. 13,709 of August 14, 2018), and began operating effectively with the appointment of its first CEO on November 5, 2020. The ANPD, like Anatel, is a special agency linked to the Ministry of Justice and Public Security, consequently having technical and decision-making autonomy and its own assets. The ANPD is the central body for interpreting the General Data Protection Law, and is responsible for establishing standards and guidelines for its implementation, seeking to ensure the right of all Brazilians to have their personal data duly protected.

Headquartered in Brasília, but without decentralized units, ANPD does not have its own staff. To form its staff, it had to request 120 (one hundred and twenty) employees from other agencies. Including cleaning staff, secretarial staff, reception staff and interns, the agency has a total of 152 (one hundred and fifty-two) people, of which only 10 (ten) work with inspection or handling of security incidents, according to information from December 2023.<sup>52</sup>

Based on the above, taking as a reference Anatel's current competences with regard to telecommunications, it is understood that this agency already has experience in carrying out activities similar to those that should be carried out by the competent AI authority, such as accreditation, certification and inspection.<sup>53</sup> Despite an apparent lack of synergy between sectors, the development of artificial intelligence solutions and systems is based on an immense mass of data in constant flow, access to which is only possible through a robust, stable, broad and resilient connectivity infrastructure, composed of multiple data access and transport networks.<sup>54</sup> Furthermore, if Bill No. 2,768 of 2022 comes into effect

52. CHAMBER OF DEPUTIES. Chamber News Agency, 2023. *ANPD president calls for competition for agency; inspection division has only 5 employees*. Available at: <https://www.camara.leg.br/noticias/1014383-president-da-anpd-asks-for-competition-for-inspection-division-agency-has-only-5-employees>. Accessed on: July 31, 2024.

53. BRAZIL. National Telecommunications Agency. *Report No. 27/2024/ARI*. Brasília, Anatel, 2024. Available at: [https://sei.anatel.gov.br/sei/modulos/pesquisa/md\\_pesq\\_documento\\_consulta\\_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD-26Q9Xx5QNDbqbjNRZm5SUvRZmQf9kFzb6NVVMeEFdPgHerLaOe9k3Jw\\_0wiL8oZeTeLc2rSt0jscq85OhSwCRK5T4BsfXOKEQg](https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD-26Q9Xx5QNDbqbjNRZm5SUvRZmQf9kFzb6NVVMeEFdPgHerLaOe9k3Jw_0wiL8oZeTeLc2rSt0jscq85OhSwCRK5T4BsfXOKEQg). Accessed on: July 30, 2024.

54. BRAZIL. National Telecommunications Agency. *AI–Artificial Intelligence: Institutional Vision of the Future*. Brasília, Anatel, 2024. Available at: [https://sei.anatel.gov.br/sei/modulos/pesquisa/md\\_pesq\\_documento\\_consulta\\_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYiHvsTCI8r6V00ltjrypit3yX4N4bkPXcoJgxuzJCUPSMamOo4UK2mN71rPT-Gc\\_Cr76yKk1yu0Gqxy4v3MR80F](https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYiHvsTCI8r6V00ltjrypit3yX4N4bkPXcoJgxuzJCUPSMamOo4UK2mN71rPT-Gc_Cr76yKk1yu0Gqxy4v3MR80F). Accessed on: July 30, 2024.

If approved under its current terms, the Agency would have its scope of action expanded in relation to emerging digital technologies. Thus, the use of this agency as the central body for AI regulation appears appropriate, taking into account its consolidated structure, regional presence and staff.

On the other hand, the ANPD already stands out as a reference entity in the protection of personal data and in guaranteeing the privacy of citizens. AI, with its capabilities for processing and analyzing large volumes of data, is directly aligned with the ANPD's competencies.<sup>55, 56, 57</sup>, a fact recognized in the substitute for Bill No. 2,338/2023<sup>58</sup>. This intersection between AI and data protection focuses AI governance on technical and operational issues, with a continued emphasis on the protection of fundamental rights and the security of personal data. In addition, it allows the formation of a technical body specialized in both areas, optimizing the application of public resources and avoiding regulatory fragmentation and overlapping of competences between different bodies.<sup>59</sup>. However, as it is a recent and still-forming body, and as it does not have its own staff or decentralized operations, changes in its responsibilities could have an impact on its structure and budgets, which would result in a compromise in its results.

## Final considerations

Through this study, it was possible to understand the specificities of the regulation of digital technologies and the possible impacts of their implementation, as well as to understand the different approaches and regulatory structures related to artificial intelligence.

The studies also enabled a better understanding of the trajectory of artificial intelligence in Brazil, which reflects an ongoing effort to align

55. BRAZIL. National Data Protection Authority. *Preliminary analysis of Bill No. 2338/2023, which provides for the use of Artificial Intelligence*. Brasília, ANPD, 2023. Available at: [https://www.gov.br/anpd/pt-br/assuntos/noticias/analisepreliminar-do-pl-2338\\_2023-formatado-ascom.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/analisepreliminar-do-pl-2338_2023-formatado-ascom.pdf) . Accessed on: October 3, 2024.

56. BRAZIL. National Data Protection Authority. *Technical Note No. 16/2023/CGTP/ANPD*. Brasília, ANPD, 2023. Available at: [https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota\\_Tecnica\\_16ANPDIA.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf) . Accessed on: July 30, 2024.

57. BRAZIL. National Data Protection Authority. *PL 2338 – SUBSTITUTE – SPECIAL COMMITTEE ON ANPD CONTRIBUTIONS – MAY - 2024*. Brasília, ANPD, 2024. Available at: [https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-apresenta-propostas-de-alteracao-do-substitutivo-ao-pl-2338-sobre-inteligencia-artificial/Versao\\_final\\_07.05.24\\_PL\\_2338\\_Substitutivo\\_Comissao\\_Especial\\_Propostas\\_ANPD1.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-apresenta-propostas-de-alteracao-do-substitutivo-ao-pl-2338-sobre-inteligencia-artificial/Versao_final_07.05.24_PL_2338_Substitutivo_Comissao_Especial_Propostas_ANPD1.pdf) . Accessed on: October 3, 2024.

58. BRAZIL. Federal Senate. *Bill No. 2338, of May 3, 2023. Provides for the use of Artificial Intelligence*. Brasília: Federal Senate, 2023. Available at: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233> . Accessed on: July 22, 2024.

59. BRAZIL. National Data Protection Authority. *Technical Note No. 16/2023/CGTP/ANPD*. Brasília, ANPD, 2023. p. 6. Available at: [https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota\\_Tecnica\\_16ANPDIA.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf) . Accessed on: July 30, 2024.

The country is aligned with international best practices, promoting responsible and innovative technological development. Although the EBIA and bills such as Bill No. 2,338/2023 represent significant advances, effective implementation and the creation of dedicated regulatory frameworks will be essential to ensure that Brazil fully leverages the potential of AI. This must be done while protecting citizens' rights and promoting a safe and ethical innovation environment.

Yet, despite the proposals put forward, Brazil faces challenges in effectively implementing these strategies and regulations. The question of whether to create a dedicated regulatory authority or to use the existing regulatory framework remains open. A dedicated authority could play a crucial role in enforcing and monitoring AI laws, as well as defining best practices and audits.

Regardless of the regulatory system chosen and in light of the public administration model organized in the 1988 Federal Constitution, it is essential that the authority be established as a special agency, with technical and decision-making autonomy, in addition to having its own assets and personnel. Experience with the implementation of regulatory agencies in Brazil indicates that the artificial intelligence regulatory authority should incorporate, in its decision-making process, practices such as public consultations and hearings, interaction with stakeholders, and the adoption of collaborative and evidence-based mechanisms. In addition, the authority should have an advisory body whose main function is to ensure the active participation of various groups and sectors of society in decisions related to AI, both in the formulation and implementation of public policies and in the actions of the central authority.

In view of the above, it is suggested that future research be carried out to evaluate the effectiveness of EBIA in practice, analyzing how it has been applied and what its impacts have been to date, as well as the analysis of regulatory policies in other jurisdictions, in order to identify factors of success or failure and implications for the regulation of artificial intelligence in Brazil.

As initially announced, the complexity of the issue of artificial intelligence in our time was confirmed. It also highlighted the urgency and inevitability of addressing the issue and the need to define its regulation so that Brazilian society can rise to the challenges that AI represents.

## References

BELLI, Luca; CURZI, Yasmin; GASPAR, Walter B. *AI Regulation in Brazil: Advancements, flows, and need to learn from the data protection experience*. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, vol. 48, p. 105767, 2023. Available at: <https://doi.org/10.1016/j.clsr.2022.105767>. Accessed on: July 23, 2024.

BELLI, Luca; ZINGALES, Nicolo. *Data protection and artificial intelligence inequalities and regulations in Latin America*. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, vol. 47, p. 105761, 2022. Available at: <https://doi.org/10.1016/j.clsr.2022.105761>. Accessed on: July 24, 2024.

BRAZIL. National Telecommunications Agency. *Report No. 27/2024/ARI*. Brasilia, Anatel, 2024. Available at: [https://sei.anatel.gov.br/sei/modulos/pesquisa/md\\_pesq\\_documento\\_consulta\\_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqBJNRZm5SUvRZmQf9kFzb6NVVMeEFdPgHerLaOe9k3Jw\\_0wiL8oZeTeLc2rSt0jscq85O4UQg](https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqBJNRZm5SUvRZmQf9kFzb6NVVMeEFdPgHerLaOe9k3Jw_0wiL8oZeTeLc2rSt0jscq85O4UQg). Accessed on: July 30, 2024.

BRAZIL. National Telecommunications Agency. *AI – Artificial Intelligence: Institutional Vision of the Future*. Brasilia, Anatel, 2024. Available at: [https://sei.anatel.gov.br/sei/modulos/pesquisa/md\\_pesq\\_documento\\_consulta\\_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx-5QNDbqYiHvsTCI8r6V00ltjrypit3yX4N4bkPXcoJgxuzJCUPSMamOo4U](https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx-5QNDbqYiHvsTCI8r6V00ltjrypit3yX4N4bkPXcoJgxuzJCUPSMamOo4U). Accessed on: July 30, 2024.

BRAZIL. National Data Protection Authority. *Preliminary analysis of Bill No. 2338/2023, which provides for the use of Artificial Intelligence*. Brasilia, ANPD, 2023. Available at: [https://www.gov.br/anpd/pt-br/assuntos/noticias/analisepreliminar-do-pl-2338\\_2023-formatado-ascom.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/analisepreliminar-do-pl-2338_2023-formatado-ascom.pdf). Accessed on: October 3, 2024.

BRAZIL. National Data Protection Authority. *Technical Note No. 16/2023/CGTP/ANPD*. Brasilia, ANPD, 2023. Available at: [https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota\\_Tecnica\\_16ANPDIA.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf). Accessed on: July 30, 2024.

BRAZIL. National Data Protection Authority. *PL 2338 – SUBSTITUTE – SPECIAL COMMITTEE ON ANPD CONTRIBUTIONS – MAY – 2024*. Brasilia, ANPD, 2024. Available at: [https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-apresenta-propostas-de-alteracao-do-substitutivo-ao-pl-2338-sobre-inteligencia-artificial/Versao\\_final\\_07.05.24\\_PL\\_2338\\_Substitutivo\\_Comissao\\_Especial\\_Propostas\\_ANPD1.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-apresenta-propostas-de-alteracao-do-substitutivo-ao-pl-2338-sobre-inteligencia-artificial/Versao_final_07.05.24_PL_2338_Substitutivo_Comissao_Especial_Propostas_ANPD1.pdf). Accessed on: October 3, 2024.

BRAZIL. Ministry of Science, Technology, Innovation and Communications. *Brazilian Artificial Intelligence Strategy – EBIA*. Brasilia, MCTIC, 2021. Available at: [https://www.gov.br/mcti/pt-br/seguidores-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia\\_estrategia\\_diagramacao\\_4-979\\_2021.pdf](https://www.gov.br/mcti/pt-br/seguidores-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_diagramacao_4-979_2021.pdf). Accessed on: July 26, 2024.

BRAZIL. Ministry of Management and Innovation in Public Services. *Bulletin of the Direct, Autonomous and Foundational Administration*. Brasília, MGI, 2024. Available at: <https://www.gov.br/gestao/pt-br/central-de-conteudo/publicacoes/boletins/boletins-da-administracao-direta>. Accessed on: July 30, 2024.

BRAZIL. Federal Senate. *Bill No. 2338, of May 3, 2023. Provides for the use of Artificial Intelligence*. Brasília: Federal Senate, 2023. Available at: <https://www25.senado.leg.br/web/activity/materials/-/materials/157233>. Accessed on: July 22, 2024.

BRAZIL. Federal Court of Auditors. *Ruling No. 616/2024*. Plenary. Rapporteur: Minister Aroldo Cedraz. Session of 04/03/2024. Brasília, TCU, 2024. Available at: <https://pesquisa.apps.tcu.gov.br/redirect/process/3363820233> . Accessed on: July 22, 2024.

CHAMBER OF DEPUTIES. Chamber News Agency, 2023. *ANPD president calls for competition for agency; inspection division has only 5 employees*. Available at: <https://www.camara.leg.br/noticias/1014383-president-da-anpd-pede-concurso-para-agencia-divisao-de-inspection-has-only-5-employees> . Accessed on: July 31, 2024.

CAMPOS, Ricardo (org.). *The future of digital platform regulation: Digital Services Act (DAS), Digital Markets Act (DMA) and their impacts in Brazil*. 1st ed. 778 p. ISBN 978-65-5396-146-3.

DATA PRIVACY BRAZIL. Data Privacy Brasil, 2023. *AI in Brazil: who will be responsible for regulation?*. Available at: <https://www.dataprivacybr.org/documentos/ia-no-brasil-quem-sera-responsavel-pela-regulamentacao/?idProject=2331> . Accessed on: October 2, 2024.

DELOITTE. Deloitte Insights, 2018. *The Future of Regulation: Principles for Regulating Emerging Technologies*. Available at: <https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html> . Accessed on: July 31, 2024.

FRAZAO, Ana; MULHOLLAND, Caitlin (Coord). *Artificial intelligence and law: ethics, regulation and responsibility*. 2nd ed. rev. updated. and increased. São Paulo: Thomson Reuters Brasil, 2020. 736 p. ISBN 978-65-5614-221-0.

GIL, Antonio Carlos. *How to develop research projects*. 4th ed. 176 p. ISBN 85-224-3169-8.

HARTMANN, Ivar A. (Coord). *Policy Paper: Regulation of Artificial Intelligence in Brazil*. Rio de Janeiro: FGV Direito Rio, 2020. 39 p. Available at: <https://diretorio.fgv.br/conhecimento/policy-paper-regulation-of-artificial-intelligence-in-brazil> . Accessed on: October 1, 2024.

IAPP. IAPP Research and Insights, 2023. *International Definitions of Artificial Intelligence*. Available at: <https://iapp.org/resources/article/international-definitions-of-ai/> . Accessed on: October 2, 2024.

KLARIĆ, Mirko. *Regulation of AI Technology Implementation in Public Administration*. 2024 47th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2024, p. 1450-14564. Available at: <https://doi.org/10.1109/MIPRO60963.2024.10569836> . Accessed on: July 24, 2024.

LESSIG, Lawrence. *The Law of the Horse: What Cyber Law Might Teach*. Harvard Law Review, Harvard, vol. 113, p. 501-546, Dec. 1999. Available at: <https://cyber.harvard.edu/works/lessig/finalhls.pdf> . Accessed on: October 1, 2024.

MELO, Ana Karolina Acris; SOUZA, Jessica Cardoso; VASCO, Amanda Corrêa; REIS, Bruno Salomon. *Regulation of Artificial Intelligence: benchmarking of selected countries*. Brasília: National School of Public Administration, 2022. 35 p. Available at: <https://repositorio.enap.gov.br/handle/1/7419> . Accessed on: October 1, 2024.

NAZARENO, Claudio. *Regulation of artificial intelligence: international experiences and challenges for Brazil*. Brasília: Chamber of Deputies, Legislative Consultancy, 2024. 32 p. Available at: <https://bd.camara.leg.br/bd/handle/bdcamara/41741> . Accessed on: October 1, 2024.

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION. *Consultation Paper on AI Regulation: Emerging Approaches Across the World*. Paris, 2024. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000390979>. Accessed on: October 1, 2024.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. *Recommendation of the Council on Artificial Intelligence*. Paris, 2024. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Accessed on: July 26, 2024.

COLLINS, Paula; *Regulatory challenges in Brazil*. Brasilia: ENAP, 2009. 342 p. ISBN 978-85-256-0062-2.

RADI, V. Gábor. *Comparative Analysis of the AI Regulation of the EU, US and China from a Privacy Perspective*. 2023 46th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2023, p. 1446-1451. Available at: <https://doi.org/10.23919/MIPRO57284.2023.10159864>. Accessed on: July 24, 2024.

RAJAGOPAL, Manikandan; SIVASAKTHIVEL, Ramkumar; RAMAR, Gobinath; ANIFA, Mansurali; KARUPPASAMY, Sathesh Kumar. *A Conceptual Framework for AI Governance in Public Administration – A Smart Governance Perspective*. 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2023, p. 488-495. Available at: <https://doi.org/10.1109/I-SMAC58438.2023.10290366>. Accessed on: July 24, 2024.

REZENDE, RM of. *The Unbearable Uncertainty in the Should-Be: reserve of legislative initiative, oscillating jurisprudence and the creation of budgetary funds*. Brasília: Center for Studies and Research/CONLEG/Senate, April/2017 (Discussion Paper No. 231. Available at: [www.senado.leg.br/studies](http://www.senado.leg.br/studies). Accessed on: October 3, 2024.

ROQUETE, Felipe Leitao Valadares. *Artificial intelligence, values and uncertainty: an insoluble problem for regulation?*. Internet & Society Journal, v. 2, n. 2, p. 150-154, Dec. 2021. Available at: <https://revista.internetlab.org.br/wp-content/uploads/2022/03/Inteligencia-artificial-valores-e-incerteza-um-problema-insolovel-para-a-regulacao.pdf>. Accessed on: October 1, 2024.

SCHOLZE, Simone Henriqueta Cossetin; VIEIRA, Vania Lucia Ribeiro; AGUIAR, Alexandre Kehrig Veronese. *Study on pro-innovation regulatory model*. 2024. e-Book. (1 online resource 304 p).

STANFORD UNIVERSITY. DigiChina, 2022. *Behind the Facade of China's Cyber Super-Regulator*. Available at: <https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/>. Accessed on: October 2, 2024.

THE ECONOMIST. The Economist, 2023. *The world wants to regulate AI, but does not quite know how*. Available at: <https://www.economist.com/business/2023/10/24/the-world-wants-to-regulate-ai-but-does-not-quite-know-how>. Accessed on: July 31, 2024.

INTERNATIONAL TELECOMMUNICATIONS UNION; WORLD BANK. *Digital Regulation Handbook*. Geneva, 2020. Available at: <http://handle.itu.int/11.1002/pub/81630556-en>. Accessed on: July 22, 2024.

WEBER, Rolf. Artificial Intelligence: A Theoretical Analysis of Regulatory Models. In: BELLI, Luca; GASPAR, Walter B. (Coord). *The Quest for AI Sovereignty, Transparency and Accountability: Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition*. Rio de Janeiro: FGV Law Rio, 2023. p. 71-83.

WHITE & CASE. White & Case, 2024. *AI Watch: Global regulatory tracker*. Available at: <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker>. Accessed on: July 31, 2024.

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

2

**Artificial Intelligence and  
Personal Data Protection:  
reflections on the appropriate legal  
basis to support  
web training**

**scraping**

Matheus Mantuani

Summary: Introduction. 1. Information Scraping *Online* in Times of *Big Data*. 2. Compatibility of Data Protection with the *Web Scraping*. 3. In Search of the Legal Hypothesis Applicable to AI Training. Final Considerations. References.

## Introduction

In 1956, ten scientists met at Dartmouth College in New Hampshire, United States, to carry out a study on artificial intelligence (“AI”), which was based on the hypothesis that aspects of learning and other characteristics of the human mind could, in principle, be precisely described so that a machine would be able to simulate them.<sup>2</sup>

Almost seventy years after the inauguration of this field of research, it is clear how AI systems<sup>3</sup> have historically continued according to this ideal of probabilistic uses based on information, in order to arrive at certain results,<sup>4</sup> increasingly complex.<sup>5</sup> This is because the computing field presupposedly defined those systems as machines that manipulated numbers, so that everything could be coded mathematically,<sup>6</sup> through algorithms – operations that would offer a way for machines to process data and automate decisions.<sup>7</sup>

1. Lawyer. Postgraduate student in Digital Law at UERJ. Graduated in Law from UERJ. Has worked in the area of technology and intellectual property at Rennó Penteadó Sampaio Advogados since 2021. He worked as Technical Editor and Coordinator of the Journal of the UERJ Law School. He interned at the Court of Justice of the State of Rio de Janeiro and at the Public Defender's Office of the State of Rio de Janeiro. He was Director of the Luiz Carpenter Academic Center and Student Representative on the Departmental Council, Department of State Law and Department of Theories and Foundations of Law of the UERJ Law School. He worked as a researcher and scholarship monitor at UERJ. Author of articles published in scientific journals and in book chapters.

2. MCCARTHY, John et al. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. USA, New Hampshire: Dartmouth College, 1955.

3. The exact concept of an AI system remains in dispute, but for the purposes of this research the notion provided for in the Artificial Intelligence Regulation, recently approved in the European Union, will be adopted: “a machine-based system designed to operate with variable levels of autonomy, and which can present adaptive capabilities after deployment and which, for explicit or implicit purposes, and based on the input data it receives, infers how to generate results, such as predictions, content, recommendations or decisions that can influence physical or virtual environments”. EU. *Artificial Intelligence Act. Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence*. European Union: European Parliament, 2024, Article 3(1).

4. BOSTROM, Nick. *Superintelligence: Paths, Dangers and Strategies for a New World*. Translation: Aurelio Monteiro, Clemente Penna, Fabiana Monteiro and Patricia Geremias. Rio de Janeiro: Darkside, 2018.

5. BARROSO, Luis Roberto; MELLO, Patricia Perrone Campos. *Artificial intelligence: promises, risks and regulation. Something new under the sun*. Law and Praxis Journal. Rio de Janeiro, 2024. In press.

6. NEWELL, Allen. *Intellectual Issues in the History of Artificial Intelligence*. IN: MACHLUP, Fritz; MANSFIELD, Una (Eds.). *The Study of Information: interdisciplinary messages*. USA, New York: Wiley, 1983, pp. 187-294.

7. BAROCAS, Solon; SELBST, Andrew. *Big Data's Disparate Impact*. California Law Review. USA, California, v. 104, no. 3, pp. 671-732, Jun., 2016.

Among the information that could be used to train and develop AI systems, personal data<sup>8</sup> available on the Internet<sup>9</sup> have gained special attention in a scenario of *Big Data*, a term used to describe the “fuel” that would make the machines work,<sup>10</sup> the raw material required for processing the systems.<sup>11</sup> As Gustavo Tepedino points out, “every day an incalculable amount of data is extracted by economic agents”,<sup>12</sup> a situation which allows machines to become more “intelligent” – in the sense of learning and improving their systems based on the personal data collected.<sup>13</sup>

One of the techniques commonly used in these contexts is data scraping ( *data scraping*) – automated extraction that aims to collect large amounts of information for structuring in a database,<sup>14</sup> in order to guarantee subsequent analyses and uses.<sup>15</sup> However, scraping information from the Internet ( *web scraping*) is criticized from a personal data protection perspective,<sup>16</sup> given that specific legislation on the matter tends to impose restrictions on the collection and processing<sup>17</sup>

8. Personal data can be defined, in light of article 5, I, of the General Law on the Protection of Personal Data (Federal Law No. 13,709/2018), such as information related to an identified or identifiable natural person. BRAZIL. *Law No. 13,709 of August 14, 2018. General Personal Data Protection Law (LGPD)*. Brasilia: National Congress, 2018.

9. The Internet is defined by article 5, I, of the Internet Civil Rights Framework (“MCI”), as the system consisting of a set of logical protocols, structured on a global scale for public and unrestricted use, with the purpose of enabling data communication between terminals through different networks. *Idem*. *Law No. 12,965 of April 23, 2014. Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil..* Brasilia: National Congress, 2014.

10. “Big Data is fundamental to the use and development of algorithms and artificial intelligence (‘AI’). Algorithms and AI are the machines; Big Data is the fuel that makes the machines run. Just as oil made the machines and factories run in the Industrial Age, Big Data makes the relevant machines run in the Algorithmic Society.” [Our translation]. BALKIN, Jack. *Free Speech in the Algorithmic Society: big data, private governance, and new school speech regulation*. University of California, Davis, Law Review. USA, California, v. 51, n. 615, pp. 1,149-1,210, Sept., 2017, p. 1,154.

11. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Struggle for a Human Future on the New Frontier of Power*. Translation: George Schlesinger. New York: Routledge, 2019.

12. TEPEDINO, Gustavo. *Technologies and the renewal of Civil Law*. OAB/RJ, Rio de Janeiro, June 12, 2019.

13. SURBLYTÈ, Gintarė. *Data as a Digital Resource*. Max Planck Institute for Innovation & Competition Research Paper no. 16-12. Germany, Bavaria, Oct., 2016, p. 29

14. Database, according to article 5, IV, of the General Law on the Protection of Personal Data, refers to the structured set of personal data, established in one or more locations, in electronic or physical support. BRAZIL. *Law No. 13,709, of August 14, 2018*, *locus citatum*.

15. AARONSON, Susan Ariel. *Data Dysphoria: the governance challenge posed by Large Language Models*. Institute for International Economic Policy Working Paper no. 2023-07. USA, Washington, DC., Aug., 2023.

16. Recently, the Brazilian National Data Protection Authority (“ANPD”) ordered the precautionary suspension of the processing of personal data for training the AI of the company Meta Platforms, Inc., considering illegal, in a judgment of likelihood, the “broad, general and indiscriminate collection of all information available and shared by users on the platforms” of that company. BRAZIL. *Vote no. 11/2024/DIR-MW/CD*. Brasilia: National Data Protection Authority, 2024, p. 11.

17. In Brazilian legislation, according to article 5, X, of the General Law on the Protection of Personal Data, the technical term processing encompasses any operation carried out with personal data, such as those referring to collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination or extraction. *Idem*. *Law No. 13,709, of August 14, 2018, locus citatum*.

later of these available data *online*,<sup>18</sup> as observed in activities aimed at training AI systems.

In this line, the present research has as its central objective to identify to what extent the General Law for the Protection of Personal Data of Brazil (Federal Law No. 13,709/2018, “LGPD”) limits the *web scraping* for the purposes of training AI systems, due to the need to substantiate the collection of information *online* in one of the hypotheses provided for in the legislation – the so-called legal bases. Based on bibliographic research and direct review of specialized literature sources, the chapters of the article present the rise of *scraping* on the Internet and in the context of *Big Data*, its clash with personal data protection legislation and the challenges of identifying a legal hypothesis that allows AI training via *scraping online*. In final considerations, the substantial role of the Brazilian National Data Protection Authority (“ANPD”) is noted,<sup>19</sup> as an interpreter of the LGPD, in the balance between the protection of the interests and fundamental rights of the holders, and the privilege of the country's technological development, with equal attention to the principle of freedom of business models promoted on the Internet.

## 1. Scraping Online Information in Times of Big Data

THE *web scraping* usually facilitates analytical processes through AI, from a coding language,<sup>20</sup> through key steps, which involve, for example, the insertion of information and the URL (“Uniform Resource Locator”), a term that includes the “specific indication” of a page on the Internet,<sup>21</sup> node *script* (script) of the scraping, so that the data and content requested by the programmer can be extracted, an act that generally occurs through spreadsheets or text files.<sup>22</sup>

This type of data mining is a prerequisite for the business model of various technology companies. The collection of available information *online* configures, in contemporary times, the necessary structuring

18. An example of limitation of *web scraping* is article 7, § 7, of the General Law on the Protection of Personal Data, according to which the subsequent processing of personal data that is public or made manifestly public by the holder may be carried out for new purposes, only if the legitimate and specific purposes for the new processing and the preservation of the rights of the holder are observed, as well as the grounds and principles provided for in that Law. *Ibid.*

19. The ANPD is, in light of article 5, XIX, of the LGPD, the public administration body responsible for overseeing, implementing and monitoring compliance with the Law throughout the national territory. *Ibid.*

20. The Python programming language is an example of a facilitator in these processes. See ASHRAF, Rasha. *Scraping EDGAR with Python*. Journal of Education for Business. United Kingdom, London, v. 92, no. 4, pp. 179-185, May, 2017.

21. SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Civil Rights Framework for the Internet: construction and application*. Juiz de Fora: Edit, 2016, p. 125.

22. TALIAFERRO, Jocelyn; HEDADJI, Fatima; DULING, Emma. *Web Scraping as a Data Collection Strategy: the pitfalls and pitfalls*. Social Sciences & Humanities Open. Netherlands, Amsterdam. In press.

ria for the creation and aggregation of value, extracted from scraping: the practice has already been used, for example, to monitor competitors' prices and to integrate and compare product prices, which has strengthened the judicialization in the area and the contestation of these operations.<sup>23</sup> There is even news of the use of data scraping on the Internet for activities *spam*, cyber scams, fraud, denial of service attacks, sales of facial images to law enforcement agencies and election manipulation.<sup>24</sup>

At the same time, the *scraping* of large-scale information on the Internet has become equally critical for training certain AI models, such as generative artificial intelligence<sup>25</sup> or general purpose systems.<sup>26</sup>

We are talking here, in fact, not only about *web scraping* of personal data, but also of the content of books,<sup>27</sup> news and journalistic articles – a framework that evokes additional discussions and impediments related to copyright and related rights.<sup>28</sup> Scraping therefore becomes a “convenient”, albeit criticized, method for obtaining raw materials for the development of AI systems.<sup>29</sup>

The construction of obstacles via intellectual property for the training of these models can represent a relevant challenge for system developers.<sup>30</sup> After all, the business model that has prevailed with the *web scraping* is the feeding of AI with considerable amounts of information, facilitated by recent technological advances, so that the models can base and form their decision patterns based on the

23. For an analysis of court cases involving companies such as Amazon, Walmart, eBay, LinkedIn, Ticketmaster and Southwest Airlines, see GOODYEAR, Michael. *Circumscribing the Spider: Trademark Law and the edge of data scraping*. Kansas Law Review. USA, Kansas, v. 70, n. 2, pp. 295-328, Dec., 2021.

24. PARKS, Andrew. *Unfair Collection: reclaiming control of publicly available personal information from internet data scrapers*. Michigan Law Review. USA, Michigan, v. 120, no. 5, pp. 913-945, Mar., 2022.

25. Generative AI was defined in article 4, IV, of the latest version of Brazilian Bill No. 2,338, of 2023, as an AI model specifically designed to generate or significantly modify, with different degrees of autonomy, texts, images, audios, videos or codes. *software*. BRAZIL. *Bill No. 2,338 of 2023. Provides for the development, promotion, ethical and responsible use of artificial intelligence based on the centrality of the human person*. Brasilia: National Congress, 2024.

26. The European AI Regulation defines general-purpose systems as AI models, including those trained on large amounts of data through self-supervision at scale, that exhibit significant generality and are capable of competently performing a wide range of distinct tasks, regardless of the form in which they are placed on the market, and that can be integrated into a variety of systems or applications, with the exception of models used as prototypes prior to circulation on the market. EU. *Artificial Intelligence Act, locus citatum*, article 3, no. 63.

27. THE GLOBE. *Writers Sue OpenAI for Using Works to Train ChatGPT Without Permission*. O Globo, Rio de Janeiro, July 20, 2023.

28. GRYNBAUM, Michael; Mac, Ryan. *The Times Sues OpenAI and Microsoft Over AI Use of Copyrighted Work*. The New York Times. USA, New York, December 27, 2023.

29. AMARIKWA, Melany. *Internet Openness at Risk: generative AI's impact on data scraping*. Richmond Journal of Law & Technology. USA, Virginia, v. 30, no. 3, pp. 533-589, May, 2024, p. 538.

30. DELACROIX, Sylvie. *Sustainable Data Rivers? Critical AI*. USA, North Carolina, 2024. In press.

data accessed, which is why it is stated that “any algorithm is only as good as the data it is based on”.<sup>31</sup>

Beyond a copyright concern, however, the training of AI systems often proceeds from the collection of personal data on a large scale from the Internet,<sup>32</sup> which opens up a complementary debate and analysis, with specific restrictions on scraping in national territory, given that the LGPD ensures that every natural person has ownership of their personal data and the guarantee of the fundamental rights of freedom, intimacy and privacy.<sup>33</sup>

## 2. Data Protection Compatibility with the Web Scraping

The protection of personal data has been described for years as a fundamental right,<sup>34</sup> even before its express inclusion in the Constitution.<sup>35</sup> This definition sought to strike a balance with other related rights – such as privacy, information and transparency –, in addition to a definition that would simultaneously privilege the insertion of personal data into the market, without this information being linked to mere legal assets owned by its holders.<sup>36-37</sup> It is true that personal data can be converted into valuable information for economic activities, so it would be reasonable to consider the advent of the LGPD as a reinforcement of self-determination.

31. DONEDA, Danilo et al. *Initial Considerations on Artificial Intelligence, Ethics and Personal Autonomy*. Think. Fortaleza, v. 23, no. 4, pp. 1-17, Oct./Dec., 2018, p. 5.

32. The literature argues that although personal data is made public by the data subject *online*, there must be reasonableness in the collection and processing of this information. See PARKS, Andrew. *Unfair Collection: reclaiming control of publicly available personal information from internet data scrapers*, *locus citatum*.

33. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*, article 17. For a critical analysis of article 17 of the LGPD, see FRAZÃO, Ana. *Basic Rights of Personal Data Holders*. Lawyer's Magazine, v. 39, n. 144, pp. 33-46, Nov., 2019.

34. “In the qualitative *fundamental* there is an indication that these are legal situations without which the human person cannot be fulfilled, cannot coexist and, sometimes, cannot even survive”. SILVA, José Afonso da. *Positive Constitutional Law Course*. New York: Routledge, 2005, p. 178.

35. BRAZIL. Constitutional Amendment No. 115, of February 10, 2022. Amends the Federal Constitution to include the protection of personal data among the fundamental rights and guarantees and to establish the exclusive competence of the Union to legislate on the protection and processing of personal data. Brasília: National Congress, 2022.

36. The data subject is the natural person to whom the personal data refer, according to article 5, V, of the LGPD. *Idem*. *Law No. 13,709, of August 14, 2018, locus citatum*. As for the term adopted by the legislation, it is important to emphasize that the “use of the term ‘holder’, although criticized by part of the doctrine (which identifies in the reference to ownership a reference to the proprietary perspective, which is completely inadequate in matters that directly concern the human person), still seems appropriate, in view of the need to clearly identify the subjects to which the law refers.” SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. *Protection of the Human Person in the General Law on the Protection of Personal Data: between the attribution of rights and the enunciation of remedies*. Thinking. Fortaleza, v. 24, n. 3, pp. 1-22, Jul./Sept., 2019, p. 8.

37. DONEDA, Danilo. *From Privacy to Personal Data Protection: elements of the formation of the General Data Protection Law*. São Paulo: Thomson Reuters, 2020.

informative termination<sup>38</sup> and a counterpoint to “retail”<sup>39</sup> of data self-regulated by the processing agents themselves.<sup>40</sup>

Thus, Brazilian personal data protection legislation establishes an environment of proactivity,<sup>41</sup> so that the controllers<sup>42</sup> “intensify care in developing your activities.”<sup>43</sup> Internet business models that involve the processing of personal data and AI therefore need to be reconciled with the legal provisions of the LGPD,<sup>44</sup> in a creative way that also includes, on the part of the regulatory State, the guarantee of freedom of initiative for the economic activities developed *online*.<sup>45-46</sup> This is not a trivial task and Carlos Affonso Souza records one of the many setbacks related to the balance between data protection and the development of AI systems:

The LGPD states that all data subjects have the right to request the rectification and erasure of their personal data held by a company.<sup>[47]</sup> But what happens when this personal data has already been used to train a model that underpins a generative AI system? Once the model has been trained, the company can even delete the personal data stored in its systems, but the result of this training can appear in the way the model is used in a variety of applications. There are currently no viable ways to untrain a model without incurring disproportionate costs, energy expenditure and labor.<sup>48</sup>

38. Informational self-determination can be described as a “right to maintain control over one’s own information”. RODOTÀ, Stefano. *Life in the Surveillance Society: Privacy Today*. Translation: Danilo Doneda and Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 92.

39. BIONI, Bruno. *Protection of Personal Data: the role and limits of consent*. New York: Forensic, 2019, p. 48.

40. FRAZAO, Ana. *Fundamentals of Personal Data Protection – introductory notions for understanding the importance of the General Data Protection Law*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *General Law on the Protection of Personal Data and its Repercussions on Brazilian Law*. São Paulo: Thomson Reuters, 2023, pp. 21-50.

41. MORAES, Maria Celina Bodin de. *LGPD: a new proactive civil liability regime*. [Civillistica.com](http://Civillistica.com). Rio de Janeiro, v. 8, n. 3, pp. 1-6, Dec., 2019.

42. The controller is, within the meaning of article 5, VI, of the LGPD, the natural or legal person, under public or private law, who is responsible for decisions regarding the processing of personal data. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*.

43. EDSON, Carlos. *Protection of Personal Data and its Effectiveness in the Brazilian Legal System: right of access, reparation and prevention of damages*. *Journal of Liability Law*. Portugal, Coimbra, v. 3, pp. 298-315, March, 2021, p. 314.

44. LAND, Aline de Miranda Valverde; MULHOLLAND, Caitlin. *The Economic Use of Online Trackers and Identifiers of Personal Data*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *General Law on the Protection of Personal Data and its Repercussions on Brazilian Law*. São Paulo: Thomson Reuters, 2023, pp. 585-604.

45. It is worth noting that the discipline of Internet use in Brazil encompasses a principled balance between, *free example*, the protection of personal data and the freedom of business models promoted on the Internet. BRAZIL. *Law No. 12,965, of April 23, 2014, locus citatum*, article 3, III and VIII.

46. Some of the literature states, *free example*, that “it is not possible to assume that a certain way or model for the exploration of an area of economic activity on the Internet is prohibited.” SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Civil Rights Framework for the Internet: construction and application, locus citatum*, p. 48.

47. Article 18, III and IV, of the LGPD, provides as rights of the holder of personal data the request for the correction of incomplete, inaccurate or outdated data, as well as the anonymization, blocking or elimination of unnecessary, excessive data or data processed in non-compliance with the provisions of the legislation. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*.

48. SOUZA, Carlos Affonso. *Meta x ANPD: separating AI and personal data spaces will not be easy*. Universe Online, São Paulo, July 4, 2024.

In addition, one of the principles provided for in the LGPD with a direct impact on the training of AI systems is transparency:<sup>49</sup>the guarantee of clear, precise and easily accessible information about the treatment being carried out.<sup>50</sup>Therefore, despite the economic importance of the automated use of personal data,<sup>51</sup>It is unfeasible for controllers to simply not provide data subjects with information regarding the development of these activities.<sup>52</sup>

However, the complexity of the associations and correlations operated during the AI's feeding, which can even become unexpected,<sup>53</sup>It represents another challenge in terms of how to identify activities that are initially unknown or poorly understood by the controllers themselves.<sup>54-55</sup>Such a scenario poses risks for potential additional violations of the principles of purpose.<sup>56</sup>and suitability.<sup>57</sup>Consequently, the criticized mystery<sup>58</sup>of the functioning of operations has paved the way for debates on algorithmic audits that aim to uncover erroneous or imprecise decisions, illicit or abusive discrimination and damages.

49. Also present in European legislation, the Spanish data protection authority ("AEPD") states that transparency should allow data subjects to be aware of the impact associated with the use of AI solutions, so that the controller would have to provide information about the efficiency, resources and limitations of the systems. This includes, in fact, specifically indicating to the data subject whether the use of their personal data for training the AI will allow their subsequent reidentification by the models developed. SPAIN. *Adjustment to the GDPR of Treatments that Incorporate Artificial Intelligence – an introduction*. Spain, Madrid: Agencia Española de Protección de Data, 2020.

50. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*, article 6, VI.

51. It is worth noting that "the processing of information and data through algorithms can be a means of simplifying economic decisions, increasing efficiency and personalizing production, as well as expanding the possibilities of monetizing digital services through the personalization of content and digital marketing." DONEDA, Danilo *et al.* *Initial Considerations on Artificial Intelligence, Ethics and Personal Autonomy, locus citatum*, p. 4.

52. After all, without the aforementioned transparency, the data subject would not be able to request the rights provided for in the LGPD from the controller, since he would not even be aware of the existence of the processing of his personal data. Some of the literature, however, believes that trust in transparency and in a model of informative self-determination in terms of AI would be insufficient to contain damages related to systems that pose risks to human beings. See SOLOVE, Daniel; HARTZOG, Woodrow. *Kafka in the Age of AI and the Futility of Privacy as Control*. Boston University Law Review. USA, Massachusetts, v. 104, no. 4, pp. 1,021-1,042, May, 2024.

53. SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. *The Right to Explanation between Experience and its Positivation in the LGPD*. IN: MENDES, Laura Schertelet *al.* (Coords.). *Personal Data Protection Treaty*. Rio de Janeiro: Forense, 2021, pp. 243-270.

54. The LGPD requires, *free example*, that the processing agent presents information regarding the specific purpose of the activity with personal data. If consent is the applicable legal basis, it will be possible to revoke it, in the event that the holder disagrees with the new purpose. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*, article 9, I and § 2.

55. "This complexity further highlights the limitations of current privacy rights in addressing the broader implications of data use and algorithmic decision-making. Even experts struggle to understand why algorithms produce certain outcomes." [Our translation]. SOLOVE, Daniel. *Artificial Intelligence and Privacy*. Florida Law Review. USA, Florida, v. 77, n. 1, Jan., 2025. In press.

56. "[I]mplementation of processing for legitimate, specific, explicit purposes and informed to the holder, without the possibility of subsequent processing in a manner incompatible with these purposes". BRAZIL. *Law No. 13,709, of August 14, 2018, operate quoted*, article 6, I.

57. "[C]ompatibility of the processing with the purposes informed to the data subject, in accordance with the context of the processing". *Ibid.*, article 6, II.

58. PASQUALE, Frank. *The Black Box Society: the secret algorithms that control money and information*. USA, Massachusetts: Harvard University Press, 2015.

us to the holder.<sup>59-60</sup> On the other hand, the notion of a prior definition of the purposes of the processing was described as an “old idea” and that it could oppose the potential for AI systems to identify new purposes, including those that are beneficial to the data subjects.<sup>61</sup>

Scraping techniques, used by developers to collect information on the Internet, furthermore, prove to be another component in the discussion of the threshold between AI and personal data protection: for some, the fact that data subjects' information is publicly available *online* should not constitute a “loophole” for conducting collection, shared use and other processing activities without due transparency and for purely commercial purposes.<sup>62</sup> On the contrary, the absence of specific, concise, understandable and easily accessible information<sup>63</sup> about the *scraping* results in the holder being prevented from exercising his rights to oppose the transaction.<sup>64</sup>

Thus, the European Data Protection Board (“EDPB”) indicates that scraping information presents particular risks to the rights and fundamental freedoms of natural persons,<sup>65</sup> and the European Data Protection Supervisor (“EDPS”) argues that the *web scraping* intended for AI training purposes may be non-compliant with personal data protection principles.<sup>66</sup>

However, a potential incompatibility does not mean that scraping should be subject to a “categorical ban”, making it difficult to train AI,

59. MITTELSTADT, Brent et al. *The Ethics of Algorithms: mapping the debate*. Big Data & Society. USA, California, v. 3, n. 2, Jul./Dec., 2016.

60. The LGPD also provides that the ANPD may conduct an audit to verify discriminatory aspects in the automated processing of personal data, in compliance with commercial and industrial secrecy, if the controller does not provide – when requested – clear and adequate information regarding the criteria and procedures used for a given automated decision. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*, article 20, § 2. For a detailed understanding of the meaning of automated processing of personal data, see VERONESE, Alexandre. *The Rights of Explanation and Objection to Fully Automated Decisions: Comparing the European Union's GDPR with the Brazilian LGPD*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *General Law on the Protection of Personal Data and its Repercussions on Brazilian Law*. São Paulo: Thomson Reuters, 2023, pp. 377-408.

61. HILDEBRANDT, Mireille. *Slaves of macrodata. Or no?* Internet, Law and Politics Magazine. Spain, Barcelona, v. 17, pp. 7-44, Nov., 2013, p. 19.

62. PARKS, Andrew. *Unfair Collection: reclaiming control of publicly available personal information from internet data scrapers*, locus citatum, p. 922.

63. Guidelines from the French Data Protection Authority (“CNIL”). FRANCE. *La Réutilisation des Données Publiquement Accessibles En Ligne à des Fins de Démarchage Commercial*. France, Paris: Commission Nationale de l'Informatique et des Libertés, 2020.

64. The Polish Data Protection Authority (“UODO”) applied this understanding when fining the company Bisnode for failing to directly inform data subjects about its data scraping practices. On the grounds that person-to-person notification would involve “disproportionate efforts”, the data controller had merely mentioned the operation in its privacy policy – which was considered insufficient by the regulator in the specific case. POLAND. *NSA Przyznał Rację UODO ws. Decyzji dotyczącej Pierwszej Kary Nałożonej przez Organ Nadzorczy*. Poland, Warsaw: Urząd Ochrony Danych Osobowych, 2023.

65. EU. *Report of the work undertaken by the ChatGPT Taskforce*. European Union: European Data Protection Board, 2024.

66. *Idem*. *Generative AI and the EUDPR. First EDPS Guidelines for ensuring data protection compliance when using Generative AI systems*. European Union: European Data Protection Supervisor, 2024.

although there is a need here to apply the legal data protection requirements proportionately, so that they do not lose their meaning if a reconciliation between the two fields is not envisaged.<sup>67</sup> Therefore, while preventing scraping would bring considerable cost to developers, since basic search and information retrieval functions “depend” on the *web scraping*,<sup>68</sup> It is true that the fundamental right to data protection must also be taken seriously and cannot be seen as a mere obstacle to the economic activities of data processing agents.

In conclusion, it is noted that data protection legislation appears, ultimately, to conflict to some extent with AI operations contextualized within a framework of *Big Data*,<sup>69</sup> which risks inhibiting innovation and new technological benefits to society,<sup>70</sup> while nation states intensify strategic competition and the relaxation of interventionism to prioritize development in the area of AI.<sup>71</sup>

Brazil has chosen, however, to practically mirror Europe's more protective regulatory framework,<sup>72-73</sup> so that the full applicability of the LGPD is maintained for AI training via *web scraping*.<sup>74</sup> It is also worth noting that Brazilian personal data protection legislation only authorizes the subsequent processing of public personal data or data made manifestly public by its holder when legitimate and specific purposes are guaranteed for the new activity and the preservation of the holder's rights, as well as the foundations and principles provided for in the LGPD.<sup>75</sup>

67. SOLOVE, Daniel; HARTZOG, Woodrow. *The Great Scrape: the clash between scraping and privacy*, p. 5. In press.

68. “Banning scraping would have a huge financial and social cost, since many basic functions of the Internet and AI, such as information search and retrieval, depend on *scraping*. Scraping can be a valuable tool to empower people, promote competition, and hold industry and government accountable for their own data practices.” [Our translation]. *Ibid.*, p. 52.

69. ZARSKY, Tal. *Incompatible: the GDPR in the age of Big Data*. Seton Hall Law Review. USA, New Jersey, v. 47, no. 4, pp. 995-1,020, Aug., 2017.

70. Carlos Affonso Souza, Christian Perrone and Eduardo Magrani argue that “the prohibition of the use of mechanisms that automate decisions or even artificial intelligence, *machine learning* and the like, would be the same as condemning humans to the use of horses after the invention of the combustion engine.” SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. *The Right to Explanation between Experience and its Positivation in the LGPD, locus citatum*, p. 246.

71. For a mapping of the different regulatory proposals on AI, not restricted to European legislation, see ITS. *How to Regulate Artificial Intelligence*. Rio de Janeiro: Rio Institute of Technology and Society, 2024.

72. EU. *Artificial Intelligence Act, locus citatum*.

73. For an understanding of the influences of European legislation around the world, see BRADFORD, Anu. *The Brussels Effect: how the European Union rules the world*. United Kingdom, Oxford: Oxford University Press, 2020.

74. According to article 30, III, of Brazilian Bill No. 2,338, of 2023, the developer of a general-purpose AI system must, before making it available on the market for commercial purposes, only process and incorporate data sets collected and treated in accordance with legal requirements, subject to adequate data governance, in particular in accordance with the LGPD. In addition, article 61, § 3, of the Bill determines that text and data mining activities involving personal data will be subject to the provisions of the LGPD. BRAZIL. *Bill No. 2,338 of 2023, locus citatum*. Similarly, European regulation indicates that the design, development and use of AI systems involving personal data remain subject to the legislation governing the protection of such information. EU. *Artificial Intelligence Act, locus citatum*, recital 10 and Article 2, paragraph 7.

75. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*, article 7, § 7.

The path that the country seems to be taking certainly prioritizes the fundamental right to the protection of personal data, with regard to the development of systems that use this information as raw material – although there is still no consensus on the appropriate regulatory choice to safeguard “against the problems that AI can bring.”<sup>76</sup>In any case, the current scenario converges towards a legislative foundation centered on the human person,<sup>77</sup>at the same time that technology companies support certain economic practices in data scraping *online*, which makes the continuity of the *scraping* a true “enigma”.

78

In order to better outline the contours and challenges of making Internet scraping viable, the next chapter of the research investigates the possibilities of substantiating the *web scraping* in one of the legal hypotheses provided for in the LGPD, given that processing agents need to select one of the bases contained in the legislation as a condition for initiating any operation with personal data,<sup>79</sup> including collection for training AI systems.

### 3. In Search of the Legal Hypothesis Applicable to Training of AI

The selection of an authorizing hypothesis is one of the “requirements” set out in the LGPD to guarantee the lawfulness of a processing activity involving personal data.<sup>80</sup>In practice, the controller must assess the specific purpose and context for which it seeks to operate the information, in order to make it compatible with one of the normative statements described in the legislation.<sup>81</sup>In Brazil, in fact, it is worth noting that there is no hierarchy between the bases, “as they are all horizontally listed” in the LGPD.<sup>82</sup>

However, there is a segmentation between the hypotheses that support the processing of sensitive personal data.<sup>83</sup>(article 11, LGPD) and non-sensitive (article

76. READ, Ronaldo. *What does Brazil want from Artificial Intelligence?* April 7, 2024.

77. BRAZIL. Bill No. 2,338 of 2023, *locus citatum*, article 2, I.

78. SOBEL, Benjamin. *A New Common Law of Web Scraping*. Lewis & Clark Law Review. USA, Idaho, v. 25, no. 1, pp. 147-207, Mar., 2021, p. 150.

79. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Processing of Personal Data in the LGPD: study on the legal bases*. *Civilis - tica.com*. Rio de Janeiro, v. 9, n. 1, pp. 1-38, May, 2020.

80. SOUZA, Carlos Affonso; VIOLA, Mario; STANDARD, Vinicius. *Initial Considerations on the Controller's Legitimate Interests in the General Personal Data Protection Law*. Public Law. Brasília, v. 16, n. 90, pp. 109-131, Dec., 2019, p. 110.

81. UNITED KINGDOM. *A Guide to Lawful Basis*. United Kingdom, Wilmslow: Information Commissioner's Office, 2022.

82. BIONI, Bruno. *Protection of Personal Data: the role and limits of consent*, *locus citatum*, p. 188.

83. Personal data regarding racial or ethnic origin, religious belief, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sexual life, genetic or biometric data, when linked to a natural person, are considered sensitive personal data, according to article 5, II, of the LGPD. BRAZIL. *Law No. 13,709, of August 14, 2018*, *locus citatum*.

7th, LGPD), since the former comprise a special category protected by the Law, which establishes stricter mechanisms to authorize controllers' activities with that information, in the face of potential improper use for illicit or abusive discrimination and other types of violations of human rights.<sup>84</sup>

Here, a first plausible conception is the argument that the collection of personal data via *web scraping* for the purpose of training AI systems is not intended or intended<sup>85</sup> the operation of sensitive information or the causing of damage to the holders, but only the guarantee, in the logic of *Big Data*, of the inputs needed to feed the systems. The EDPB states, in this line, that the simple fact that a processing agent carries out a large-scale activity does not automatically mean that there is a purpose to infer<sup>86</sup> sensitive data, in the event that this information is also collected during the operation.<sup>87</sup> Still in this context of *scraping* on the Internet, it can be said that it would be difficult to conduct a detailed analysis of each piece of information processed in order to detect the presence of sensitive data in the scraped set.<sup>88</sup>

On the other hand, it is equally possible to argue that scraping processing to train AI systems should be based on a more protective basis, if sensitive personal data is collected over the course of the process. *scraping*, regardless of the purpose and potential for harm of the activity.<sup>89</sup>

The French data protection authority (“CNIL”) points out, however, that if the controller implements measures to automatically exclude the collection of

84. TEFFÉ, Chiara Spadaccini de. *Sensitive Personal Data: qualification, treatment and good practices*. Indaiatuba: Foco, 2022. The same author also argues that: “[a]s artificial intelligence has been frequently used for decision-making, people’s lives become increasingly vulnerable to illicit or abusive discriminatory treatments, such as in situations involving analysis of the probability of committing crimes, health protection, granting of credit and participation in job selection processes, for example.” *Idem*. *The Special Category of Sensitive Data: Fundamentals and Outlines*. IN: SCHREIBER, Anderson; MONTEIRO FILHO, Carlos Edison do Rêgo; OLIVA; Milena Donato (Orgs.). *Problems of Civil Law*. Rio de Janeiro: Forense, 2021, pp. 97-123, p 105.

85. For an overview of potential uses of AI for the purpose of collecting or inferring sensitive personal data, see ARTICLE 19. *Privacy and Freedom of Expression in the Age of Artificial Intelligence*. United Kingdom, London: Article 19, 2018.

86. Article 11, § 1, of the LGPD provides that the particular protection of sensitive data is applicable to any processing of personal data that reveals sensitive personal data and that may cause harm to the holder. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*.

87. EU. *Guidelines 8/2020 on the Targeting of Social Media Users*. European Union: European Data Protection Board, 2021. The reasoning seems similar to that used in the literature when describing the capture, via closed-circuit television (“CCTV”), of the image of a person dressed in religious attire: since the cameras are used to ensure the security of the environment, without collecting biometric data or to identify people’s religious beliefs, it would not make sense to impose the justification for processing on a more protective basis linked to sensitive data. See NGUYEN, Alexander. *Videoüberwachung in Sensitiven Bereichen*. *Datenschutz und Datensicherheit*. Germany, Bonn, v. 35, no. 10, pp. 715- 717, Oct., 2011.

88. EU. *Report of the work undertaken by the ChatGPT Taskforce, locus citatum*.

89. In this scenario, it should be reiterated that it would be essential to identify a specific, more restrictive legal hypothesis before proceeding with the treatment. See UNITED KINGDOM. *Guidance on AI and Data Protection*. United Kingdom, Wilmslow: Information Commissioner's Office, 2023. It should also be noted that European legislation authorizes activities with sensitive data aimed at “ensuring the detection and correction” of biases related to AI systems, subject to additional requirements to guarantee the protection of data subjects. EU. *Artificial Intelligence Act, locus citatum*, article 10, paragraph 5.

sensitive data through scraping, incidental and residual operations with this information, not supported by a more restrictive basis, would no longer be illegal in these cases.<sup>90</sup>

In the national context, among the main hypotheses contained in the LGPD and related to the processing of non-sensitive data for training AI systems, for commercial purposes and via *web scraping*, only consent and legitimate interest stand out.<sup>91</sup> More restrictively, only specific and highlighted consent, in theory, could justify scraping *online* for commercial AI training with sensitive personal data.<sup>92</sup> This is because the specific purpose of improving the systems does not seem to be confused with the execution of a possible contract between the *scraper* and the holder, nor with the credit analysis possibly conducted by a *bureau* for the protection of the credit itself – other hypotheses that could be presented by the processing agent in order to support the scraping activity, but which would require a greater argumentative effort in this direction, as they are related to exclusive and unusual cases.<sup>93</sup>

At the same time, the legal basis for consent itself, which consists of the data subject providing a free, informed and unequivocal statement, by which he/she agrees to the processing of his/her personal data for a specific purpose,<sup>94</sup> faces challenges in the framework under analysis, since – as mentioned above – the holder may not understand the purposes of certain “opaque” operations conducted for AI training,<sup>95–96</sup> nor revoke your authorization and request the deletion of data that has already been fed

90. FRANCE. *IA: ensure that the trait is permitted – define a legal basis*. France, Paris: Commission Nationale de l'Informatique et des Libertés, 2024.

91. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*, article 7, I and IX.

92. *Ibid.*, article 11, I.

93. For an analysis of the legal basis for the execution of a contract and the regular exercise of rights under a contract, see PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. *Digital Compliance and LGPD*. São Paulo: Thomson Reuters, 2021. For a specific view on credit protection and LGPD, see OLIVA, Milena Donato; VIÉGAS, Franciso de Assis. *Data Processing for Granting Credit*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *General Law on the Protection of Personal Data and its Repercussions on Brazilian Law*. São Paulo: Thomson Reuters, 2023, pp. 547-584.

94. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*, article 5, XII. For a detailed analysis of the legal hypothesis of consent, see TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. *Consent to the Circulation of Personal Data*. *Brazilian Journal of Civil Law*. Belo Horizonte, v. 25, n. 3, pp. 83-116, Nov., 2020; and BIONI, Bruno. *Protection of Personal Data: the role and limits of consent, locus citatum*.

95. MITROU, Lilian. *Data Protection, Artificial Intelligence and Cognitive Services: is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?* Social Science Research Network. USA, New York, pp. 1-90, Jun., 2019, p. 70; and UNITED KINGDOM. *Guidance on AI and Data Protection, locus citatum*.

96. This concern is even more relevant when it comes to consent for the processing of sensitive data, since the manifestation in these cases needs to be specific. According to the literature, “[s]pecific should be understood as a consent expressed in relation to concrete purposes and clearly determined by the controller and before the processing of the data, with there also being, and with greater emphasis, the obligations of granularity.” TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Processing of Personal Data in the LGPD: study on the legal bases, locus citatum*, p. 34.

the systems,<sup>97</sup> to the detriment of the requirements of free, informed and unambiguous consent. Furthermore, obtaining individual consent from each data subject seems unfeasible and a disproportionately costly effort in light of the activities of *web scraping*, which involve the large-scale collection of personal data.<sup>98</sup>

There would therefore remain only the legal hypothesis of the legitimate interest of the controller, inapplicable to the processing of sensitive personal data, and described by the Dutch data protection authority (“AP”), albeit critically, as the only adequate basis for scraping.<sup>online</sup><sup>99</sup> Legitimate interest is the “authorizing hypothesis designed precisely to put an end to situations in which seeking the consent of the holder could even become an obstacle to the regular exploitation of personal data”:<sup>100</sup> its correct use “provides and increases new business models and diverse commercial strategies”.<sup>101</sup>

However, this legal basis needs to be weighed on a case-by-case basis in light of the fundamental rights and freedoms of the data subject,<sup>102</sup> also susceptible to inspection by the National Authority, which has already presented a test model for the controller to balance the interests of the processing with possible undesirable impacts, which must be read in accordance with the LGPD.<sup>103</sup> This means that purely economic activities of processing agents need to be functionalized, to the benefit of the human person and the protection of their personal data.<sup>104</sup>

Finally, regarding data processing for training systems via *web scraping*, the hypothesis of legitimate interest appears as a flexible solution to justify the operation, as it allows for a balance between the commercial and social benefits of AI and the rights and interests of the holders.<sup>105</sup>

However, it is important that the controller adopts concrete measures

97. UNITED KINGDOM. *How to Use AI and Personal Data Appropriately and Lawfully*. United Kingdom, Wilmslow: Information Commissioner's Office, 2022; and SOUZA, Carlos Affonso. *Meta x ANPD: separating AI and personal data spaces will not be easy, locus citatum*.

98. SOLOVE, Daniel. *Artificial Intelligence and Privacy, locus citatum*; SOLOVE, Daniel; HARTZOG, Woodrow. *The Great Scrape: the clash between scraping and privacy, locus citatum*; and NOVELLI, Claudio et al.. *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*. ArXiv Working Paper No. 2401.07348. USA, New York, March, 2024.

99. NETHERLANDS. *Handreiking Scraping door Particulieren in Private Organizations*. Netherlands, The Hague: Autoriteit Persoonsgegevens, 2024.

100. SOUZA, Carlos Affonso; VIOLA, Mario; STANDARD, Vinicius. *Initial Considerations on the Controller's Legitimate Interests in the General Personal Data Protection Law*. Public Law. Brasília, v. 16, n. 90, pp. 109-131, Dec., 2019, p. 110.

101. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Processing of Personal Data in the LGPD: study on the legal bases, locus citatum*, p. 19.

102. BRAZIL. *Law No. 13,709, of August 14, 2018, locus citatum*, articles 7, IX, and 10.

103. BRAZIL. *Legal Hypotheses for the Processing of Personal Data – legitimate interest*. Brasília: National Data Protection Authority, 2024.

104. BUCAR, Daniel; VIOLA, Mario. *Processing of Personal Data for the “Legitimate Interest of the Controller”: first questions and notes*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *General Law on the Protection of Personal Data and its Repercussions on Brazilian Law*. São Paulo: Thomson Reuters, 2023, pp. 453-472.

105. UNITED KINGDOM. *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. United Kingdom, Wilmslow: Information Commissioner's Office, 2017, p. 34.

robust security and risk mitigation measures<sup>106</sup>—such as pseudonymization, the selection of criteria to collect only information necessary for training,<sup>107</sup>and the implementation of mechanisms to oppose the activity (“*opt-out*”)<sup>108</sup>—, in addition to providing transparent and constantly updated information regarding the treatment,<sup>109</sup>without which the aforementioned legal basis will also remain inadequate and in disharmony with the LGPD, with the ANPD guidelines<sup>110</sup>and with best practices in terms of privacy and personal data protection.

## Final Considerations

This article sought to identify the most appropriate legal basis to support the training of AI systems with personal data, through practices of *web scraping*. From an analysis of information scraping in the era of *Big Data*, it was pointed out how the LGPD inaugurated a notable scenario of privilege for the human person, so that the economic activities of the controllers began to be considered *vis-à-vis* to the various requirements and obligations present in the governing legislation. In this complex situation, it is up to the ANPD to deliberate in a conclusive manner on the interpretation of the LGPD, while balancing scraping practices *online* with the protection of personal data, and while also positioning itself as the competent authority to coordinate the National System of Regulation and Governance of Artificial Intelligence. This is a challenging task and will require special attention from the Authority, which already contemplates the *web scraping* and AI in its map of priority themes and regulatory agenda.

Finally, it is worth noting that the selection of a legal hypothesis appropriate to a processing activity does not guarantee, in itself, the compliance of the operation with the LGPD, which is why it is important that controllers continue to implement good practices to safeguard the rights of the holder and the principles of

106. SPAIN. *Adjustment to the GDPR of Treatments that Incorporate Artificial Intelligence – an introduction*, *locus citatum*.

107. FRANCE. *IA: ensure that the trait is legal – define a legal basis*, *locus citatum*. Pseudonymization is the processing by which data loses the possibility of association, directly or indirectly, with an individual, except through the use of additional information kept separately by the controller in a controlled and secure environment. Furthermore, the principle of necessity (article 6, III, LGPD) deserves reinforcement when processing is based on legitimate interest. BRAZIL. *Law No. 13,709, of August 14, 2018*, *locus citatum*, articles 10, § 1, and 13, § 4.

108. UNITED KINGDOM. *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, *locus citatum*, p. 34.

109. ITALY. *ChatGPT: Guarantees privacy, provisionally limited if OpenAI adopts the richest mix*. Italy, Rome: Garante per la Protezione dei Dati Personali, 2023. The LGPD also determines that the controller must adopt measures to guarantee the transparency of data processing based on legitimate interest. BRAZIL. *Law No. 13,709, of August 14, 2018*, *locus citatum*, articles 10, § 2.

110. The Authority also recommends proving the legitimate expectations of data subjects regarding the processing, providing mechanisms for the exercise of rights, respecting the principle of necessity, developing a three-phase balancing test, as well as paying greater attention to the processing of data of children and adolescents. BRAZIL. *Legal Hypotheses for the Processing of Personal Data – legitimate interest*, *locus citatum*.

principles and foundations provided for in the Law. Only with cooperation between the regulated agents and the ANPD will it be possible to ensure the freedom of business models promoted on the Internet, in a creative balance with the protection of privacy and personal data in Brazil, towards the development, promotion, ethical and responsible use of AI, based on the centrality of the human person.

## References

AARONSON, Susan Ariel. *Data Dysphoria: the governance challenge posed by Large Language Models*. Institute for International Economic Policy Working Paper no. 2023-07. USA, Washington, DC., Aug., 2023.

AMARIKWA, Melany. *Internet Openness at Risk: generative AI's impact on data scraping*. Richmond Journal of Law & Technology. USA, Virginia, v. 30, no. 3, pp. 533-589, May, 2024.

ARTICLE 19. *Privacy and Freedom of Expression in the Age of Artificial Intelligence*. United Kingdom, London: Article 19, 2018.

ASHRAF, Rasha. *Scraping EDGAR with Python*. Journal of Education for Business. United Kingdom, London, v. 92, no. 4, pp. 179-185, May, 2017.

BALKIN, Jack. *Free Speech in the Algorithmic Society: big data, private governance, and new school speech regulation*. University of California, Davis, Law Review. USA, California, v. 51, n. 615, pp. 1,149-1,210, Sep., 2017.

BAROCAS, Solon; SELBST, Andrew. *Big Data's Disparate Impact*. California Law Review. USA, California, v. 104, no. 3, pp. 671-732, Jun., 2016.

BARROSO, Luis Roberto; MELLO, Patricia Perrone Campos. *Artificial intelligence: promises, risks and regulation. Something new under the sun*. Law and Praxis Journal. Rio de Janeiro, 2024. In press.

BIONI, Bruno. *Protection of Personal Data: the role and limits of consent*. New York: Forensic, 2019.

BOSTROM, Nick. *Superintelligence: Paths, Dangers and Strategies for a New World*. Translation: Aurelio Monteiro, Clemente Penna, Fabiana Monteiro and Patricia Geremias. Rio de Janeiro: Darkside, 2018.

BRADFORD, Ann. *The Brussels Effect: how the European Union rules the world*. United Kingdom, Oxford: Oxford University Press, 2020.

BRAZIL. *Constitutional Amendment No. 115, of February 10, 2022. Amends the Federal Constitution to include the protection of personal data among the fundamental rights and guarantees and to establish the exclusive competence of the Union to legislate on the protection and processing of personal data..* Brasilia: National Congress, 2022.

BRAZIL. *Legal Hypotheses for the Processing of Personal Data – legitimate interest*. Brasilia: National Data Protection Authority, 2024.

BRAZIL. *Law No. 12,965 of April 23, 2014. Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil..* Brasilia: National Congress, 2014.

BRAZIL. *Law No. 13,709 of August 14, 2018. General Personal Data Protection Law (LGPD)*. Brasilia: National Congress, 2018.

BRAZIL. *Bill No. 2,338 of 2023. Provides for the development, promotion, ethical and responsible use of artificial intelligence based on the centrality of the human person*. Brasilia: National Congress, 2024.

BRAZIL. *Vote no. 11/2024/DIR-MW/CD*. Brasilia: National Data Protection Authority, 2024.

BUCAR, Daniel; VIOLA, Mario. *Processing of Personal Data for the “Legitimate Interest of the Controller”: first questions and notes*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *General Law on the Protection of Personal Data and its Repercussions on Brazilian Law*. São Paulo: Thomson Reuters, 2023, pp. 453-472.

DELACROIX, Sylvie. *Sustainable Data Rivers? Critical AI*. USA, North Carolina, 2024. In press.

DONEDA, Danilo. *From Privacy to Personal Data Protection: elements of the formation of the General Data Protection Law*. São Paulo: Thomson Reuters, 2020.

DONEDA, Danilo; MENDES, Laura Schertel; SOUZA, Carlos Affonso Pereira de; ANDRADE, Norberto. *Initial Considerations on Artificial Intelligence, Ethics and Personal Autonomy*. *Thinking*. Fortaleza, v. 23, n. 4, pp. 1-17, Oct./Dec., 2018.

SPAIN. *Adjustment to the GDPR of Treatments that Incorporate Artificial Intelligence – an introduction*. Spain, Madrid: Agencia Española de Protección de Data, 2020.

FRANCE. *IA: ensure that the trait is permitted – define a legal basis*. France, Paris: Commission Nationale de l'Informatique et des Libertés, 2024.

FRANCE. *La Réutilisation des Données Publiquement Accessibles En Ligne à des Fins de Démarchage Commercial*. France, Paris: Commission Nationale de l'Informatique et des Libertés, 2020.

FRASAO, Ana. *Basic Rights of Personal Data Holders*. *Lawyer's Magazine*, v. 39, n. 144, pp. 33-46, Nov., 2019.

FRASAO, Ana. *Fundamentals of Personal Data Protection – introductory notions for understanding the importance of the General Data Protection Law*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *General Law on the Protection of Personal Data and its Repercussions on Brazilian Law*. São Paulo: Thomson Reuters, 2023, pp. 21-50.

GOODYEAR, Michael. *Circumscribing the Spider: Trademark Law and the edge of data scraping*. *Kansas Law Review*. USA, Kansas, v. 70, n. 2, pp. 295-328, Dec., 2021.

GRYNBAUM, Michael; MAC, Ryan. *The Times Sues OpenAI and Microsoft Over AI Use of Copyrighted Work*. *The New York Times*. USA, New York, December 27, 2023.

HILDEBRANDT, Mireille. *Slaves of macrodata. Or no?* Internet, Law and Politics Magazine. Spain, Barcelona, v. 17, pp. 7-44, Nov., 2013.

NETHERLANDS. *Handreiking Scraping door Particulieren in Private Organizations*. Netherlands, The Hague: Autoriteit Persoonsgegevens, 2024.

ITALY. *ChatGPT: Guarantees privacy, provisionally limited if OpenAI adopts the richest mix*. Italy, Rome: Garante per la Protezione dei Dati Personali, 2023.

ITS. *How to Regulate Artificial Intelligence?* Rio de Janeiro: Rio Institute of Technology and Society, 2024.

READ, Ronaldo. *What does Brazil want from Artificial Intelligence?* April 7, 2024.

MCCARTHY, John; MINSKY, Marvin; ROCHESTER, Nathaniel; SHANNON, Claude. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. USA, New Hampshire: Dartmouth College, 1955.

MITROU, Lilian. *Data Protection, Artificial Intelligence and Cognitive Services: is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?* Social Science Research Network. USA, New York, pp. 1-90, June, 2019, p. 70.

MITTELSTADT, Brent; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. *The Ethics of Algorithms: mapping the debate*. Big Data & Society. USA, California, v. 3, n. 2, Jul./Dec., 2016.

MONTEIRO FILHO, Carlos Edison do Rêgo. *Protection of Personal Data and its Effectiveness in the Brazilian Legal System: right of access, reparation and prevention of damages*. Journal of Liability Law. Portugal, Coimbra, v. 3, pp. 298-315, March, 2021.

MORAES, Maria Celina Bodin de. *LGPD: a new proactive civil liability regime*. [Civiltica.com](http://Civiltica.com). Rio de Janeiro, v. 8, n. 3, pp. 1-6, Dec., 2019.

NEWELL, Allen. *Intellectual Issues in the History of Artificial Intelligence*. IN: MACHLUP, Fritz; MANSFIELD, Una (Eds.). *The Study of Information: interdisciplinary messages*. USA, New York: Wiley, 1983, pp. 187-294.

NGUYEN, Alexander. *Videoüberwachung in Sensitiven Bereichen*. Datenschutz und Datensicherheit. Germany, Bonn, v. 35, no. 10, pp. 715-717, Oct., 2011.

NOVELLI, Claudio; CASOLARI, Federico; HACKER, Philipp; SPEDICATO, Giorgio; FLORIDI, Luciano. *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*. ArXiv Working Paper No. 2401.07348. USA, New York, March, 2024.

THE GLOBE. *Writers Sue OpenAI for Using Works to Train ChatGPT Without Permission*. O Globo, Rio de Janeiro, July 20, 2023.

OLIVA, Milena Donato; VIÉGAS, Franciso de Assis. *Data Processing for Granting Credit*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *General Law for the Protection of*

Protection of Personal Data and its Repercussions on Brazilian Law. São Paulo: Thomson Reuters, 2023, pp. 547-584.

COLLINS, Philip; *Digital Compliance and LGPD*. São Paulo: Thomson Reuters, 2021.

PARKS, Andrew. *Unfair Collection: reclaiming control of publicly available personal information from internet data scrapers*. Michigan Law Review. USA, Michigan, v. 120, no. 5, pp. 913-945, Mar., 2022.

PASQUALE, Frank. *The Black Box Society: the secret algorithms that control money and information*. USA, Massachusetts: Harvard University Press, 2015.

POLAND. *NSA Przyznał Rację UODO ws. Decyzji dotyczącej Pierwszej Kary Nałożonej przez Organ Nadzorczy*. Poland, Warsaw: Urząd Ochrony Danych Osobowych, 2023.

UNITED KINGDOM. *A Guide to Lawful Basis*. United Kingdom, Wilmslow: Information Commissioner's Office, 2022.

UNITED KINGDOM. *Guidance on AI and Data Protection*. United Kingdom, Wilmslow: Information Commissioner's Office, 2023.

UNITED KINGDOM. *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. United Kingdom, Wilmslow: Information Commissioner's Office, 2017.

UNITED KINGDOM. *How to Use AI and Personal Data Appropriately and Lawfully*. United Kingdom, Wilmslow: Information Commissioner's Office, 2022.

RODOTÀ, Stefano. *Life in the Surveillance Society: Privacy Today*. Translation: Danilo Doneda and Luciana Doneda. Rio de Janeiro: Renovar, 2008.

SILVA, Jose Afonso da. *Positive Constitutional Law Course*. New York: Routledge, 2005.

SOBEL, Benjamin. *A New Common Law of Web Scraping*. Lewis & Clark Law Review. USA, Idaho, v. 25, no. 1, pp. 147-207, Mar., 2021

SOLOVE, Daniel. *Artificial Intelligence and Privacy*. Florida Law Review. USA, Florida, v. 77, n. 1, Jan., 2025. In press.

SOLOVE, Daniel; HARTZOG, Woodrow. *The Great Scrape: the clash between scraping and privacy*. In press.

SOLOVE, Daniel; HARTZOG, Woodrow. *Kafka in the Age of AI and the Futility of Privacy as Control*. Boston University Law Review. USA, Massachusetts, v. 104, no. 4, pp. 1,021-1,042, May, 2024.

SOUZA, Carlos Afonso. *Meta x ANPD: separating AI and personal data spaces will not be easy*. Universe Online, São Paulo, July 4, 2024.

BROWN, Charles; *Civil Rights Framework for the Internet: construction and application*. Juiz de Fora: Edit, 2016.

SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. *The Right to Explanation between Experience and its Positivation in the LGPD*. IN: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo; RODRIGUES JR., Otavio; BIONI, Bruno (Coords.). *Personal Data Protection Treaty*. Rio de Janeiro: Forense, 2021, pp. 243-270.

SOUZA, Carlos Affonso; VIOLA, Mario; STANDARD, Vinicius. *Initial Considerations on the Controller's Legitimate Interests in the General Personal Data Protection Law*. *Public Law*. Brasília, v. 16, n. 90, pp. 109-131, Dec., 2019.

SILVA, Rodrigo da Guia. *Protection of the Human Person in the General Law on the Protection of Personal Data: between the attribution of rights and the enunciation of remedies*. *Thinking*. Fortaleza, v. 24, n. 3, pp. 1-22, Jul./Sept., 2019.

SURBLYTÈ, Gintarė. *Data as a Digital Resource*. Max Planck Institute for Innovation & Competition Research Paper no. 16-12. Germany, Bavaria, Oct., 2016.

TALIAFERRO, Jocelyn; HEDADJI, Fatima; DULING, Emma. *Web Scraping as a Data Collection Strategy: the pitfalls and pitfalls*. *Social Sciences & Humanities Open*. Netherlands, Amsterdam. In press.

TEFFÉ, Chiara Spadaccini de. *The Special Category of Sensitive Data: Fundamentals and Outlines*. IN: SCHREIBER, Anderson; MONTEIRO FILHO, Carlos Edison do Rêgo; OLIVA, Milena Donato (Orgs.). *Problems of Civil Law*. Rio de Janeiro: Forense, 2021, pp. 97-123.

TEFFÉ, Chiara Spadaccini de. *Sensitive Personal Data: qualification, treatment and good practices*. Indaiatuba: Focus, 2022.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Processing of Personal Data in the LGPD: study on the legal bases*. *Civillistica.com*. Rio de Janeiro, v. 9, n. 1, pp. 1-38, May, 2020.

TEPEDINO, Gustavo. *Technologies and the renewal of Civil Law*. OAB/RJ, Rio de Janeiro, June 12, 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. *Consent to the Circulation of Personal Data*. *Brazilian Journal of Civil Law*. Belo Horizonte, v. 25, n. 3, pp. 83-116, Nov., 2020.

LAND, Aline de Miranda Valverde; MULHOLLAND, Caitlin. *The Economic Use of Online Trackers and Identifiers of Personal Data*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *General Law on the Protection of Personal Data and its Repercussions on Brazilian Law*. São Paulo: Thomson Reuters, 2023, pp. 585-604.

EU. *Artificial Intelligence Act. Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence*. European Union: European Parliament, 2024.

EU. *Generative AI and the EUDPR. First EDPS Guidelines for ensuring data protection compliance when using Generative AI systems*. European Union: European Data Protection Supervisor, 2024.

EU. *Guidelines 8/2020 on the Targeting of Social Media Users*. European Union: European Data Protection Board, 2021.

EU. *Report of the work undertaken by the ChatGPT Taskforce*. European Union: European Data Protection Board, 2024.

VERONESE, Alexander. *The Rights of Explanation and Objection to Fully Automated Decisions: Comparing the European Union's GDPR with the Brazilian LGPD*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *General Law on the Protection of Personal Data and its Repercussions on Brazilian Law*. São Paulo: Thomson Reuters, 2023, pp. 377-408.

ZARSKY, Tal. *Incompatible: the GDPR in the age of Big Data*. *Seton Hall Law Review*. USA, New Jersey, v. 47, no. 4, pp. 995-1,020, Aug., 2017.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Struggle for a Human Future on the New Frontier of Power*. Translation: George Schlesinger. New York: Routledge, 2019.

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

3

# Algorithmic Racism: The Challenges of Artificial Intelligence and Social Justice in Digital Context

Barbara Gomes D'Ascencao

Summary: Introduction. 1. Data Capitalism and Inequalities. 2. Algorithmic Racism in Public Safety and the Labor Market. 3. Data Colonialism and Culture; 4. Transparency, Algorithmic Ethics and Public Policies. Final Considerations. References.

## Introduction

Artificial intelligence (AI) has become a constant and transformative presence in many sectors of modern society, from virtual assistants to complex decision-making systems in critical areas such as healthcare, public safety and the job market. Notable examples include the use of AI for medical diagnosis and predictive surveillance systems used by police forces in many cities. While AI offers numerous advantages, it also brings with it significant challenges, especially with regard to social justice and equity. One of the most pressing issues is algorithmic racism, in which algorithms reflect and reinforce racial inequalities present in society. As Noble points out,<sup>2</sup> “algorithms have the power to perpetuate historical and structural biases under the guise of technical neutrality.”

Racism is a social construct that permeates various spheres of life, and technology, developed by social subjects, is not immune to these influences. Technology, despite its neutral appearance, can perpetuate dominant and hegemonic logics. The central question that this article aims to address is: in what way do algorithms used in different social spheres contribute to the reinforcement of structural racism? This question is crucial because, according to Silva<sup>3</sup>, “AI systems are not mere technical tools, but reproductions of the values and prejudices of their societies of origin.”

The relevance of the study lies in the need for a critical, ethical and political understanding of AI systems. The decisions made by these systems directly affect the lives of millions of people, especially those belonging to minority groups. Understanding and mitigating algorithmic racism is crucial to promoting a more just and equitable society. As Zuboff<sup>4</sup>

1. D'ASCENÇÃO, Bárbara Gomes. CV available at: <https://www.linkedin.com/in/b%C3%A1rbara-dascencao/>.

2. NOBLE, Safiya Umoja. *Algorithms of Oppression: How Google Fuels and Profit from Racism*. Santo André: Publisher Rua do Sabão, 2021. p. 34.

3. SILVA, Tarcizio da. *Algorithmic Racism: Artificial Intelligence and Discrimination in Digital Networks*. New York: Routledge, 2019. p.

4. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018. p. 102.

argues, “surveillance capitalism deepens inequalities by monetizing personal data, often reinforcing existing biases.”

## 1. Data Capitalism and Inequalities

The current capitalist model has exacerbated existing inequalities by relying on the extraction and commercialization of large volumes of data. Zuboff<sup>5</sup> defines “surveillance capitalism” as the economic logic that uses personal data to predict and modify human behavior for profit. According to Van Dijck<sup>6</sup>, the process of “datafication” transforms social behaviors and practices into quantifiable data, which are often used without regard for underlying biases.

Personal data is collected across a variety of digital platforms, including social media, search engines, and online services. This data is used to create detailed user profiles, allowing companies and governments to make decisions based on personal information. The problem is that this data often carries historical and structural biases. For example, location data can reflect racial and socioeconomic segregation in cities, perpetuating existing inequalities.<sup>7</sup>

Data collection, therefore, is not a neutral process, but rather loaded with meanings and prejudices that can be used to further discriminate against and marginalize certain groups.

The data used to train AI systems often carries historical biases. These systems, when applied to areas such as public safety, health care, and the labor market, can perpetuate and even amplify racial inequalities. O’Neil<sup>8</sup> states that “algorithms are not impartial; they reflect the priorities and biases of their creators and the data that feeds them.” For example, a study by Noble<sup>9</sup> revealed that Google searches for traditionally African-American names returned ads related to criminal records more often than for names

5. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018.

6. VAN DIJCK, José. *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*. Surveillance & Society, 2014. p. 198.

7. NOBLE, Safiya Umoja. *Algorithms of Oppression: How Google Fuels and Profit from Racism*. Santo André: Publisher Rua do Sabão, 2021. p. 43.

8. O’NEIL, Cathy. *Algorithms of Mass Destruction: How Big Data Increases Inequality and Threatens Democracy*. Santo André: Publisher Rua do Sabão, 2020. p. 56.

9. NOBLE, Safiya Umoja. *Algorithms of Oppression: How Google Fuels and Profit from Racism*. Santo André: Sabão Street Publishing, 2021.

traditionally white months, demonstrating how historical biases are embedded in the data that feeds these systems.

Furthermore, the use of data for decision-making can lead to discriminatory practices. In a study conducted by Pasquale<sup>10</sup>, it has been shown that credit algorithms tend to deny loans to individuals from racial minorities at a disproportionate rate. These algorithms, trained on historical credit data, reflect past biases and discrimination, perpetuating financial exclusion for these communities. A lack of transparency about how data is collected, processed, and used also exacerbates the problem, making it difficult to identify and correct biases.

Surveillance capitalism as described by Zuboff<sup>11</sup> not only exploits personal data for profit, but also contributes to the construction of a social system where inequality is institutionalized through technology. This economic model prioritizes profit maximization over equity and justice, resulting in a vicious cycle where the marginalized continue to be disadvantaged. The lack of regulation and the opacity of data collection and use practices make it difficult for individuals to understand and challenge the decisions made by algorithms.

To better understand how data capitalism perpetuates inequality, it is important to analyze the intersection between technology, society, and the economy. The current capitalist model uses technology not only as a tool for efficiency, but as a mechanism for social and economic control. The “datafication” of social practices transforms aspects of everyday life into commodities, which are then used to predict and influence consumer behavior, reinforcing patterns of discrimination and exclusion. Zuboff<sup>12</sup> argues that this model creates a new form of power, where those who control data have the ability to shape social reality in ways that perpetuate inequality.

Gomes' critical analysis<sup>13</sup> on data colonialism shows that data control and manipulation are modern forms of colonialism, in which power and exploitation are no longer achieved through territorial control, but through data control. Gomes argues that “data colonialism perpetuates the exploitation and marginalization of already vulnerable populations, while

10. PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press, 2015. p. 97.

11. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018. p. 124.

12. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018. p. 132.

13. GOMES, Barbara. *Cybercrime and Culture: An Analysis of Data Colonialism and Its Implications*. TCC. 2023. p. 25.

while consolidating the power of large technology corporations.” This critical perspective complements Zuboff’s analysis<sup>14</sup> by highlighting how historical and colonial power structures are reproduced and reinforced in the digital environment.

Gomes<sup>15</sup> also highlights that data extraction practices are often carried out without the explicit consent of individuals, which reinforces the asymmetry of power between data collectors and data subjects. This results in a form of colonization where data is extracted and used in ways that primarily benefit technology corporations and governments, to the detriment of the most vulnerable populations.

## 2. Algorithmic Racism in Public Safety and Job Market

In Sergipe, during a football match of the Sergipe Football Championship, the facial recognition system caused the arrest of an innocent person, due to a false positive, causing embarrassment and fear to the citizen who was incorrectly detained.<sup>16</sup> This incident highlights how technology can reinforce existing biases, becoming a tool of oppression rather than justice. Facial recognition systems, widely used by law enforcement agencies, demonstrate how the uncritical application of AI can result in discriminatory practices that exacerbate the marginalization of vulnerable groups.

Public safety systems often use algorithms that associate blackness and poverty with crime, resulting in increased incarceration rates and violence against minorities. According to Silva<sup>17</sup>, “algorithmic surveillance systems perpetuate the criminalization of Black bodies, reinforcing structural racism through automated practices.” These algorithms, developed based on historical policing data, often embed and amplify biases, resulting in surveillance and control practices that disproportionately affect Black communities.

14. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018.

15. GOMES, Barbara. *Cybercrime and Culture: An Analysis of Data Colonialism and Its Implications*. TCC. 2023. p. 23.

16. G1. 'Scared, frustrated and embarrassed', says man detained by mistake in stadium after error in facial recognition system. *Fantastic*, Apr 21, 2024. Available at: <https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml>. Accessed on: Oct 18, 2024.

17. SILVA, Tarcizio da. *Algorithmic Racism: Artificial Intelligence and Discrimination in Digital Networks*. New York: Routledge, 2019. p.

Studies show that facial recognition systems are more likely to make mistakes when identifying individuals of certain ethnicities. The study *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* revealed, through the comparison of 189 algorithms from 99 different developers, that most algorithms showed variations in accuracy based on demographic factors, generating a higher rate of false positives for Asian and African-American faces compared to Caucasian faces, reaching 10 to 100 times higher depending on the algorithm<sup>18</sup>. These errors are not merely technical; they have profound implications, such as the unjust criminalization of individuals and the perpetuation of racial stereotypes. Bezerra and Costa<sup>19</sup> highlight that “facial recognition algorithms often fail to correctly identify people with darker skin, exacerbating discriminatory surveillance practices.”

The application of algorithms in the job market also reveals deep inequalities. Algorithms used by companies to select candidates often disadvantage racial minorities. Noble<sup>20</sup> notes that these algorithms may reflect programmers' biases and the historical data used to train them. The study *Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination* from the University of Washington showed that AI systems used to screen resumes tend to reject African-sounding names.

- Americans, even when all other qualifications are equal<sup>21</sup>. This practice not only excludes qualified candidates, but also perpetuates racial segregation in the labor market, demonstrating how algorithms can reinforce social and economic barriers.

Furthermore, a lack of diversity on AI development teams can exacerbate these issues. AI developers often do not represent the diversity of the populations their technologies will impact, which can lead to a feedback loop where biases are inadvertently encoded into the algorithms. Benjamin<sup>22</sup> argues that “the inclusion of

18. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NIST Interagency/Internal Report (NISTIR) - 8280. 2019. Available at: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Accessed on: October 18, 2024.

19. BEZERRA, Arthur Coelho; COSTA, Camila Mattos da. Black skin white algorithms: information and racism in sociotechnical networks. *Liinc em Revista*, v. 18, n. 2, 2022. p. 89.

20. NOBLE, Safiya Umoja. *Algorithms of Oppression: How Google Fuels and Profit from Racism*. Santo André: Publisher Rua do Sabão, 2021. p. 92.

21. BERTRAND, Marianne; MULLAINATHAN, Sendhil. *Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination*. National Bureau of Economic Research, Working Paper 9873, 2003. Available at: [https://www.nber.org/system/files/working\\_papers/w9873/w9873.pdf](https://www.nber.org/system/files/working_papers/w9873/w9873.pdf). Accessed on: October 18, 2024.

22. BENJAMIN, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. Medford, MA: Polity, 2019. p. 88.

“Including diverse voices in algorithm development is crucial to creating more fair and equitable systems.” This means that diversity must be a central consideration not only in the data, but also in the teams that develop and implement these systems.

The interplay between algorithmic racism and public safety and employment practices reveals how technologies, when not properly supervised and regulated, can reinforce unequal power structures. Technology, which was supposed to serve as a tool for justice and equity, often ends up perpetuating the very inequities it promised to solve. The lack of diversity and the presence of bias in data and development teams are crucial factors that contribute to this perpetuation.

Gomes<sup>23</sup> offers an in-depth analysis of the implications of algorithmic racism in the context of cybercrime and public safety. Gomes<sup>24</sup> highlights specific cases where predictive surveillance systems have led to disproportionate police interventions in predominantly black neighborhoods, exacerbating distrust and conflict between these communities and law enforcement.

It also discusses how the lack of transparency and difficulty in accessing the criteria used by surveillance algorithms creates an environment where abuses can occur without adequate oversight. This point is crucial to understanding how technology can be used for both good and bad, depending on how it is implemented and regulated.

### 3. Data and Cultural Colonialism

The concept of *data colonialism*, as discussed by Zuboff<sup>25</sup>, refers to the control and exploitation of data from marginalized populations by technology corporations and governments, without the consent or adequate benefit of these populations. This process perpetuates inequalities and further marginalizes already vulnerable groups, creating a new type of colonialism in the digital environment.

Couldry and Mejias<sup>26</sup> defined *data colonialism* as “a new phase of capitalism, where data extraction is the main form of accumulation of

23. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018.

24. GOMES, Barbara. *Cybercrime and Culture: An Analysis of Data Colonialism and Its Implications*. TCC. 2023

25. GOMES, Barbara. *Cybercrime and Culture: An Analysis of Data Colonialism and Its Implications*. TCC. 2023.

26. COULDRY, Nick; MEJIAS, Ulises A. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019. p. 336.

capital". They argue that this practice reflects and amplifies global inequalities, with technology companies from developed countries extracting data from users in developing countries for their own economic gain. This dynamic creates a relationship of dependency and exploitation, where people in developing countries are reduced to mere data providers.

Furthermore, Thatcher, O'Sullivan and Mahmoudi<sup>27</sup> highlight that the *data colonialism* involves the "production of knowledge from extracted data, which is often used to control and govern populations in non-transparent ways." They argue that the production of knowledge from extracted data often ignores the social and cultural contexts from which these data are drawn, resulting in policies and practices that perpetuate marginalization and exclusion.

A clear example of *data colonialism* This can be seen in the use of data collected by social media companies to influence elections and shape public opinion. The Cambridge Analytica scandal, in which data from millions of Facebook users was used without consent to influence the 2016 US presidential election, highlights how data can be exploited for political and economic purposes.<sup>28</sup> This case illustrates the implications of *data colonialism*, in which data extraction is used to manipulate democratic processes, reinforcing the power of elites over the masses.

The cultural implications of *data colonialism* are deep. Gomes<sup>29</sup> discusses how the appropriation and exploitation of data can lead to the loss of cultural control and the erosion of community autonomy. The author highlights that "the collection and use of data without adequate community involvement can result in the distortion and decontextualization of cultural practices, contributing to the alienation and devaluation of these cultures". This process

27. THATCHER, Jim; O'SULLIVAN, David; MAHMOUDI, Dillon. *Data colonialism through accumulation by dispossession: New metaphors for understanding the societal impacts of Big Data*. Environment and Planning D: Society and Space, 2016. p. 991.

28. The Cambridge Analytica scandal, exposed in 2018, involved the misuse of data from millions of Facebook users. Cambridge Analytica used an app called *thisisyourdigitallife*, which collected personal data under the guise of a personality test for academic purposes. However, this data was shared with Cambridge Analytica and used to create detailed psychological profiles, with the aim of influencing voters during the 2016 US presidential campaign and other campaigns around the world. The US Federal Trade Commission (FTC) sued the company and its executives for deceptive practices, resulting in significant penalties and raising questions about privacy and the ethical use of data.

FTC - Federal Trade Commission. Cambridge Analytica, LLC, In the Matter of. Federal Trade Commission, 24 Jul. 2019. Available at: <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer>. Accessed on: October 15, 2024.

29. GOMES, Barbara. *Cybercrime and Culture: An Analysis of Data Colonialism and Its Implications*. TCC. 2023. p. 23.

so not only perpetuates inequalities, but also threatens the integrity and continuity of marginalized cultures.

Furthermore, the *data colonialism* has significant impacts on the self-determination of communities. By being reduced to data sources, communities lose the ability to define their own narratives and destinies. As Couldry and Mejias state<sup>30</sup>, “data colonialism undermines the ability of populations to exercise control over their own lives, replacing forms of local governance with algorithmic management systems.”

To mitigate the effects of *data colonialism*, it is essential to develop public policies that protect the rights of marginalized populations and ensure an equitable distribution of the benefits of the data economy. This participatory approach is essential to mitigate the negative effects of *data colonialism* and promote social justice in the digital environment.

Couldry and Mejias<sup>31</sup> advocate for the creation of data sovereignty policies, in which communities have control over their own data and can decide how it is used. They argue that “data sovereignty is a critical response to *data colonialism*, enabling communities to regain control over their digital resources.”

Implementing robust regulations that protect privacy and ensure informed consent is another crucial step. The General Data Protection Law (LGPD) in Brazil and the General Data Protection Regulation (GDPR) in the European Union are examples of legislation that aims to protect individuals’ rights regarding their personal data. These laws set standards for the collection, storage, and use of data, promoting transparency and accountability.

Therefore, it is important to promote critical digital literacy that allows populations to understand and question power dynamics in the digital environment. Gomes<sup>32</sup> argues that digital education must include a critical understanding of the social and political implications of data collection and use, empowering individuals to resist forms of digital exploitation. Education is a powerful tool to empower individuals and communities to exercise control over their data and resist practices of *data colonialism*.

30. COULDRY, Nick; MEJIAS, Ulises A. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019. p. 341.

31. COULDRY, Nick; MEJIAS, Ulises A. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019. p. 342.

32. GOMES, Barbara. *Cybercrime and Culture: An Analysis of Data Colonialism and Its Implications*. TCC. 2023. p. 34.

## 4. Transparency, Algorithmic Ethics and Public Policy

The opacity of algorithms and the lack of transparency in the decisions made by these systems raise significant ethical questions. Pasquale<sup>33</sup> argues that “the black box of algorithms hides biases and prejudices that have real and harmful consequences for marginalized groups.” It is essential to develop an algorithmic ethics that promotes transparency, accountability, and equity. Capurro<sup>34</sup> suggests that it is necessary to understand the cultural and historical context in which algorithms are developed to mitigate their discriminatory effects. Noble<sup>35</sup> also emphasizes that “resistance to algorithmic racism must involve both the critique of technologies and the transformation of the social systems that produce them.”

To mitigate these issues, it is essential that governments and institutions develop public policies that regulate the use of AI, ensuring that these systems are auditable and accountable. Yeshimabeit and Traub<sup>36</sup> propose that “AI regulation should include transparency and accountability mechanisms to avoid perpetuating racial inequalities.” Silva<sup>37</sup> argues that human rights impact assessments should be a prerequisite for the adoption of algorithmic systems, emphasizing that “transparency and accountability are essential to ensuring fairness in algorithmic processes.”

Implementing regular audits to identify and correct biases is one of the proposed solutions. O’Neil<sup>38</sup> suggests that “independent audits are needed to ensure that algorithms are not reinforcing bias and inequity.” Auditing should be incorporated as a standard into algorithm development and implementation processes, allowing biases to be detected and corrected before they cause significant harm.

Furthermore, it is crucial to create algorithms that are trained on diverse and representative data. Benjamin<sup>39</sup> highlights that “the inclusion of diverse

33. PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press, 2015. p. 128.

34. CAPURRO, Rafael. *Enculturating Algorithms*. In: *Proceedings of the International Conference: Artificial Intelligence & Regulation*. LUISS Rome, 2019. p. 94.

35. NOBLE, Safiya Umoja. *Algorithms of Oppression: How Google Fuels and Profit from Racism*. Santo André: Publisher Rua do Sabão, 2021. p. 111.

36. YESHIMABEIT, M.; TRAUB, A. *Data capitalism and algorithmic racism*. Paper Knowledge: Toward a Media History of Documents, 2021. p. 75.

37. SILVA, Tarcizio da. *Algorithmic Racism: Artificial Intelligence and Discrimination in Digital Networks*. New York: Routledge, 2019. p.

38. O’NEIL, Cathy. *Algorithms of Mass Destruction: How Big Data Increases Inequality and Threatens Democracy*. Santo André: Editora Rua do Sabão, 2020. p. 143.

39. BENJAMIN, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. Medford, MA: Polity, 2019. p. 88.

their voices in the development of algorithms is crucial to creating more fair and equitable systems.” Furthermore, Pasquale<sup>40</sup> argues that “the data used to train algorithms must be carefully selected to avoid reproducing historical biases.” Data diversity and the inclusion of different perspectives are essential to developing algorithms that serve society as a whole in a fair way.

Raising awareness about the risks and impacts of AI on society is another essential step. Capurro<sup>41</sup> emphasizes the importance of digital literacy that includes a critical understanding of algorithms and their social implications. Noble<sup>42</sup> argues that “education about the impacts of AI should be an integral part of academic curricula to prepare future generations to deal with the ethical and social issues of these technologies.” Education is a powerful tool to empower individuals to question and better understand the influence of algorithms on their daily lives. This educational process not only builds critical subjects, but also empowers them to use technology for their own benefit and for social good.

Gomes<sup>43</sup> suggests that effective public policy implementation must include the active participation of communities affected by algorithms. It is crucial that policies be developed with the inclusion of the voices of marginalized communities, ensuring that their concerns and needs are considered in the development and implementation of AI systems. This participatory approach is essential to creating policies that not only mitigate the negative effects of algorithms, but also promote justice and equity.

In this way, AI can be used to promote social justice, developing technologies that contribute to reducing inequalities and empowering marginalized communities. Noble<sup>44</sup> suggests that “AI technologies should be designed with a social justice lens, considering the needs and experiences of historically disadvantaged groups.”

40. PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press, 2015. p. 151.

41. CAPURRO, Rafael. *Enculturating Algorithms*. In: *Proceedings of the International Conference: Artificial Intelligence & Regulation*. LUISS Rome, 2019. p. 101.

42. NOBLE, Safiya Umoja. *Algorithms of Oppression: How Google Fuels and Profit from Racism*. Santo André: Publisher Rua do Sabão, 2021. p. 135.

43. GOMES, Barbara. *Cybercrime and Culture: An Analysis of Data Colonialism and Its Implications*. TCC. 2023. p. 28.

44. NOBLE, Safiya Umoja. *Algorithms of Oppression: How Google Fuels and Profit from Racism*. Santo André: Sabão Street Publishing House, 2021. p. 149.

marginalized”. Capurro<sup>45</sup> highlights the need for an ethical and responsible approach in implementing these technologies, stating that “social justice must be a guiding principle in the development and use of AI”.

A lack of transparency in algorithmic systems can result in biased and unfair decisions that negatively impact marginalized groups. A study presented at the NeurIPS conference in 2023, titled *Reevaluating COMPAS: Base Rate Tracking and Racial Bias*, analyzed the flaws in COMPAS, showing significant deviations and raising concerns about the presence of racial biases in the system.<sup>46</sup>

To mitigate these issues, it is essential that algorithmic systems are transparent and auditable. This means that organizations using these systems must be able to explain how the algorithms work and what data is used to train and operate these models. Diakopoulos<sup>47</sup> suggests that “auditability is a crucial tool for ensuring that algorithms operate fairly and equitably.” He argues that auditability allows third parties to examine and verify the fairness and accuracy of algorithmic decisions.

Furthermore, it is essential that algorithms are developed ethically. This includes implementing practices that ensure diversity in training data and development teams. Binns<sup>48</sup> emphasizes the importance of “adopting an ethical approach to AI development that includes consideration of values such as fairness, accountability, and transparency.” He argues that developers should be aware of the social and ethical impacts of their creations and take proactive steps to mitigate risks.

A concrete example of AI regulation is the European Union’s General Data Protection Regulation (GDPR)<sup>49</sup>. The GDPR sets out strict guidelines on how personal data should be collected, stored and used, ensuring that individuals have control over their data. One of the provisions of the GDPR, as per Article 22, requires that

45. CAPURRO, Rafael. *Enculturating Algorithms*. In: *Proceedings of the International Conference: Artificial Intelligence & Regulation*. LUISS Rome, 2019. p. 110.

46. CRESPO, Victor; RANDO, Javier; EVA, Benjamin; KESWANI, Vijay; SINNOTT-ARMSTRONG, Walter. *Reevaluating COM-PAS: Base Rate Tracking and Racial Bias*. *NeurIPS*, 2023. Available at: NeurIPS Conference. Accessed on: October 13, 2024.

47. DIAKOPOULOS, Nicholas. *Accountability in algorithmic decision making*. *Communications of the ACM*, vol. 59, n. 2, 2016. p. 59.

48. BINNS, Reuben. *Fairness in Machine Learning: Lessons from Political Philosophy*. *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT)*, 2018, pp. 149-159. Available at: <https://proceedings.mlr.press/v81/binns18a.html>. Accessed on: October 20, 2024.

49. EUROPEAN UNION. *General Data Protection Regulation (GDPR), Article 22*. 2016. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>. Accessed on: 11 Oct. 2024.

automated decisions that significantly affect individuals are explainable, allowing people to understand how these decisions are made and to challenge them if necessary.

Another example is the General Data Protection Law (LGPD)<sup>50</sup> in Brazil, which aims to protect the privacy rights of Brazilian citizens and regulate the collection, storage and use of personal data. The LGPD establishes several legal bases for data processing, with explicit consent being one of them, but it also includes bases such as the execution of contracts, compliance with legal obligations and the legitimate interest of the controller, among others. In addition, the law requires organizations to implement measures to ensure the security and privacy of the personal data processed.

In addition to regulations, self-regulatory initiatives have also been proposed. For example, the Partnership on AI, a coalition of technology companies, academics, and civil society organizations, has developed guidelines for the ethical development of AI, including principles of transparency and accountability. This coalition works to promote AI practices that respect human rights and promote social justice.<sup>51</sup>

Implementing independent audits is also a best practice to ensure transparency and fairness of algorithms. O'Neil<sup>52</sup> suggests that “independent audits are needed to ensure that algorithms are not reinforcing bias and inequity.” These audits should be conducted by independent entities that can objectively assess the fairness and effectiveness of algorithmic systems.

## Final Considerations

It is clear that while AI algorithms and systems have the potential to benefit society, it is crucial to address and mitigate the racial biases embedded in these systems. Promoting algorithmic ethics is essential to ensuring that technology advances in an equitable and fair manner. Recognition and transparency about algorithmic biases are essential.

50. BRAZIL. Law No. 13,709 of August 14, 2018. Provides for the protection of personal data and amends Law No. 12,965 of April 23, 2014 (Marco Civil da Internet). Available at: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm) . Accessed on: October 11, 2024.

51. PARTNERSHIP ON AI. *Tenets of Partnership on AI*. Partnership on AI, 2018. Available at: <https://partnershiponai.org>. Accessed on: September 20, 2024.

52. O'NEIL, Cathy. *Algorithms of Mass Destruction: How Big Data Increases Inequality and Threatens Democracy*. Santo André: Sabão Street Publishing House, 2020. p. 143.

essential for building a more just society<sup>53</sup>. The fight against algorithmic racism is not just a technical issue, but a battle for equity and justice in an increasingly digitalized world.

Therefore, the need for robust public policies and the implementation of regular audits are essential measures to ensure that AI systems do not perpetuate injustices. Including diverse data and raising awareness about the impacts of AI are fundamental steps to creating a technological environment that serves everyone fairly. Experts in the field argue that combating algorithmic racism is part of a larger fight for social justice and human rights in the digital context.

Furthermore, promoting digital literacy that enables a critical understanding of algorithms and their social implications is crucial to empower individuals to question and better understand the influence of algorithms on their lives. Education must prepare future generations to deal with the ethical and social issues of these technologies, promoting a more conscious and equitable society. There is consensus that education on the impacts of AI should be an integral part of academic curricula to prepare future generations for these challenges.

Therefore, social justice must be a guiding principle in the development and use of AI. AI technologies should be designed with a social justice perspective, considering the needs and experiences of historically marginalized groups. This can mitigate the negative effects of algorithmic racism and promote a more just and inclusive society.

## References

BENJAMIN, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. Medford, MA: Polity, 2019.

BERTRAND, Marianne; MULLAINATHAN, Sendhil. Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination. *National Bureau of Economic Research, Working Paper 9873*, 2003. Available at: [https://www.nber.org/system/files/working\\_papers/w9873/w9873.pdf](https://www.nber.org/system/files/working_papers/w9873/w9873.pdf) . Accessed on: October 18, 2024.

BEZERRA, Arthur Coelho; COSTA, Camila Mattos da. Black skin, white algorithms: information and racism in sociotechnical networks. *Liinc in Review*, v. 18, n. 2, 2022.

53. SILVA, Tarcizio da. *Algorithmic Racism: Artificial Intelligence and Discrimination in Digital Networks*. New York: Routledge, 2021.

BINNS, Reuben. Fairness in Machine Learning: Lessons from Political Philosophy. *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT)*, 2018. Available at: <https://proceedings.mlr.press/v81/binns18a.html> . Accessed on: October 20, 2024.

BRAZIL. Law No. 13,709 of August 14, 2018. Provides for the protection of personal data and amends Law No. 12,965 of April 23, 2014 (Marco Civil da Internet). Available at: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm) . Accessed on: October 11, 2024.

COULDRY, Nick; MEJIAS, Ulises A. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019.

CRESPO, Victor; RANDO, Javier; EVA, Benjamin; KESWANI, Vijay; SINNOTT-ARMSTRONG, Walter. Reevaluating COMPAS: Base Rate Tracking and Racial Bias. *NeurIPS*, 2023. Available at: NeurIPS Conference. Accessed on: October 13, 2024.

DIAKOPOULOS, Nicholas. Accountability in algorithmic decision making. *Communications of the ACM*, v. 59, n. 2, 2016.

FTC – Federal Trade Commission. Cambridge Analytica, LLC, In the Matter of. *Federal Trade Commission*, 24 Jul 2019. Available at: <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer> . Accessed on: October 15, 2024.

G1. 'Fearful, frustrated and embarrassed', says man detained by mistake at stadium after facial recognition system error. *Fantastic*, Apr 21, 2024. Available at: <https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-stadium-after-facial-recognition-system-error.ghtml> . Accessed on: October 18, 2024.

GOMES, Barbara. *Cybercrime and Culture: An Analysis of Data Colonialism and Its Implications*. TCC. 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NIST Interagency/Internal Report (NISTIR) –8280, 2019. Available at: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> . Accessed on: October 18, 2024.

NOBLE, Safiya Umoja. *Algorithms of Oppression: How Google Fuels and Profit from Racism*. Santo André: Sabão Street Publishing, 2021.

O'NEIL, Cathy. *Algorithms of Mass Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: New York Times, 2019.

PARTNERSHIP ON AI. Tenets of Partnership on AI. *Partnership on AI*, 2018. Available at: <https://partnershiponai.org> . Accessed on: September 20, 2024.

PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press, 2015.

SILVA, Tarcizio da. *Algorithmic Racism: Artificial Intelligence and Discrimination in Digital Networks*. New York: Routledge, 2021.

THATCHER, Jim; O'SULLIVAN, David; MAHMOUDI, Dillon. Data colonialism through accumulation by dispossession: New metaphors for understanding the societal impacts of Big Data. *Environment and Planning D: Society and Space*, v. 34, n. 6, 2016.

EUROPEAN UNION. General Data Protection Regulation (GDPR), Article 22. 2016. Available at: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679> . Accessed on: October 11, 2024.

VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, v. 12, n. 2, 2014.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018.

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

4

**Collection of Personal Data  
for the Training of  
Artificial intelligence  
Generative: A Challenge for  
Data Protection and  
Privacy**

Rodrigo Santana dos Santos

Summary: Introduction. 1. Main Concepts. 1.1 Machine Learning in the Context of Generative AI. 1.2 Data Extraction on the Internet (Data Scraping). 1.3 Privacy and Data Protection and AI in Brazil. 2. International Good Practices on AI, Privacy and Data Governance. 2.1 Organization for Economic Cooperation and Development. 2.2 European Union Guidelines for Trustworthy AI. 3. Analysis of Case Studies. 3.1 Data extraction from the internet through data scraping. 3.2 Data collection from Meta for AI training. 3.3 Possible Regulatory Solutions. Final Considerations. References.

## Introduction

Regulation is an art that seeks to balance the protection of a service, an activity or a right with the promotion of a regulated environment that fosters new technologies and business models for the socioeconomic development of the country. In the digital environment, the evaluation of models that seek this balance is of great relevance, given the dynamism of technological development and the need for trust in commercial, economic and social relations in such an environment.

In this sense, the General Data Protection Law (LGPD) creates an important regulatory framework for the activity of processing personal data with the aim of protecting the fundamental rights of data protection and privacy.

Artificial Intelligence (AI), considering its disruptive technological innovations, presents great challenges in building a regulatory framework that balances the protection of fundamental rights with innovation and the potential benefits that AI can provide.

One of the main challenges is to ensure data protection and privacy during the training of generative AI, given the need for excessive data collection, including personal data. The potential opportunities with the advancement of this segment of AI are undeniable, such as in improving scientific and creative writing,<sup>2</sup> education and learning,<sup>3</sup> accessibility and

1. He is currently the General Coordinator of Standardization at the National Data Protection Authority (ANPD). He is a civil servant in the career of Regulatory Specialist – Technological Area, working in the area of regulation of telecommunications services and personal data protection. He holds a master's degree in Electrical Engineering from UNB. He has a postgraduate degree in Digital Law from ITS Rio/UERJ. He is a member of Study Commission 20 of the International Telecommunication Union (ITU) - Internet of Things, Communities and Smart Cities.

2. SPRINGER NATURE. Tools such as ChatGPT threaten transparent science; here are our ground rules for their use. *Nature*. 2023. 613 p. Available at: doi:<https://doi.org/10.1038/d41586-023-00191-1> . Accessed on: August 2, 2024.

3. SAÚDE, Sandra; BARROS, João Paulo; ALMEIDA, Inês. Impacts of Generative Artificial Intelligence in Higher Education: Research Trends and Students' Perceptions. *Social Sciences*. 2024, 13, 410 p. Available at: <https://doi.org/10.3390/socsci13080410> . Accessed on: July 27, 2024.

inclusion, reduction of social economic inequality,<sup>4</sup>as well as in health and medicine.<sup>5</sup>

In view of this, this article seeks to identify the main problems and challenges involved in the excessive collection of personal data for training AIs, considering internet data extraction techniques, such as data scraping, and the movement perceived by the so-called Big Techs to change their privacy policies to collect massive personal data from users, aiming to train generative AIs.

The article is divided into a theoretical part, which includes: main concepts, in which technical and legal concepts are presented, good interactional practices on AI, privacy and data governance and a part of case studies of data extraction from the internet through data scraping and another of data collection from Meta for AI training, with identification of possible regulatory solutions.

## 1. Main Concepts

### 1.1 Machine Learning in the Context of Generative AI

Machine learning represents a subfield of AI focused on developing algorithms that allow machines to learn from data and make predictions or decisions without being explicitly programmed for each specific task.<sup>6</sup>It can also be defined as a computational method using experiments to improve performance or make more accurate predictions.<sup>7</sup>

Among the various types of machine learning, deep learning (*deep learning*) is a subfield that focuses on algorithms inspired by brain architecture, that is, a deep neural network and are used for learning in generative AI.

Deep learning algorithms are used for various applications, including: facial recognition, image classification, object detection, speech-to-text conversion, virtual assistants, diagnostics,

4. CARPRARO, Valerio, et al. The impact of generative artificial intelligence on socioeconomic inequalities and policy making. *Pnax Nexus*. 2024, 3, 191 p. Available at:<https://doi.org/10.1093/pnasnexus/pgae191> . Accessed on: July 29, 2024.

5. ZHANG, Peng; BOULOS, Maged N. Kamel. Generative AI in Medicine and Healthcare: Promises, Opportunities and Challenges. *Future Internet*. 2023, 15, 286 p. Available at:<https://doi.org/10.3390/fi15090286> . Accessed on: August 1, 2024.

6. MITCHELL, Tom. *Machine Learning*. 1997. McGraw-Hill.

7. MOHRI, M; Rostamizadeh, THE; Talwalkar. THE. *Foundations of Machine Learning*. Second Edition. MIT Press. 2018.

disease management, medical image analysis, autonomous driving and navigation systems.

In this sense, the deep learning model requires a large volume of data to effectively train the various parameters constituted in the neural network and obviously obtain more precise and correct results.<sup>8</sup>

## 1.2 Internet Data Extraction (Data Scraping)

Internet data extraction, also known as scraping, can be understood as the automated practice of extracting large amounts of data published on websites. This extraction is done through software that sends requests to web pages, collects and analyzes the content of these pages, and extracts specific information of interest. Extraction allows for the rapid and cost-effective collection of data, often without the consent or knowledge of the data owners or the individuals to whom the data belongs.<sup>9</sup>

The general term “data scraping” refers to any time “a computer program extracts data from the output generated by another program.” More specifically, scraping is the “retrieval of content posted on the World Wide Web through the use of a program other than a web browser or an application programming interface (API).” Scraping “is used to transform unstructured data on the web into structured data that can be stored and analyzed in a central local database or spreadsheet.”<sup>9</sup>

Web scraping is a method that allows you to obtain a huge amount of data at a relatively low cost. This scenario is ideal for meeting the demands of AI machine learning, such as deep learning, that need a large amount of data.

One of the most notorious cases of AI scraping was carried out by *Clearview* AI, a startup that scraped over three billion images to develop a facial recognition system.<sup>9</sup>

Another case was recently presented by *Human Rights Watch*, an international, non-profit, non-governmental human rights organization, which analyzed 0.0001% of the LAION-5B database, which has 5.85 billion images and captions contained in the dataset, used

8. GOODFELLOW, I., Bengio, Y., & Courville, A. *Deep Learning*. MIT Press. 2016.

9. SOLOVE, Daniel J; HARTZOG, Woodrow. The Great Scrape: The Clash Between Scraping and Privacy. *SSRN*. 2024. Available at: <http://dx.doi.org/10.2139/ssrn.4884485> . Accessed on: August 2, 2024.

to do AI training.<sup>10</sup>In this investigation, photos of children from 10 Brazilian states were found.<sup>11</sup>

Many cases of data scraping have been taken to court, such as the case of hiQ Labs and LinkedIn in the United States.<sup>12</sup>hiQ is a small data analytics company that used *botshiQ* Labs has been using automated means to collect information from public LinkedIn profiles. LinkedIn has used legal means to prevent this collection, however, hiQ Labs filed a lawsuit against LinkedIn seeking an injunction against this limitation, which was granted. LinkedIn appealed and the district court's preliminary injunction was upheld, preventing LinkedIn from denying hiQ Labs access to the public profiles of LinkedIn members. However, upon further appeal in another court, hiQ was found to have violated LinkedIn's terms of use and a settlement was reached.<sup>12</sup>

There are several legal cases in US courts involving companies that own platforms that have their users' information scraped. In this veritable data scraping war, several companies claim that such conduct would conflict with privacy and personal data protection laws, but in fact, in some cases they are seeking to protect data that they believe to be theirs or to protect their website and their own commercial interests. Ultimately, user privacy and security end up being invoked when they align with corporate interests.<sup>12</sup>

On the other hand, we can see the emergence of a new data scraping market.<sup>12</sup>For example, Open AI has done business with the Associated Press and Axel Springer, the parent company of Politico and Business Insider, to obtain data, including involving personal data.<sup>13</sup>

### 1.3 Privacy and Data Protection and AI in Brazil

The General Data Protection Law (LGPD) is a regulatory framework that provides for the processing of personal data, including in digital media, by a natural person or by a legal entity under public or private law, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the natural person's personality.

10. HUMAN RIGHTS WATCH. Brazil: *Photos of children are being misused to feed AI*. 2024. Available at: <https://www.hrw.org/pt/news/2024/06/10/brazil-childrens-personal-photos-misused-power-ai-tools> . Accessed on: August 2, 2024.

11. EUROPEAN UNION. *Artificial Intelligence Act*. 2024. Available at: <https://artificialintelligenceact.eu/ai-act-explorer/> . Accessed on: August 3, 2024.

12. SOLOVE, Daniel J; HARTZOG, Woodrow. The Great Scrape: The Clash Between Scraping and Privacy. *SSRN*. 2024. Available at: <http://dx.doi.org/10.2139/ssrn.4884485> . Accessed on: August 2, 2024.

13. SOLOVE, Daniel J; HARTZOG, Woodrow. The Great Scrape: The Clash Between Scraping and Privacy. *SSRN*. 2024. Available at: <http://dx.doi.org/10.2139/ssrn.4884485> . Accessed on: August 2, 2024. Apud BARRADI, Thomas, OpenAI Offering Media Outlets as Little as \$1M to Use News Articles for AI Models, *New York Post*. 2024.

In this sense, it is observed that the application of the law established a regulatory framework for the processing of personal data, regardless of the medium, physical or digital, or the technology used, such as blockchain, AI.

It is also worth noting that Article 3 of the LGPD states that the law applies if: i) the processing operation is carried out in the national territory, ii) the processing activity aims to offer or provide goods or services or to process data of individuals located in the national territory or iii) the personal data, which are the object of the processing, were collected in the national territory.

Thus, it is concluded that the LGPD is applicable when personal data is processed, even through AI, under the terms of art. 3 of the law.

In this regard, the principles, rights and guarantees provided for by law must be observed, highlighting the principles of purpose, necessity, non-discrimination, transparency and accountability in the context of AI.

All processing of personal data must be based on some legal hypothesis provided for in art. 7 and 11 of the LGPD, with no hierarchy between them. It is worth noting that there are greater restrictions in the legislation on sensitive personal data provided for by law and on processing that reveals these types of data, and the legal hypothesis of legitimate interest cannot be applied.

Another highlight in the LGPD related to AI is provided for in art. 20. This article provides for the right to review decisions made solely based on automated processing when it affects the interest of the data subject. §1 provides for the right to information on the criteria and procedures used for the decision made, also known as the right to explanation.

The article is directly related to AI systems, but some points need to be subject to regulation or interpretation by the ANPD. The parameters for considering “decision-making solely based on automated processing” stand out. In this case, it is interesting to define the level of human intervention that could occur for it to be considered automated processing. Another highlight would be the criteria for determining when an interest is effectively being affected.

In this regard, in addition to art. 20 of the LGPD, one point has shown concern on the part of authorities and academia and concerns the relationship between the excessive collection of personal data for training AI systems and privacy.

In relation to this collection of personal data, there are legal aspects that need to be observed, such as, for example, compliance with the aforementioned principles, legal hypotheses for processing and obligations provided for in the LGPD.

It is also worth highlighting the likely limitation of the rights of data subjects provided for in the LGPD, such as access, correction, anonymization, blocking, deletion and explanation, which will be discussed in more detail later. In addition, informational self-determination is a fundamental pillar of the LGPD for the data subject's actions.

Furthermore, it is worth noting that the data protection and privacy policy is a good practice instrument provided for in art. 50 of the LGPD. The aforementioned article provides that controllers and operators, within the scope of their competences, for the processing of personal data, individually or through associations, may formulate rules of good practice and governance that establish the conditions of organization, the operating regime, the procedures, including complaints and petitions from data subjects, the security rules, the technical standards, the specific obligations for the various parties involved in the processing, the educational actions, the internal mechanisms of supervision and risk mitigation and other aspects related to the processing of personal data.

It also provides in § 2 that the controller or operator demonstrates commitment to adopting internal policies that ensure compliance with standards and good practices regarding the protection of personal data, as well as establishing appropriate policies and safeguards based on a systematic assessment process of impacts and risks to privacy.

In this sense, the policy can be considered as an internal governance instrument with guidelines and measures regarding data processing from data collection to data deletion. This set of rules is addressed to employees or entities, public or private, that have a relationship with the controller or operator.

Another relevant document is the privacy notice, the purpose of which is to provide transparency regarding the processing of personal data to society in general, especially to the data subject. The LGPD did not expressly provide for this governance instrument, but there are several international experiences on the subject.

In this sense, considering the rules of good practices and governance, provided for in art. 50 of the LGPD, it is necessary for the controller to adopt internal processes and policies that ensure compliance,

comprehensive manner, of standards and good practices regarding the protection of personal data. For example, the UK data protection authority (*Information Commissioner's Office-ICO*) has published guidance material on how to provide privacy information to data subjects.<sup>14</sup>

## 2. Good Practices on AI, Privacy and Governance Data

There are several international rules and best practices that address data governance, including during the training process of AI systems. These practices are essential to ensure that models are trained ethically, efficiently, and safely. Two relevant best practices are presented below.

### 2.1 Organization for Economic Cooperation and Development Economic

The Organization for Economic Cooperation and Development (OECD)<sup>15</sup> published a document that analyzes the intersection between privacy and artificial intelligence, especially generative AI, which requires huge volumes of data for learning<sup>16</sup>. This analysis was conducted on the basis of the guiding principles included in the 1980 OECD Privacy Guidelines, updated in 2013, and the 2019 OECD Recommendation on AI (the “OECD Recommendation on AI”), updated in 2024.

This analysis concludes that, despite the challenges, innovative technological and regulatory developments in AI are mostly compatible with, and may even reinforce, privacy and personal data protection rules.

The document points out possible similarities and differences in the principles of AI and privacy.

Principle 1.1: *Inclusive growth, sustainable development and well-being*. The document points out some positive social benefits, such as improved health and the fight against climate change, and in the economy, such as reduced costs in the production of products and services through AI. However,

14. ICO. What methods can we use to provide privacy information? Available at: <https://ico.org.uk/for-organisations/uk-g-dpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/>. Accessed on: August 3, 2024.

15. Organization for Economic Cooperation and Development (OECD). Intergovernmental economic organization with 38 member countries, founded in 1961 to stimulate economic progress and world trade.

16. OECD. *AI, Data Governance and Privacy*. 2024. Available at: [https://www.oecd.org/en/publications/ai-data-governance-and-privacy\\_2476b1a4-en.html](https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html). Accessed on: August 4, 2024.

Greater accuracy of systems may conflict with privacy and data protection rights, as larger amounts of data are required for training. The document highlights that data protection authorities and courts have been dealing with these conflicts for many years, applying constitutional mechanisms to resolve conflicts between competing rights and interests in specific cases, for example, the application of the “balancing test” to identify the proportionality between privacy and AI systems.

Principle 1.2: *Respect for the rule of law, human rights and democratic values, including justice and privacy.* This principle can be divided into three categories: bias and discrimination; privacy and data governance; and human rights and democratic values. Generative AI, as currently developed, deployed, and used, in the absence of protective boundaries, magnifies these risks due to the massive scale and scope of application of such systems and their input training data during their training phase.

Principle 1.3: *Transparency and explainability.* The document describes that transparency is based on responsible disclosure to ensure that people are aware that AI is being used in a prediction, recommendation, decision, or in an interaction (e.g., a *chatbot*). It highlights that important disclosures, such as making people aware that they are dealing with AI or that their personal data is being used, are a common goal of AI and privacy regulation and are increasingly being discussed in the context of generative AI, where *chatbots* have emerged as very popular applications across all sectors.

Regarding explainability and interpretability, the paper points out that they are present in policy discussions in both the AI and privacy communities. The complexity and often “black box” nature of AI systems derived from machine learning, and particularly generative AI models, make these issues increasingly urgent.

Principle 1.4: *Robustness, safety and protection.* This principle deals with security and protection measures in relation to data processing that must be adopted.

It addresses that this principle largely converges with the data security principle in the OECD Privacy Guidelines: “Personal data should be protected by reasonable security safeguards against risks

such as loss or unauthorized access, destruction, use, modification or disclosure of data.”<sup>17</sup>The paper points out that robust machine learning models traditionally need large, representative datasets for training. This can conflict with the data minimization principle.<sup>18</sup> However, some safeguards, such as Privacy Enhancing Technologies (PETs) – can help bridge the gap between developing safe AI models and protecting individuals’ privacy rights.

Principle 1.5:*Accountability*.The paper states that both the privacy and AI communities have developed approaches to accountability and risk management. It highlights OECD work on AI classification<sup>19</sup>and accountability,<sup>20</sup> which provide a detailed and robust framework for identifying risks, relevant stakeholders, and mitigation measures for AI systems based on the AI system lifecycle.

## 2.2 European Union Guidelines for Trustworthy AI

The European Union has published guidelines for considering a trustworthy AI. According to the document, a trustworthy AI would consist of three elements, which should be observed throughout the system's life cycle: a) it must be legal, complying with all applicable legislation and regulations; b) it must be ethical, ensuring compliance with ethical principles and values; and c) it must be sound, both from a technical and social point of view, since, even with good intentions, AI systems can cause unintended harm.<sup>21</sup>

Regarding the aspect of privacy and data governance, the document states that linked to the principle of prevention of harm is the right to privacy, a fundamental right that is particularly affected by AI systems. Preventing threats to privacy also requires governance

17. OECD. *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. 1980. Available at:<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188> . Accessed on: November 4, 2024.

18. OECD. *AI, Data Governance and Privacy*. 2024. Available at:[https://www.oecd.org/en/publications/ai-data-governance-and-privacy\\_2476b1a4-en.html](https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html) . Accessed on: August 4, 2024. Apud Global Privacy Assembly, *Resolution on Generative Artificial Intelligence Systems*, 2023.

19. OECD. *AI, Data Governance and Privacy*. 2024. Available at:[https://www.oecd.org/en/publications/ai-data-governance-and-privacy\\_2476b1a4-en.html](https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html) . Accessed on: August 4th. Apud OCDE. “OECD Framework for the Classification of AI systems”, *OECD Digital Economy Papers*, No. 323, OECD Publishing, Paris, 2022.

20. OECD. *AI, Data Governance and Privacy*. 2024. Available at:[https://www.oecd.org/en/publications/ai-data-governance-and-privacy\\_2476b1a4-en.html](https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html) . Accessed on: Aug 4th. Apud OECD. “Advancing accountability in AI: Governing and managing risks throughout the lifecycle for trustworthy AI”, *OECD Digital Economy Papers*, No. 349, OECD Publishing, Paris. 2023.

21. EUROPEAN UNION. *Ethics guidelines for trustworthy AI*. 2019. Available at:<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> . Accessed on August 4, 2024.

adequate data collection, which ensures the quality and integrity of the data used, its relevance to the domain in which AI systems will be deployed, its access protocols and the ability to process data in a way that protects privacy.

### 3. Analysis of Data Extraction Case Studies for Generative AI Training

The analysis will address two cases related to the collection of personal data for training generative AI and is restricted to Brazilian legislation.

The first case concerns the extraction of data from the internet through data scraping and the second is related to the change in Meta's privacy policy to collect data from its platform for training generative AI.

#### 3.1 Extracting data from the Internet through scraping of data

Initially, it is worth mentioning that there is a huge challenge in balancing internet extractions with the principles, foundations and guarantees provided for in the LGPD.

Companies claim that they need a huge amount of personal data to improve the accuracy of automated decisions made by AI systems. However, this activity of collecting data published on the internet conflicts with the principles of purpose, necessity, free access, transparency, accountability and accountability, provided for in art. 6 of the LGPD.

The principle of purpose is the processing of data for legitimate, specific, explicit purposes that are informed to the data subject, without the possibility of further processing in a manner that is incompatible with these purposes. The principle of necessity is the limitation of processing to the minimum necessary to achieve its purposes, covering relevant, proportionate and non-excessive data in relation to the purposes of data processing.

When a data processing agent extracts data from the internet for the purpose of AI training, some points become unclear and difficult to comply with the law, such as how to consider the purpose of AI training as being specific, how to inform this purpose to the data subject and how to measure which data is necessary if generic AI applications can be very diverse?

The purpose of AI training is often not clearly defined, resulting in indiscriminate data collection. This practice aims to improve the effectiveness of AI systems, but it runs counter to the principle of necessity.

Another highlight is related to informational self-determination, the basis of the LGPD, as provided for in item II of art. 2, which grants the data subject the right to control their own personal data, based on the precepts of good faith and transparency.

The data subject cannot exercise this right to control their data, considering that they do not even know that their data is being processed. Failure to comply with these guidelines can lead to serious legal consequences and compromise users' trust in AI systems.

It is observed that data scraping is an activity that is difficult to comply with the principle of transparency, considering it to be a silent activity that occurs without the knowledge of the data owner.

Regarding the legal hypotheses for the activity of collecting data for AI training, provided for in art. 7 and 11 of the LGPD, the most used hypothesis is legitimate interest.

The LGPD has stricter parameters for the processing of data based on this hypothesis, under the terms of art. 10, for example, it may only justify the processing of personal data for legitimate purposes, considered based on specific situations. Furthermore, it may be used to protect, in relation to the data subject, the regular exercise of their rights or the provision of services that benefit them, respecting their legitimate expectations and fundamental rights and freedoms, under the terms of the Law.

In addition, the ANPD published a guide<sup>22</sup> which exposed the need for a balancing test to assess whether the processing activity does not override fundamental rights and freedoms, as well as respecting the legitimate expectations of the data subject. There is no need to speak of legitimate expectations in this case, given that the data subject is unaware of the processing.

With regard to the rights of data subjects, the data subject is prevented from exercising the rights provided for in articles 9, 18 and 20, such as confirmation of the existence of processing, access to data, access to data, anonymization, blocking or deletion of unnecessary data. The fact of being unaware of the processing being carried out and of not having clear communication channels with the controller weakens the entire legal model established.

22. ANPD. *Guidance on Legal Hypotheses for the Processing of Personal Data: Legitimate Interest*. 2024. Available at: [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia\\_legitimo\\_interesse.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf). Accessed on: October 28, 2024.

Article 20 establishes the obligation of the data controller to provide, whenever requested, clear and adequate information regarding the criteria and procedures used for automated decision-making, taking into account commercial and industrial secrets. This provision deals with the so-called right to explanation, which is in line with good explainability practices.

Another aspect discussed concerns internet data already being public.<sup>23</sup>, whether these could be processed without the consent of the holder. Art. 7, § 4 of the LGPD, provides that the requirement for consent provided for data made manifestly public by the holder is waived, safeguarding the rights of the holder and the principles provided for in the Law.

Furthermore, it is also worth highlighting that art. 7, § 3 provides that the processing of personal data that is publicly accessible must consider the purpose, good faith and public interest that justified its provision.

Therefore, even if it is considered that there is no need for the consent of the holder, the collection of public personal data for AI training must observe the purpose, good faith, rights and principles provided for in the LGPD.

It is worth noting that the legislator provided that it would not be necessary to obtain consent; however, in order to carry out data processing, it will be necessary to use some legal hypothesis that authorizes the processing.

In this sense, it is observed that data scraping for generic AI systems has a high potential for non-compliance with the LGPD and does not observe best practices for the development of AI systems, notably transparency, explainability, data governance, accountability and accountability. However, the use of AI, as already mentioned in this article, is undeniable for the development of new business models and technological solutions, requiring legal, technical and administrative safeguards, which will be presented in item 3.3, to reduce risks to fundamental rights of data protection and privacy.

## 3.2 Collecting Meta data for AI training

Meta recently announced a new privacy policy that has raised concerns among users. Meta announced that starting June 26, 2024, users' public posts would be used to train generative AI without the need for prior permission.

23. SOLOVE, Daniel J; HARTZOG, Woodrow. The Great Scrape: The Clash Between Scraping and Privacy. *SSRN*. 2024. Available at: <http://dx.doi.org/10.2139/ssrn.4884485> . Accessed on: August 2, 2024.

Meta's privacy policy states that the data collected is shared with companies in the Meta economic group, including Facebook, Messenger, Instagram, among others.

In research conducted on Meta's privacy policy,<sup>24</sup> It is observed that the following data are collected:

- The content created, such as publications, comments or audios;
- Content provided through our camera feature, camera roll settings, or our voice-enabled features;
- Messages sent and received, including content, subject to applicable laws;
- Metadata about content and messages, subject to applicable laws;
- The types of content, including advertisements, that you view or interact with and how you do so;
- The apps and features used and what actions the user takes on them;
- Purchases or other transactions you make, such as through Meta checkout experiences, including credit card information;
- The hashtags used;
- The timing, frequency and duration of your activities on Meta products.

It also clarifies that it collects contact data, such as information about friends, followers, groups, accounts, Facebook pages and other users and communities with whom users have connections or interact. The company informs that it collects the name and email address or telephone number, if it is uploaded or imported from a device, such as when synchronizing a contact list.

Meta describes how it performs processing for AI training in the privacy center and that the generative AI model is capable of creating content when a person gives instructions or asks a question, such as text, images, and audio.

It clarifies that it uses models that generate text and images that need massive amounts of data to estimate and be more effective.

24. GOAL. *Meta Privacy Policy*. 2024. Available at: <https://pt-br.facebook.com/privacy/genai>. Accessed on: August 4, 2024.

It also provides that data is processed based on five pillars: privacy and security, impartiality and inclusion, robustness and security, transparency and control, governance and accountability.

It also describes that it carries out the processing based on legitimate interest, in the same way as it does in the European region and the United Kingdom.

In view of the possible change in Meta's privacy policy, the ANPD, through Order No. 20/2024/PR/ANPD, published in the DOU on July 2, 2024, substantiated by Vote No. 11/2024/DIR-MW/CD, by director Miriam Wimmer, issued a preventive measure determining the immediate suspension, in Brazil, of the validity of the new privacy policy of the company Meta, which authorized the use of personal data published on its platforms for the purposes of training AI systems.<sup>25</sup>

The company had its request for reconsideration denied by means of Decision Order PR/ANPD No. 24/2024, considering the need to postpone the analysis of the requests for granting of a suspensive effect and the request for full reconsideration of the decision, until a technical analysis of the proposed measures is carried out considering and a compliance plan is presented by Meta, specifying specific deadlines for the implementation of the measures under the terms of art. 36 of the Inspection Regulation (Resolution CD/ANPD No. 01/2021), or documentation proving their entry into force, and the presentation of the balancing test of the legal hypothesis regarding Legitimate Interest, within a period of up to 10 (ten) business days.

However, after presenting all the requested documentation, Decision Dispatch PR/ANPD No. 33/2024, based on VOTE No. 23/2024/DIR-JR/CD, decided to suspend the precautionary decision in the following terms: (i) approve the updated compliance plan presented by the company, in accordance with the grounds presented in vote No. 23/2024/DIR-JR/CD and in Technical Note No. 39/2024/FIS/CGF/ANPD; and (ii) suspend the preventive measure applied to Meta by the Board of Directors, in accordance with Decision Dispatch PR/ANPD No. 20/2024, with the determination of full compliance with the compliance plan.

In terms of privacy and data protection, the decision to suspend was based on four important points: legal hypothesis, principles of purpose, necessity and transparency, limitation on the rights of data subjects and use of personal data of children and adolescents.

25. ANPD. *ANPD determines precautionary suspension of personal data processing for training Meta's AI*. 2024. Available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta> . Accessed on: August 4, 2024.

## Legal Hypothesis

According to the vote of the director who supported the decision on the preventive measure, with regard to the legal hypothesis, it was concluded that legitimate interest does not appear to be the most appropriate basis for processing, considering that sensitive personal data may be processed, notably given the possibility of using images, audios, texts and videos, which may reveal political, religious and sexual affiliations of the holders, among other aspects of personality indicated in art. 5, II, of the LGPD.

He also highlighted that for the appropriate use of the legal hypothesis, the interest must be based on concrete situations, that is, real, clear and precise situations, which aim at specific and well-defined interests, even in the near future, which excludes interests considered based on abstract or merely speculative situations.

Furthermore, the analysis concluded that it is reasonable to assume that, in principle, there is no expectation on the part of the holders that information posted on the social network years ago would be used to train generative AI.

The vote also addressed the purpose, which it called the generic and broad purpose of training generative AI systems. It was found that there is strong evidence that the processing carried out by the company for training AI systems is not supported by the legal hypothesis of legitimate interest, whether due to the processing of sensitive data, or due to the violation of the legitimate expectations of the holders, or due to the failure to comply with the principles of purpose and necessity.

Given the director's analysis that legitimate interest would not be the most appropriate legal hypothesis for the processing of data for the purpose of training generative AI and considering that there is sensitive data or that the processing is likely to reveal sensitive data, only consent could be the legal basis used.

However, if the legal basis of legitimate interest were used, reservations would be necessary to adapt the processing to the LGPD. Firstly, greater data governance would be necessary in the context of data collection, taking into account the inventory to identify the types of data processed in order to segregate those that would not be considered sensitive, to have the record of operations, as provided for in art. 37, and the preparation of the Data Protection Impact Report.

In addition, it would be necessary to develop a balance test to assess the specific purpose of the training, the need for data and the

proportionality of the agent's interest in relation to the fundamental rights of the holders, as well as their legitimate expectations.

In this sense, the vote of the reporting director of the company's request for reconsideration, based on Technical Note No. 39/2024/FIS/CGF/ANPD, indicated that the company presented all the required documentation, including the legitimate interest balancing test, which contains more detailed information on the processing of personal data for the purpose of training a generative AI system, in addition to several safeguards implemented in order to prevent the identification of data subjects and third-party personal data through inferences.

According to Technical Note No. 39/2024/FIS/CGF/ANPD, the company, by applying safeguards that guarantee the possibility of pseudonymizing users' personal data, with the aim of mitigating possible harmful effects to data subjects arising from the processing, enables the incidence of the legal hypotheses of art. 7 of the LGPD for the processing of personal data with a view to training generative AI models.

Furthermore, it concluded that the transparency measures to be implemented and the facilitation of the exercise of the "opt-out" option are also elements that strengthen respect for the rights and legitimate expectations of data subjects.

## Transparency of data processing

Regarding transparency, the analysis by the director who supported the preventive measure concluded that there was a lack of disclosure of clear, precise and easily accessible information about the change in the privacy policy to allow the use of personal data for AI training purposes.

However, the vote of the director who analyzed the request for reconsideration indicated that the company has improved the mechanisms for providing information regarding data processing for generative AI. In addition, the compliance plan presented includes a series of measures, such as notifications, updates to the privacy policy and the creation of a dedicated area on the website, which demonstrates significant changes to provide greater transparency in compliance with ANPD determinations.

In this regard, it should be understood that the privacy policy is an internal regulatory document aimed at employees or individuals or legal entities that have a relationship with the agent. Transparency, according to the LGPD, must ensure that clear, accurate and easily accessible information is available.

on the performance of the treatment and the respective treatment agents are accessed by the holder, observing commercial and industrial secrets.

In this sense, it is understood that the most appropriate transparency mechanism to inform the data subject about the processing is the privacy notice. Attention should be paid to the use of means of communication that can guide the data subject in a clear and simple manner. For example, if data from children and adolescents is involved, the physical-motor, perceptive, sensory, intellectual and mental characteristics of the user should be taken into account, with the use of audiovisual resources when appropriate, in order to provide the necessary information to the parents or legal guardian and appropriate for the child's understanding.

### Exercise of the rights of the holders

Regarding the exercise of the rights of the holders, the vote of the director who supported the effective measure stated that there appear to be obstacles that excessively limit the exercise of rights. It highlighted that to exercise the right to object, the holder needs to go through several steps, including having to click on eight options in the case of the Facebook application.

In this regard, unlike scraping personal data from the internet, the data processing agent is able to develop solutions and channels through which the data subject can exercise the rights provided for in the LGPD.

If the agent can justify the use of the legal basis of legitimate interest, it is interesting to have mechanisms for *opt-out*, given the provision for the elimination of unnecessary, excessive data or data that does not comply with the LGPD, which appears to fit the case.

The vote of the reporting director who analyzed the suspension of the measure indicated that the company improved the opt-out mechanisms, facilitated access to the exercise of rights for users and non-users, reducing the number of clicks required to access them, in addition to facilitated transparency measures, as mentioned above, under the terms determined by the ANPD.

### Processing of data of children and adolescents

Regarding the processing of data from children and adolescents, the vote that supported the preventive measure pointed out that the necessary safeguards for the processing of personal data from children and adolescents for the purposes of training AI systems do not appear to be present, notably based on the legal hypothesis of legitimate interest.

The legal hypothesis of legitimate interest can be used for the treatment of children and adolescents. The ANPD has published a guide on the legal basis of legitimate interest<sup>26</sup> and ratified its understanding of the possibility of its use for the treatment of minors. However, according to the ANPD's analyses in the specific case, safeguards would be necessary to guarantee greater protection of the fundamental rights of these data subjects for the processing of data for AI training purposes, specifically based on the legal hypothesis of legitimate interest.

In this sense, the company presented, in its compliance plan, that it will not process personal data from accounts of users under 18 years of age for the purpose of training and developing its generative AI models, eliminating the risks to this category of data subjects for now. However, Meta emphasized that it would continue to discuss with the ANPD, within the scope of the ongoing inspection process, the legitimacy of the processing of personal data of this category of data subjects.

In this sense, it is worth noting that, in Europe, Meta announced that “it is not training its Llama models with content generated by accounts of Europeans under the age of 18”.<sup>27</sup>

### 3.3 Possible Regulatory Solutions

The article written by *Solove and Hartzog*<sup>28</sup> points out some possible solutions, among which, from the perspective of data protection and privacy, the ban on data scraping for use in generative AI training and the use of consent stand out. The article also proposes an agenda for regulators composed of four principles that cover reasonable risks and harms, benefits to society, transparency processes, accountability and responsibility, and protection of data used for AI training.

It is also worth noting that technical or safeguard measures can be sought to improve data collection for training AI systems, notably based on the legal hypothesis of legitimate interest and, thus, guarantee fundamental rights.

Personal data, according to the LGPD, is information related to an identified or identifiable natural person. For the training of AI systems, there does not seem to be a need to identify the data subject. Therefore, it seems to make sense

26. ANPD. *Guidance guide on legal hypotheses for the processing of personal data: Legitimate Interest*. 2024. Available at: [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/quia\\_legitimo\\_interesse.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/quia_legitimo_interesse.pdf). Accessed on November 3, 2024.

27. GOAL. Building AI Technology for Europeans in a Transparent and Responsible Way. 2024. <https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/>, Accessed on November 4, 2024.

28. SOLOVE, Daniel J; HARTZOG, Woodrow. The Great Scrape: The Clash Between Scraping and Privacy. *SSRN*. 2024. Available at: <http://dx.doi.org/10.2139/ssrn.4884485>. Accessed on: August 2, 2024.

use techniques that ensure that the person is not identified, such as anonymization or pseudonymization.

Privacy Enhancing Technologies techniques (in English: *Privacy-Enhancing Technologies*–PETs), which are a set of tools and methodologies designed to protect the privacy and security of personal data during collection, processing and storage, as well as the use of deep learning that creates synthetic data, can help solve the regulatory problems for the use of personal data in training generative AI.<sup>29</sup>

If the legal hypothesis used is legitimate interest, the right to object is considered necessary (*opt-out*) so that the holder has the option of not having their personal data processed for this purpose.

In this sense, the French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), in a recent public consultation publication<sup>30</sup>, suggested some safeguards in relation to AI training, among which the following stand out: anonymization or pseudonymization, use of synthetic data, greater transparency in data processing, development of more transparent and auditable systems and facilitation of the exercise of rights.

## Final Considerations

The research highlighted enormous regulatory challenges, in terms of data protection and privacy, that must be addressed in order to develop ethical and responsible generative AI solutions that bring trust and benefits to society.

Data protection and privacy cannot be the object of limiting innovation and new business models, however, the processing agent must observe the principles and guarantees provided for in the LGPD to provide an environment of greater trust and security for the development of AI systems.

Data governance, transparency, accountability, and accountability are fundamental pillars for the ethical and legal use of data in generative AI training. These principles ensure that practices comply with laws and regulations and help build an environment of trust and stability for society as a whole.

29. PANGHANGAM. Nivarthi, KS How Privacy-Enhanced Technologies (Pets) are Transforming Digital Healthcare Delivery. *American Scientific Research Journal for Engineering, Technology, and Sciences*, 9(1), 351–361. 2022. Available at: [https://asrjetsjournal.org/index.php/American\\_Scientific\\_Journal/article/view/8268](https://asrjetsjournal.org/index.php/American_Scientific_Journal/article/view/8268) . Accessed on November 4, 2024.

30. CNIL. Relying on the legal basis of legitimate interests to develop an AI system. Available at: <https://www.cnil.fr/en/relying-legal-basis-legitimate-interests-develop-ai-system> . Accessed on 04 Nov 2024.

The use of anonymization or pseudonymization techniques, notably Privacy Enhancement Technologies (PET), use of synthetic data, processing transparency measures and measures to encourage the exercise of rights can support the guarantee of fundamental data protection and privacy rights during the processing of personal data with a view to training generative AI systems.

The ANPD's actions, in the case of changes to Meta's Privacy Policy, are in line with international concerns discussed in academia and public authorities about the excessive collection of data for training generative AI.

Research can evolve to assess opportunities for regulatory solutions and their impacts on fundamental data protection and privacy rights, innovation and socio-economic development.

## References

ANPD. *ANPD determines precautionary suspension of personal data processing for training Meta's AI*. 2024. Available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta> .

Accessed on: August 4, 2024.

ANPD. *Guidance on Legal Hypotheses for the Processing of Personal Data: Legitimate Interest*. 2024. Available at: [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia\\_legitimo\\_interest.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interest.pdf) .

Accessed on: October 28, 2024.

BARRADI, Thomas, OpenAI Offering Media Outlets as Little as \$1M to Use News Articles for AI Models, *New York Post*. 2024.

CARPRARO, Valerio, et al. The impact of generative artificial intelligence on socioeconomic inequalities and policy making. *Pnax Nexus*. 2024, 3, 191 p. Available at: <https://doi.org/10.1093/pnasnexus/pgae191> . Accessed on: July 29, 2024.

CNIL. Relying on the legal basis of legitimate interests to develop an AI system. Available at: <https://www.cnil.fr/en/relying-legal-basis-legitimate-interests-develop-ai-system> . Accessed on 04 Nov 2024.

GOODFELLOW, I., Bengio, Y., & Courville, A. *Deep Learning*. MIT Press. 2016.

<https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/> . Accessed on November 4, 2024.

HUMAN RIGHTS WATCH. Brazil: *Photos of children are being misused to feed AI*. 2024. Available at: <https://www.hrw.org/pt/news/2024/06/10/brazil-childrens-personal-photos-misused-power-ai-tools> . Accessed on: August 2, 2024.

ICO. What methods can we use to provide privacy information? Available at:<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/> . Accessed on: August 3, 2024.

GOAL. Building AI Technology for Europeans in a Transparent and Responsible Way. 2024.

GOAL. *Meta Privacy Policy*. 2024. Available at:<https://pt-br.facebook.com/privacy/genai> . Accessed on: August 4, 2024.

MITCHELL, Tom. *Machine Learning*. 1997. McGraw-Hill.

MOHRI, M; Rostamizadeh, THE; Talwalkar, THE. *Foundations of Machine Learning*. Second Edition. MIT Press. 2018.

OECD. *AI, Data Governance and Privacy*. 2024. Available at:[https://www.oecd.org/en/publications/ai-data-governance-and-privacy\\_2476b1a4-en.html](https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html) . Accessed on: August 4, 2024.

OECD. *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. 1980. Available at:<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188> . Accessed on: November 4, 2024.

Organization for Economic Cooperation and Development (OECD). Intergovernmental economic organization with 38 member countries, founded in 1961 to stimulate economic progress and world trade.

PANGHANGAM, Nivarthi, KS How Privacy-Enhanced Technologies (Pets) are Transforming Digital Healthcare Delivery. *American Scientific Research Journal for Engineering, Technology, and Sciences*, 9(1), 351–361. 2022. Available at:[https://asrjetsjournal.org/index.php/American\\_Scientific\\_Journal/article/view/8268](https://asrjetsjournal.org/index.php/American_Scientific_Journal/article/view/8268) . Accessed on November 4, 2024.

SAÚDE, Sandra; BARROS, João Paulo; ALMEIDA, Inês. Impacts of Generative Artificial Intelligence in Higher Education: Research Trends and Students' Perceptions. *Social Sciences*. 2024, 13, 410 p. Available at:<https://doi.org/10.3390/socsci13080410> . Accessed on: July 27, 2024.

SOLOVE, Daniel J; HARTZOG, Woodrow. The Great Scrape: The Clash Between Scraping and Privacy. *SSRN*. 2024. Available at:<http://dx.doi.org/10.2139/ssrn.4884485> . Accessed on: August 2, 2024.

SPRINGER NATURE. Tools such as ChatGPT threaten transparent science; here are our ground rules for their use. *Nature*. 2023. 613 p. Available at: doi:<https://doi.org/10.1038/d41586-023-00191-1> . Accessed on: August 2, 2024.

EUROPEAN UNION. *Artificial Intelligence Act*. 2024. Available at:<https://artificialintelligenceact.eu/ai-act-explorer/> . Accessed on: August 3, 2024.

EUROPEAN UNION. *Ethics guidelines for trustworthy AI*. 2019. Available at:<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> . Accessed on August 4, 2024.

ZHANG, Peng; BOULOS, Maged N. Kamel. Generative AI in Medicine and Healthcare: Promises, Opportunities and Challenges. *Future Internet*. 2023, 15, 286 p. Available at:<https://doi.org/10.3390/fi15090286> . Accessed on: August 1, 2024.

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

5

# Damage classification arising from incidents

of AI

Vinicius Azevedo Coelho

Summary: Introduction. 1. Incidents arising from artificial intelligence systems. 2. Types of damage related to AI incidents. 3. Levels of criticality of damage in AI incidents. Final considerations. References.

## Introduction

In the networked society, information and communication technologies have revolutionized the way people interact and relate to one another. According to sociologist Manuel Castells, one of the leading theorists of the information age, the digital transformation has profoundly altered human sociability, with impacts that transcend geographical and cultural borders.<sup>2</sup>

Among these technologies, artificial intelligence (AI) stands out as a particularly powerful agent of change. Its rapid and continuous evolution has the potential to reshape entire sectors, from the economy to science, promoting inclusive and sustainable growth and enabling significant scientific advances. In addition, its ability to integrate and analyze data from multiple sources improves decision-making and the automation of complex processes, demonstrating its broad utility in different systems<sup>3</sup>.

For example, in commerce, AI helps automate tasks, personalize customer experiences, and predict market trends.<sup>4</sup> In healthcare, it is used to diagnose diseases, develop treatments and provide personalized care.<sup>5</sup> In transportation, AI is present in the development of autonomous cars, in improving the safety and efficiency of public transportation, and in traffic management.<sup>6</sup> In the environment, it helps monitor air and water quality, develop renewable energy and reduce pollution.<sup>7</sup> In science, it accelerates research, tests

1. Postgraduate student in Digital Law at ITS/UERJ. E-mail:[viniciusazevedocoelho@gmail.com](mailto:viniciusazevedocoelho@gmail.com) .

2. CASTELLS, Manuel. The information age: economy, society and culture, v. 1 - *The network society*. Translated by Roneide Venâncio Majer. 17th ed. New York: Routledge, 2016.

3. BALTRUŠAITIS, T.; AHUJA, C.; MORENCY, LP Multimodal Machine Learning: A Survey and Taxonomy. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 41, no. 2, p. 423-443, 2019. DOI: 10.1109/TPAMI.2018.2798607.

4. For example, AI is already being used to recommend products to customers based on their purchase histories, and to predict demand for products and services.

5. As an illustration, AI is already being used to develop software that can diagnose cancer more accurately than doctors, and to create robots that can perform surgeries more accurately and safely.

6. For example, AI is already being used to develop self-driving cars that can drive without human intervention, and to create systems that can manage traffic in real time to reduce congestion.

7. AI is already being used to develop sensors that can monitor air quality in real time, and to create systems that can generate solar and wind power more efficiently.

hypotheses, discovers new medicines and develops new technologies<sup>8</sup>. These are just a few examples of how AI can transform society. As technology continues to develop, AI will have an even greater impact on our lives.

However, despite its transformative impacts, AI also brings with it a number of risks and ethical challenges. These risks can range from privacy and security concerns to broader social and economic impacts, and can lead to incidents with substantial harm. Understanding and managing these adverse consequences is key to ensuring that the benefits of AI are maximized while its harms are minimized.

AI incidents can be caused by a variety of factors, including systemic vulnerabilities, human error, and cyberattacks. These incidents can cause a range of negative consequences, such as physical and environmental damage, and reputational and financial impacts. The damage can have different levels of criticality, from insignificant impacts to damage to property, health, critical infrastructure, and even human fatalities. In this scenario, assessing and classifying damage is a fundamental part of an effective response to AI incidents, and its primary purpose is to mitigate consequences and protect organizations and users of AI-based systems.

In this context, the general objective of this article will be to map and identify the main concepts related to damages resulting from AI security incidents. Thus, it is expected that it will be possible to categorize and understand incidents involving AI and their main consequences, as well as to develop general frameworks indicating the types of damages resulting from AI incidents and their levels of criticality. The two problem questions that guided the elaboration of this research were: 1. What are the types of damages related to the different AI systems? and 2. What are the levels of criticality of the damages resulting from AI incidents?

This work, then, starts from the central problem of mapping and identifying the types of damage caused by security incidents in artificial intelligence systems, as well as assessing the levels of criticality of these damages. This problem is relevant because the growing adoption of AI systems in various areas of society increases the exposure to risks associated with

8. AI is already being used today to analyze large sets of scientific data, as well as to create models that can predict the behavior of molecules and materials.

security incidents. The lack of a clear and precise classification of these damages makes it difficult to respond appropriately to such incidents, compromising both the mitigation of impacts and the formulation of effective security policies. The research seeks to answer questions about the types of damages that can arise and how they vary in terms of criticality, contributing to an understanding of the challenges posed by AI and to the development of measures that can ensure a safer use of these technologies.

The methodology chosen to seek answers to the problem questions includes a bibliographic review, specifically in relation to the conceptual and terminological basis, using as primary sources texts published by authors specialized in cybersecurity, information technology and artificial intelligence.

In addition, this study also draws on publications from international organizations such as the Organization for Economic Cooperation and Development (OECD), the National Institute of Standards and Technology (NIST) of the United States, and the European Union on AI incidents and their consequences. These organizations have published documents on the topic of information security in AI, which may be useful for researchers and professionals in the field. Still regarding research sources, to search for practical examples of AI incidents, we used the AI Incident Database platform (<https://incidentdatabase.ai>), which collects, categorizes, and shares information about incidents involving artificial intelligence systems. This database serves as a resource for researchers, developers, and policymakers, helping them better understand the harms associated with AI.

The results of this research were structured as follows: the first topic explores the essential definitions for its development, and is dedicated to the definitions of AI incidents and damage. The second topic deals with the types of damage in kind. The third and final topic discusses levels of criticality of damage resulting from AI incidents.

## **1. Incidents arising from intelligence systems artificial**

This topic introduces the fundamental concepts for understanding and developing research. Its purpose is to present notions related to artificial intelligence and briefly address the idea of risks related to systems that use AI, in order to then arrive at a definition of incidents resulting from AI.

For the meaning of artificial intelligence, contributions from authors such as McCarthy, Newell and Simon and Boden were used. For the notions of risk and damage, the theory of German sociologist Niklas Luhmann was used, who emphasizes the importance of an assessment of social impacts in his theory of risk. This approach, with a sociological bias, was preferred over a quantitative treatment of risk, typical of the exact sciences.

The very definition of artificial intelligence is challenging in itself. Maria Regina Rigolon Korkmaz points out that the controversial quest to replicate human understanding appears in various historical records, with the aim of understanding the foundations of thought and memory, whether philosophically, physiologically or biologically. It is no coincidence that the initial definition of artificial intelligence, which has been widely debated, emerged as a specific area of computer science aimed at developing computers that can imitate human intelligence in performing tasks.<sup>9</sup>

This initial definition, proposed by John McCarthy<sup>10</sup>, considered by many to be the creator of the term, describes artificial intelligence as the engineering of intelligent machines. That is, machines that demonstrate characteristics associated with human intelligence. In the infamous conference proposal, McCarthy and his colleagues based their approach on the idea that “any aspect of learning or any characteristic of intelligence can, in principle, be so precisely described that a machine can be created to simulate it.”<sup>11</sup>

A few decades later, Allen Newell and Herbert Simon<sup>12</sup> incorporated the idea of a cognitive system into the definition, indicating a system that can learn and solve problems autonomously. In one of the most influential definitions on the subject, they conceptualized AI as a way of creating intelligent systems<sup>13</sup>.

Margaret Boden, one of today's leading experts in AI, defines AI as the way to create systems that can think, learn and act intelligently.<sup>14</sup>

9. KORKMAZ, Maria Regina Rigolon. *Automated Decisions: Explained, Reviewed and Protected in the Age of Artificial Intelligence*. São Paulo: Thomson Reuters Brazil, 2023, p. 95.

10. McCarthy was an award-winning American computer scientist, and he first used the concept of AI in an invitation to an academic conference on the subject, which was held in the summer of 1956 at Dartmouth University.

11. MCCARTHY, John. *Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. Dartmouth College, 1955.

12. Newell and Simon were American researchers. They received the 1975 Turing Award for their contributions to artificial intelligence as it relates to cognitive science.

13. NEWELL, Allen; Simon, Herbert A. *Computer science as empirical inquiry: Symbols and search*. Communications of the ACM 19.3 (1976): 113-126.

14. BODEN, Margaret A. *Artificial intelligence: A very short introduction*. Oxford University Press, 2018.

These definitions highlight several aspects of AI. McCarthy's definition emphasizes the creation of machines that exhibit intelligent characteristics previously related to human behavior. Newell and Simon's definition emphasizes the creation of systems that can learn and solve problems autonomously. Boden's definition emphasizes the creation of systems that can act intelligently.

It is important to note that there is no consensus on what defines artificial intelligence. Today, the term is considered a broad concept, encompassing quite different applications, whether in relation to specific mathematical structures or their practical uses.<sup>15</sup>

Although different or complementary, these definitions show us the versatility of this new technology, capable of being used in simple or complex systems. Understanding this multivalence of AI systems is relevant for an adequate understanding of the risks and damages arising from each type.

This is because simple uses of AI often involve specific, limited tasks, such as customer service chatbots that use natural language processing to answer frequently asked questions. Another example is product recommendations in e-commerce, where algorithms analyze user purchase history and preferences to suggest items. The risks associated with these simple uses are relatively low, and can include language misunderstandings or inappropriate suggestions, which typically result in minor user dissatisfaction and limited impact.

On the other hand, complex uses of AI involve more sophisticated and integrated systems, such as autonomous vehicles, which use multiple data sources (sensors, cameras, GPS) to navigate and make decisions in real time. Another example is predictive analytics in healthcare, where AI processes large volumes of medical data to predict disease outbreaks or personalize treatments. The risks and harmful consequences of these complex applications are significantly higher, including fatal traffic accidents in the event of an autonomous vehicle failure or incorrect medical diagnoses that can lead to inappropriate treatments. Therefore, while simple systems present lower and more controllable risks,

15. KORKMAZ, Maria Regina Rigolon. *Automated Decisions: Explained, Reviewed and Protected in the Age of Artificial Intelligence*. São Paulo: Thomson Reuters Brazil, 2023, p. 98.

Complex applications require greater robustness, transparency and regulation to mitigate potentially serious impacts.

To understand the risk, within the scope of this study, Niklas Luhmann's social perspective was used.<sup>16</sup> According to the author, risks are inherent to the modernization of society itself, which is increasingly contingent. For Luhmann, the future of society increasingly depends on decision-making: the future becomes a risk as possibilities increase

Luhmann proposes a concept of risk that assumes the existence of uncertainty regarding future damage: we speak of risk when the probable damage is the consequence of an action. For Luhmann, the concept of risk is associated with the condition of decision. Every decision implies the possibility that something will go wrong, that is, that a risk will materialize in damage. Thus, risk is the probability that an undesirable event will occur as a result of a decision.<sup>17</sup> Advanced technologies like AI make social complexity increasingly greater, and make it more difficult to predict and measure consequences.

Therefore, based on Luhmannian theory, risks are an inevitable consequence of the modernization and complexification of society. In the context of artificial intelligence, this perspective is particularly relevant, as the implementation of AI systems in various spheres of modern life exemplifies this increasing complexity. Every application of AI, from simple chatbots to autonomous vehicles, involves decisions that can potentially transform the future into a field of uncertainty. The ability to predict and control the consequences of such decisions becomes increasingly challenging as technology advances, increasing the possibilities and, consequently, the risks.

We have seen that Luhmann argues that risk is inherent in the decision condition, where any choice carries the probability of resulting in harm. Thus, applying this to AI, each implementation of an artificial intelligence system involves decisions about algorithms, data, and application contexts that may fail or produce undesirable results. For example, a biometric-based visual recognition system in public spaces may misidentify individuals, resulting in false accusations or privacy violations. These technological decisions, although designed to improve security and efficiency, carry the risk of materializing significant harms to citizens' freedom and privacy.

16. In the sociology of risk, Luhmann reveals his concern with the lack of precision of the concept and the difficulty that *hard sciences* found to adequately analyze the problem of risk. Their concepts were vague and based on quantitative models. Luhmann then proposes an assessment of risks as a social problem, supported by social factors.

17. LUHMANN, Niklas. *Risk: A Sociological Theory*. New York: Routledge, 1993.

As society becomes more dependent on advanced technologies such as AI, social complexity increases, making it harder to predict and mitigate adverse consequences. The risks associated with complex AI systems, such as autonomous vehicles or surveillance systems, illustrate this difficulty. Uncertainty about future harms is magnified by the contingent nature of technological decisions, where the failure of a system can have catastrophic consequences.

Thus, based on the elements studied so far, we can define risk in AI as the uncertain possibility of an undesirable consequence occurring, resulting from a decision made by a system based on artificial intelligence.

The materialization of risk into harm characterizes an AI incident. According to the CSET taxonomy, harm caused by AI has four elements that, once properly defined, allow the identification of harm caused by AI. These key components serve to distinguish harm from non-harm and harm caused by AI from harm not caused by AI. For there to be harm caused by AI, there must be: (1) an entity that has suffered (this could be a person, thing or place); (2) a harm event or issue that (3) can be directly linked to a consequence of the behavior of (4) an AI system. All four elements must be present for there to be harm caused by AI.<sup>18</sup>

Additionally, according to a study conducted by the OECD to define an AI incident, harm is expressed as the probability that a loss will actually occur.<sup>19</sup> Risk is a function of both the likelihood of an event occurring and the severity of the consequences that would result. In this context, it is necessary to understand and manage risks and harms related to AI to ensure its reliability and safe and responsible use. According to a study by the OECD<sup>20</sup>:

Defining harm and assessing its types, severity levels and other relevant dimensions (e.g. scope, geographic scale, quantification, etc.) is critical to identifying the incidents that lead or could lead to such harm and developing an effective framework to address them.<sup>21</sup>

18. CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET). *CSET V1 AI Annotation Guide*. CSET, 2023.

19. OECD. *Stocktaking for the development of an AI incident definition*. Paris: OECD, 2023. 36 p. Available at: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm> . Accessed on: January 17, 2024.

20. *Ibid.*, p. 8.

21. Free translation of the original: "Defining harm and assessing its types, severity levels and other relevant dimensions (eg scope, geographic scale, quantifiability, etc.) is key to identifying the incidents that lead or might lead to that harm, and to elaborate an effective framework to address them".

It follows, then, that the idea of harm as a consequence of risk is central to understanding AI incidents. Having made these considerations, we move on to - if by the definition of AI incidents.

Amodei et al., in the article *Concrete Problems in AI Safety*, describe AI incidents as events where an artificial intelligence system behaves in an unintended or harmful manner due to issues such as specification flaws, robustness errors, scalability failures, or security complexity<sup>22</sup>.

Crawford and Calo, in *There is a Blind Spot in AI Research*, define AI incidents as events where artificial intelligence technologies cause harm or fail to operate as expected, often due to limitations in research and development that do not fully consider their social and ethical impacts<sup>23</sup>.

In addition to the above authors, some organizations also provide relevant definitions for AI incidents. According to the CSET taxonomy developed for the AI Incident Database, AI incidents involve failures or near-failures in the real world using artificial intelligence systems.<sup>24</sup> In addition, the AI Index Report 2024 – Stanford HAI defines AI incidents as events in which artificial intelligence systems malfunction or behave unexpectedly, resulting in adverse consequences. These incidents may include technical failures, biases in automated decisions, or privacy and security violations.<sup>25</sup> The definition proposed by the OECD for an AI incident says that<sup>26</sup>:

AI Incident: An event in which the development or use of an AI system:

- (i) caused harm to person(s), property or the environment;
- (ii) impacted human rights, including privacy and non-discrimination<sup>27</sup>

22. AMODEI, D. et al. *Concrete Problems in AI Safety*. 2016. Available at: <https://arxiv.org/abs/1606.06565> . Accessed on: August 6, 2024, p. 1-2.

23. Crawford, K., Calo, R. *There is a blind spot in AI research*. *Nature* 538, (2016). <https://doi.org/10.1038/538311a> . Accessed on: August 7, 2024, pp. 311-313.

24. AI Incident Database. *CSET Taxonomy AI Incident Database*. Available at: <https://incidentdatabase.ai/taxonomy/cset/> . Accessed on: August 7, 2024.

25. Stanford HAI. *AI Index Report 2024*. Stanford Institute for Human-Centered Artificial Intelligence, 2024. Available at: [https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI\\_2024\\_AI-Index-Report.pdf](https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf) . Accessed on: August 7, 2024.

26. OECD. *Stocktaking for the development of an AI incident definition*. Paris: OECD, 2023. 36 p. Available at: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm> . Accessed on: January 17, 2024, p. 11.

27. Free translation of the original: "AI Incident: an event where the development or use of an AI system: (i) caused harm to person(s), property, or the environment; or (ii) infringed upon human rights, including privacy and non-discrimination".

Thus, based on the above contributions, for the purposes of this study, an AI incident will be considered as an event or situation in which an AI system fails or behaves in an unexpected manner, resulting in negative consequences. This may include technical errors, malfunctions, incorrect decisions, or biases that lead to harmful outcomes for individuals, organizations, or society at large. Such incidents may occur due to problems in the design, training, implementation, or operation of AI systems. The types of harm related to AI incidents will be addressed in the following topic.

## 2. Types of damages related to AI incidents

The increased use of AI systems around the world leads to an increase in the number of AI systems, which, as seen in the previous topic, can cause real harm to people, organizations and the environment.

The unintended consequences related to AI systems differ from traditional cybersecurity risks in several ways<sup>28</sup>. This difference arises in part from the intrinsic nature of AI systems, which rely heavily on large volumes of data to operate efficiently. This requirement in itself introduces issues such as data quality and bias, which can distort the results and decisions made by AI. The accuracy and fairness of data thus become critical issues, directly impacting the effectiveness and reliability of AI systems.

Furthermore, the inherent complexity of AI systems and their reliance on data for training and decision-making create additional challenges, especially in terms of privacy and security. Unlike traditional software, AI systems can be opaque, making it difficult for users to understand how decisions are made and the data used. This opaqueness, coupled with complexity, broadens the spectrum of potential incidents, which can range from affecting a small number of individuals to having significant impacts across multiple sectors, with varying degrees of harm. Managing these risks requires a more sophisticated approach, involving not only technical aspects but also ethical and regulatory considerations.

So far, we have established the concept of risk as potential damage. When this risk materializes, we are faced with real damage. The definitions

28. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST AI 100-1: *Artificial Intelligence Risk Management Framework*. Gaithersburg, MD: NIST, 2020. Available at: <https://doi.org/10.6028/NIST.AI.100-1> . Accessed on January 17, 2024.

Definitions of actual harm in standards and regulations are highly context-dependent and typically focus on physical injury or damage to the health of persons, property or the environment (IEC 61508-1:2010, ISO/IEC 51:2014, ISO 26262-1:2018). In some cases, such as in regulations on personal data protection, they may refer to losses caused by data breaches, including physical, material or non-material harm to natural persons, such as loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage for the natural person concerned.

The research center focused on emerging technologies, CSET, in its framework on AI harms, divides these harms into two broad categories: tangible harms and intangible harms.<sup>29</sup>

Tangible damage is damage that is material in nature and is therefore observable, verifiable, and definitive. Common examples include physical injury (including death), financial loss, and damage to private or public property. This type of damage is usually quantifiable and can be expressed in monetary terms. Examples include damage to a car, a broken arm, or loss of income.

Intangible harm, in contrast, is generally not directly observable. Although the event causing the harm may be observable and its effects and consequences may be expressed in an observable manner, the harm itself is not. Intangible harm may include, but is not limited to, mental/psychological harm, pain and suffering, damage to intangible property (e.g., theft of intellectual property, damage to a company's reputation), and loss of trust or confidence.

The figure below, adapted and translated from the CSET material, indicates the types of damage categorized as tangible and intangible.

29. HOFFMANN, Mia; PHRASE, Heather. *Adding Structure to AI Harm: An Introduction to CSET's AI Framework*. Georgetown: Center for Security and Emerging Technology, 2023. Available at: <https://cset.georgetown.edu/wp-content/uploads/20230022-Adding-structure-to-AI-Harm-FINAL.pdf>. Accessed on: August 6, 2024, p. 9.

**Table 1 – Tangible and intangible damages divided into categories (CSET)<sup>30</sup>**

Tangible damage category	Category of intangible damages
Damage to Health/Physical Safety	Harmful content
Damage to infrastructure	Differentiated Treatment
Damage to material property	Human/Civil Rights
Financial loss	Democratic Norms
Environmental damage	Privacy
Others	Others

According to the CSET, damages can be classified, according to their types, into:

Regarding tangible damages:

- **Harm to health/physical safety:** include death, injury or reduced life expectancy.
- **Damage to infrastructure:** involve the network of roads, railways, public services and buildings needed to maintain commerce, transportation, political structures and the normality of daily life. Infrastructure can be damaged by destruction, reduced capacity or reduced effectiveness
- **Damage to physical property:** referring to the destruction of a physical object.
- **Financial loss:** covers any loss of an economic nature that does not arise from injury or damage.
- **Environmental damage:** related to ecological degradation that results in pollution, destruction of habitats, waste of natural resources or industrial accidents.

About intangible damages:

- **Harmful content:** involves deepfakes, misinformation, cyberbullying, impersonation, insults, threats of violence, promotion of eating disorders or self-harm, extremist content, disinformation, sexual abuse material and fraudulent emails

30. Adapted by the author from HOFFMANN, Mia; FRASE, Heather. *Adding Structure to AI Harm: An Introduction to CSET's AI Framework*. Georgetown: Center for Security and Emerging Technology, 2023. Available at: <https://cset.georgetown.edu/wp-content/uploads/20230022-Adding-structure-to-AI-Harm-FINAL.pdf> . Accessed on: August 6, 2024.

- **Differentiated treatment:** covering issues of bias and fairness related to AI. However, the bias must be associated with a group that has a protected characteristic. Differential treatment based on protected characteristics often overlaps with or occurs with a violation of civil rights.
- **Violation of human rights, civil liberties, civil rights or democratic norms:** related to violations of the protection and promotion of fundamental rights and freedoms.
- **Privacy:** can occur through unwarranted surveillance, data breaches, or collection and use of personal information without consent.
- **Other damages:** other damages that do not fit into any of the other categories mentioned.

This CSET taxonomy is used as the main reference for other specific and relevant studies on the topic, such as the OECD proposal, which presents similar categories, as indicated in the table below:

**Table 2 – Types of damage related to AI incidents<sup>31</sup>**

Damage Type	Description	Example
Physical damage	Refers to bodily injury or direct physical harm caused to a person. It may involve harm to health or safety, or other negative impacts on physical health.	Failures in industrial robots, causing work accidents.
Environmental damage such	They indicate undesirable consequences for the environment such as soil contamination, air pollution or water pollution.	Use of AI in industrial processes, resulting in pollutant leakage.
Financial damages- pink, including property	Includes economic losses, financial losses or negative impacts on personal or business finances. It may involve material damage to physical properties such as buildings, vehicles, equipment, among others.	Failures in automated trading systems, resulting in financial losses.

Continued

31. Prepared by the author, based on OECD. *Stocktaking for the development of an AI incident definition*. Paris: OECD, 2023. 36 p. Available at: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm>. Accessed on: January 17, 2024.

**Table 2 – Types of damage related to AI incidents**

Continuation

Damage Type	Description	Example
Reputational damage national	It refers to the loss of trust, credibility or respect that an organization, institution or individual may suffer as a result of an error, failure or misuse of AI-based systems.	AI algorithm that unfairly discriminates against customers, causing a negative perception of the institution.
Damage to the interest- if public	Refers to damage that affects the protection of critical infrastructure and social institutions.	AI used to manipulate public information, affecting trust in government institutions
Restrictions on civil liberties	Harms that result in the restriction or violation of an individual's civil rights, such as discrimination, privacy violations, among others.	Facial recognition systems leading to mass surveillance and invasion of privacy.
Psychological damage gical	Refers to emotional, mental or psychological damage, such as stress, trauma, anxiety, among others.	Artificial intelligence in social networks, contributing to anxiety and depression.

Classifying harms resulting from AI incidents is essential to understanding and effectively mitigating the risks associated with the use of this technology. Categorizing harms, whether in terms of their tangibility or intangibility, or in terms of their type, allows for a more accurate and detailed analysis of the consequences of incidents. Tangible harms, such as physical injuries, financial losses, and property damage, are more easily quantifiable and verifiable, which facilitates immediate response and corrective measures. On the other hand, intangible harms, such as psychological distress, loss of trust, and privacy violations, although more difficult to quantify, are equally important and require specific approaches to be adequately addressed.

Clear harm classification also improves the collection and analysis of data on AI incidents, enabling the identification of patterns and trends. This contributes to the development of best practices and security policies, helping to prevent similar incidents from recurring. In addition, detailed categorization of harm types facilitates communication between different stakeholders, including AI developers, end users, and researchers, fostering a common understanding of the risks and consequences associated with AI use.

In the regulatory context, the classification of harms arising from AI incidents plays an important role in the formulation of effective laws and policies. Regulators need an accurate understanding of the types of harms that can occur in order to establish appropriate safety and liability standards. Thus, classifying harms not only improves incident response and mitigation, but also supports the creation of a robust regulatory framework that protects society from potential AI risks.

### 3. Damage criticality levels in AI incidents

A second relevant factor to be considered in relation to harms resulting from AI concerns their criticality. Assessing the criticality of harms caused by Artificial Intelligence (AI) incidents is a fundamental aspect of risk management in this area. A stratified approach to classifying the criticality of harms allows for a more accurate and differentiated analysis of the impacts that these incidents can generate. This is essential not only for the development of appropriate regulatory policies, but also for the implementation of effective preventive and corrective measures.

Additionally, categorization into levels of criticality plays a critical role in prioritizing incident responses. By identifying and focusing on the most serious incidents, it is possible to allocate resources more efficiently, aiming to protect public interests and safeguard individual rights and security. This classification system also promotes clear communication about the risks and consequences associated with the use of AI, reinforcing transparency and accountability in the management of this technology.

According to the aforementioned OECD study, there is currently no widely accepted and comprehensive classification system to account for all dimensions of harm caused by AI systems (i.e., in terms of scope, scale, severity, types and impacts, etc.). An important step in this direction is the taxonomy developed by CSET, which proposes five levels of criticality of harm caused by AI systems, namely, negligible harm (*negligible*), light damage (*minor*), moderate damage (*moderate*), serious damage (*severe*) and critical damage (*critical*). Based on these levels, we have prepared the table below:

**Table 3 – Damage criticality levels in AI incidents<sup>32</sup>**

Criticality	Description	Examples
<b>Negligible</b> <i>(Negligible)</i>	Minimal damage, easily remedied.	Rounding error in low-impact financial calculations by an AI system.
<b>Light</b> <i>(Minor)</i>	Damage limited to property, social stability, political system or civil liberties.	Content moderation AI failing to detect and remove offensive posts on a social network, causing limited discomfort.
<b>Moderate</b> <i>(Moderate)</i>	Injury or near injury to human beings. Significant damage to financial interests.	AI system for medical diagnosis providing incorrect result, resulting in unnecessary treatment. Error in an AI algorithm used for automated trading in the stock market.
<b>Serious</b> <i>(Severe)</i>	Serious injury or near death of human beings. Significant disruption to financial interests on a regional or national scale. Serious damage to property or the environment.	AI failure in autonomous vehicles leads to traffic accident with serious injuries. Failure in AI systems used to forecast and manage a city's electrical grids.
<b>Critical</b> <i>(Critical)</i>	Death or near death of many human beings. Critical disruption to financial interests on a national or global scale.	Failure in AI systems responsible for managing critical infrastructures, such as nuclear power plants or dams. AI-based high-frequency trading systems collapse, causing a stock market crash with global economic impact.

The relevance of classifying harm can be exemplified by the provisions of art. 73 of the EU IA Act. Although it does not cover all the levels of criticality encompassed by the CSET taxonomy, the European regulatory framework typifies the legal obligation to report serious incidents resulting from AI to the supervisory authorities. According to the EU IA Act (art. 3, point 49, b),

(49) “serious incident” means an incident or malfunction of an AI system that, directly or indirectly, leads to any of the following: (a) the death of a person or damage to

32. Prepared by the author, based on OECD. *Stocktaking for the development of an AI incident definition*. Paris: OECD, 2023. 36 p. Available at: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm>. Accessed on: January 17, 2024.

serious harm to the health of a person; (b) a serious and irreversible disruption to the management or operation of a critical infrastructure; (c) a breach of obligations under Union law designed to protect fundamental rights; (d) serious damage to property or the environment.

In short, categorizing harm is crucial to ensuring compliance with the provisions of the AI Act, which requires responses that are proportionate to the severity of incidents, contributing to transparency and effectiveness in risk management and response to AI incidents. This could serve as a basis for future legislation as AI incidents become more frequent and regulations evolve to keep pace with technological advances.

## Final considerations

Upon concluding this introductory study on incidents arising from Artificial Intelligence (AI), several reflections emerge, integrating the theoretical and practical aspects explored in the previous topics.

First, the conceptualization of AI itself, as presented by McCarthy, Newell, and Simon and Boden, establishes an essential theoretical framework. These definitions, which emphasize the engineering of intelligent machines, the autonomy of cognitive systems, and the capacity of systems to think and act intelligently, are fundamental to understanding the basis of its functioning and serve as a starting point for reflecting on the risks and harms associated with these systems. Luhmann's approach to the concept of risk, which considers the complexities and uncertainties associated with decisions, provides a critical lens for assessing the risks and harms of AI in a societal context.

This study has highlighted how AI, despite its transformative potential in sectors as diverse as healthcare, transportation and the environment, carries inherent risks and consequences. These consequences, varying in likelihood and impact, can affect individuals, groups, environments and societies in significant ways. The analysis of the types of harms related to AI, discussed in the second topic, revealed a range of potential consequences, from physical and environmental harms to financial, reputational and psychological impacts.

The definition of damage criticality levels, as proposed by the CSET taxonomy, illustrates the need for a well-founded and adaptable regulatory framework. Establishing an accurate classification of damages

at criticality levels not only helps in accurately assessing impacts, but also guides in formulating appropriate and prioritized responses to AI incidents.

In summary, this work reveals the complexity and dynamism of the challenges presented by AI. While the technology offers unprecedented opportunities for advancement and innovation, it also requires careful reflection on the risks and responsibilities associated with its use.

Looking ahead to future work, we intend to continue exploring this topic, with a particular focus on the assessment of AI incidents. Deepening our understanding of how to best manage risks and mitigate harm will be essential to ensuring the safe and responsible use of AI, aligned with ethical and social values. Thus, the study of risks and harms associated with AI remains not only relevant, but essential, as we move into the era of digital transformation.

## References

AI Incident Database. *CSET Taxonomy AI Incident Database*. Available at: <https://incidentdatabase.ai/taxonomy/cset/> . Accessed on: August 7, 2024.

AMODEI, D. et al. *Concrete Problems in AI Safety*. 2016. Available at: <https://arxiv.org/abs/1606.06565> . Accessed on: August 6, 2024.

BALTRUŠAITIS, T.; AHUJA, C.; MORENCY, LP Multimodal Machine Learning: A Survey and Taxonomy. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 41, no. 2, p. 423-443, 2019. DOI: 10.1109/TPAMI.2018.2798607.

BODEN, Margaret A. *Artificial intelligence: A very short introduction*. Oxford University Press, 2018.

BRAZIL. Law No. 13,709 of August 14, 2018. *General Personal Data Protection Law (LGPD)*. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709compilado.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm). Accessed on January 17, 2024 .

Crawford, K.; Calo, R. *There is a blind spot in AI research*. *Nature* **538**, 311–313 (2016). <https://doi.org/10.1038/538311a> . Accessed on: August 7, 2024.

CASTELLS, Manuel. *The information age: economy, society and culture*, v. 1 – *The network society*. Translated by Roneide Venâncio Majer. 17th ed. New York: Routledge, 2016.

CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET). *Understanding AI Harms: An Overview*. Available at: <https://cset.georgetown.edu/article/understanding-ai-harms-an-overview/> . Accessed on: August 6, 2024.

CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET). *CSET V1 AI Annotation Guide*. CSET, 2023.

HOFFMANN, Mia; FRASE, Heather. *Adding Structure to AI Harm: An Introduction to CSET's AI Framework*. Georgetown: Center for Security and Emerging Technology, 2023. Available at: <https://cset.georgetown.edu/wp-content/uploads/20230022-Adding-structure-to-AI-Harm-FINAL.pdf> . Accessed on: August 6, 2024.

KORKMAZ, Maria Regina Rigolon. *Automated Decisions: Explained, Reviewed and Protected in the Age of Artificial Intelligence*. São Paulo: Thomson Reuters Brazil, 2023.

LUHMANN, Niklas. *Risk: A Sociological Theory*. New York: Routledge, 1993.

MCCARTHY, John. *Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. Dartmouth College, 1955.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST AI 100-1: *Artificial Intelligence Risk Management Framework*. Gaithersburg, MD: NIST, 2020. Available at: <https://doi.org/10.6028/NIST.AI.100-1> . Accessed on January 17, 2024.

NEWELL, Allen; Simon, Herbert A. *Computer science as empirical inquiry: Symbols and search*. Communications of the ACM 19.3 (1976): 113-126.

OECD. *Stocktaking for the development of an AI incident definition*. Paris: OECD, 2023. 36 p. Available at: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm> . Accessed on: January 17, 2024.

REGULATION (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Available at: <https://eurlex.europa.eu/legalcontent/PT/TXT/?uri=CELEX%3A32016R0679> . Accessed on: August 7, 2024.

Stanford HAI. *AI Index Report 2024*. Stanford Institute for Human-Centered Artificial Intelligence, 2024. Available at: [https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI\\_2024\\_AI-Index-Report.pdf](https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf) . Accessed on: August 7, 2024.

EUROPEAN UNION. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 9 August 2024 laying down harmonised rules on artificial intelligence (AI Act) and amending certain Union legislative acts*. Official Journal of the European Union, Brussels, 2024. Available at: <https://eurlex.europa.eu/eli/req/2024/1689> . Accessed on: October 6, 2024.

**PL 2.338/2023: a study  
on the provisions of  
copyright**

Nina Ramalho Pinheiro

Summary: Introduction. 1. The Copyright Law (Law No. 9,610/1998) and concepts - key: protected works, moral and patrimonial rights and limitations. 2. Copyright and related rights in light of the 4th substitute of PL 2.338/23 and the proposed amendments. 2.1. Rights of holders and limitations on copyright. 2.2. Remuneration. 2.3. Transparency and regulatory sandbox. 2.4. Personality rights and use of image. Final considerations. References.

## Introduction

Advances in the development and use of artificial intelligence (AI) systems are noticeable at a global level and the accelerated incorporation of this technology in the most diverse areas attracts regulatory challenges that involve addressing issues such as competitiveness, risk of economic concentration, impacts on employment/work, etc.

The need to establish clear rules for the development and application of technology in a safe, responsible, sustainable manner and in compliance with fundamental rights gives rise to different regulatory models (e.g. general/sectoral, principle-based, vertical/horizontal) based on the strategies of each national policy.

In Brazil, although there are previous initiatives<sup>2</sup>, it was with PL 21/2020, authored by deputy Eduardo Bismarck, that the debates on the subject gained more defined contours, culminating, in 2022, in the formation of the Senate Federal Jurists Committee to prepare a draft of the substitute to instruct the regulation of artificial intelligence in the country<sup>3</sup>.

The work of the Commission (CJUSBIA) marks a significant advance in the structuring of legal guidelines for AI in Brazil, since, based on public hearings and consultations with more than fifty experts from different sectors (public authorities, business, civil society and academic community), the proposal for the substitute was presented, converted into PL n° 2338/2023.<sup>4</sup>

1. Bachelor of Laws from the Pontifical Catholic University of São Paulo (PUC/SP). Postgraduate degree in Civil Procedure from FGV Direito SP (FGV LAW). Postgraduate degree in Digital Law from the Institute of Technology and Society (ITS Rio), in partnership with the State University of Rio de Janeiro (UERJ) and the Center for Studies and Research in Legal Education (CEPED). Lawyer in the area of Strategic Litigation, focusing on issues involving Digital Law, Technology and Data Protection. Contact: [nina.rpinheiro@gmail.com](mailto:nina.rpinheiro@gmail.com).

2. Example: PLs 5051/20219 and 5691/2019, which establish general principles for the use of AI.

3. Based on the assessment of Bills No. 5051/2019, 21/2020 and 872/2021.

4. BRAZIL. Federal Senate. *Bill No. 2338, of 2023*. Provides for the use of Artificial Intelligence. Brasília: Federal Senate, 2023. <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Accessed on: July 15, 2024.

Bill No. 2338/2023 can be interpreted as a step forward, as it reflects a long process of multisectoral discussion, and sought to reconcile an approach<sup>5</sup> risk-based regulatory action with the promotion of the protection of fundamental rights, without ignoring the promotion of innovation and the accountability of agents.

Despite the progress, numerous points have still been subject to maturation and debates led by Technical Notes<sup>6</sup>, issued by entities representing society, and contributions in public hearings. As a result, by November 2024, 150 proposed amendments and four substitutes to the text of the law were presented to the Federal Senate.

Among the topics that generate the most disagreement and uncertainty, the protection of copyright in the development and use of artificial intelligence systems, especially generative intelligence, stands out. The topic is the subject of nineteen amendments<sup>7</sup>, to date, of which two have been accepted<sup>8</sup>, one was partially accepted<sup>9</sup>, one was removed by the author<sup>10</sup> and fifteen were rejected<sup>11</sup>.

From this perspective, this study's main objective is to analyze these amendments, the justifications presented, the arguments for approval or not and the change in the wording of the related articles in PL 2,338/23, in order to identify the main points of discussion for improving the regulation regarding copyright protection.

To this end, the primary research material consists of the amendments that deal with copyright as opposed to the articles of "Section IV – Copyright and related rights" of the 4th amendment of Bill 2,338/23, of November 28, 2024. The secondary material consists of guidelines applicable to the topic, specific legislation, foreign regulatory experience, supporting bibliography and technical notes issued by competent entities. From the primary material, we sought to extract the macro themes addressed, hereinafter referred to as "points", which will be analyzed individually based on the identified problem-issues and possible solutions considering the secondary material analyzed.

5. PUBLIC POLICY AND INTERNET LABORATORY (LAPIN). *Bill No. 2338/2023 - Technical Note*. August, 2023. Available at: <https://direitosnarede.org.br/2023/08/23/coalizao-direitos-na-rede-divulga-nota-tecnica-sobre-o-pl-2338-2023-which-seeks-to-regulate-it/>. Accessed on: 07/13/2024.

6. For example: IDEC, ANDP, Rights on the Net Coalition.

7. Amendments Nos. 4, 6, 20, 24, 36, 44, 45, 55, 56, 61, 72, 102, 103, 109, 110, 112, 118, 119, 128.

8. Amendments No. 4 and 44.

9. Amendment No. 45.

10. Amendment No. 24.

11. Amendments Nos. 6, 20, 36, 40, 55, 56, 61, 72, 102, 103, 109, 110, 112, 118, 119, 128.

To present the study, the first chapter was chosen to address, based on the mapping of the Copyright Law (Law No. 9,619/98 or “LDA”), essential definitions for understanding its scope, such as protected work, moral and patrimonial rights, and related rights. This chapter also presented basic concepts of artificial intelligence, introducing the definition of model training and data and text mining. In the second chapter, the four points selected from the analysis of the primary research material, namely (i) rights of holders and limitations on copyright, (ii) remuneration, (iii) transparency and regulatory sandbox, and (iv) personality rights and use of image, are now addressed based on the wording of the articles of the 4th substitute of the PL and the related amendments presented. The study concludes with an assessment of the advances and uncertainties involving the topic and future perspectives for facing the challenges identified.

## **1. The Copyright Law (Law No. 9,610/1998) and key concepts: protected works, moral and patrimonial rights and limitations**

Before delving into the analysis of the provisions of Bill 2,338/23 that seek to establish guidelines for establishing copyright in the context of artificial intelligence, it is important to make brief comments on the special legislation applicable to the topic, in order to provide essential definitions for understanding the points addressed in the Bill.

In Brazil, the protection of copyright and related rights is established in the Copyright Law (Law No. 9,619/98). To understand the object of copyright protection, based on art. 7 of the LDA<sup>12</sup>, it is clear that creations of the spirit expressed by any means or support will be protected, regardless of whether they are related to the field of letters, arts or sciences. From the legal provision, it is clear that concepts, styles or ideas will not be protected, but only the externalized expression of these elements.

12. Art. 7º Intellectual works protected are creations of the mind, expressed by any means or fixed in any tangible or intangible medium, known or to be invented in the future, such as: I - the texts of literary, artistic or scientific works; II - conferences, speeches, sermons and other works of the same nature; III - dramatic and dramatic-musical works; IV - choreographic and pantomime works, the stage performance of which is fixed in writing or in any other form; V - musical compositions, whether or not with lyrics; VI - audiovisual works, with or without sound, including cinematographic works; VII - photographic works and those produced by any process analogous to photography; VIII - works of drawing, painting, engraving, sculpture, lithography and kinetic art; IX - illustrations, geographical maps and other works of the same nature; X - projects, sketches and plastic works concerning geography, engineering, topography, architecture, landscaping, scenography and science; XI - adaptations, translations and other transformations of original works, presented as new intellectual creations; XII - computer programs; XIII - collections or compilations, anthologies, encyclopedias, dictionaries, databases and other works, which, by their selection, organization or arrangement of their content, constitute an intellectual creation. (BRAZIL. Presidency of the Republic. Law No. 9,610, of February 19, 1998. Amends, updates and consolidates the legislation on copyright and provides other measures.) Available at: [https://www.planalto.gov.br/ccivil\\_03/leis/l9610.htm](https://www.planalto.gov.br/ccivil_03/leis/l9610.htm) . Accessed on July 3, 2024.

Although the legislation is not express, and there are opposing positions, the majority doctrine also defends the originality of the work as a requirement for the granting of legal protection. Such originality, as Sérgio Branco points out,<sup>13</sup> should not be confused with “absolute novelty”, and should be understood as the element capable of differentiating a given work from others, due to the intellectual and creative effort of the author.

In addition to these points, the protection of a work must also observe the term of protection established by law, currently limited to 70 years from January 1st of the year following milestones such as: death (works in general), publication (anonymous, pseudonymous or posthumously published works) and dissemination (collective, audiovisual and photographic works), period after which the work enters the public domain.

Although art. 7 of the LDA lists types of protected works, considering the mutability associated with external factors such as cultural issues and technological development, specialized doctrine argues that the list presented is exemplary, so that, if the essential requirements presented here are met, the work will have copyright protection.

In addition to the object of protection, the LDA defines that protected works need an author, responsible for holding creative control of the work.<sup>14</sup> According to art. 11 of the LDA, the author is the “natural person who creates a literary, artistic or scientific work”.

As Luca Schirru suggests<sup>15</sup>, although technological development and market interest attract other forms of creation, calling into question the individual and human character attributed to authorship, the concept of author reproduced in the law, as rightly observed by Guilherme Carboni<sup>16</sup>, started from the conception of Romanticism reproduced in the Berne Convention (1886), from which, assuming that works would be a true extension of the personality of their creator, the granting of exclusive rights to the natural person author over his works was justified.

13. WHITE, Sergio. *Copyright on the Internet and the use of other people's works*. Rio de Janeiro: Lumen Juris, 2007. Available at: <https://repositorio.fgv.br/items/9d286b3c-c77e-46f2-ad95-1bc48debd48c> . Accessed on: July 13, 2024.

14. CANTALI, Fernanda Borghetti. Artificial intelligence and copyright: disruptive technology requiring reconfiguration of legal categories. *Journal of Law, Innovation, Intellectual Property and Competition*. Porto Alegre. v. 4. p. 1–21. Jul/Dec. 2018. Available at: <https://www.indexlaw.org/index.php/revistadipic/article/view/4667/pdf> . Accessed on: July 20, 2024.

15. SCHIRRU, Luca. *Copyright and artificial intelligence: authorship and ownership in AI products*. Thesis (PhD in Public Policies, Strategies and Development) - Institute of Economics, Federal University of Rio de Janeiro, Rio de Janeiro, 2020. P. 99. Available at: [https://www.ie.ufrj.br/images/IE/PPED/Teses/2020/Vers%C3%A3o%20final\\_Tese%20Luca\\_PDFa.pdf](https://www.ie.ufrj.br/images/IE/PPED/Teses/2020/Vers%C3%A3o%20final_Tese%20Luca_PDFa.pdf) . Accessed on: July 13, 2024.

16. CARBONI, Guilherme. *Copyright, Diversity of Cultural Expressions and Plurality of Authorships*. In: *Intellectual Property Law, Vol II: studies in honor of Father Jorge Hammes* (Org. by Luiz Gonzaga Silva Adolfo and Marcos Wachowicz). Curitiba: Juruá. 2014.

In order to understand the exclusivity of the rights granted to the author, it is essential to define the nature of these rights. Although it is not a peaceful understanding, the LDA adopted the dualist theory, which provides for two distinct categories of rights over the work: the moral order and the patrimonial order.

Moral rights, dealt with in articles 24, 25, 26 and 27 of the LDA, would result from the projection of the author's personality in the work<sup>17</sup> due to the indissoluble bond<sup>18</sup> between the two. In this context, they reflect the author's relationship with the work itself and include the right to indicate authorship<sup>19</sup>, circulation control<sup>20</sup> and alteration of the work<sup>21</sup>.

Although the conceptualization of the moral rights of authors as personality rights is questionable<sup>22</sup>, since they are not innate to the individual, manifesting themselves only from the creation of a protected work, by force of art. 27 of the LDA, said rights are also inalienable, irrevocable, imprescriptible and unattachable.

In turn, patrimonial rights, which can be transacted and transferred for a fee or free of charge, partially or in full, refer to the forms of economic exploitation of the work based on the exercise of the powers of the author or owner.<sup>23</sup> to use, enjoy and dispose of the work before it falls into the public domain.

As Eliane Abrão defends<sup>24</sup>, such rights may also be considered exclusive, since, by force of art. 28 of the LDA, the modalities of use of the work provided for in art. 29 of the LDA, among which the reproduction, editing, adaptation, translation, distribution and inclusion of the work in a database stand out, will depend on prior and express approval of the author/holder.

In addition to copyright, the LDA, in articles 89 to 96, establishes related rights to guarantee the participation and remuneration of artists in future uses of a work in which they participated. This includes the rights of artists

17. SOUZA, Allan Rocha de. Author's moral rights. *Civilistica.com*. Rio de Janeiro, a. 2, n. 1, Jan.-Mar./2013. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/73/53> . Accessed on: July 27, 2024.

18. STAUT JUNIOR, Sergio Said. *Copyright: between social relations and legal relations*. Mill of the Verb. Curitiba. 2006.

19. Right to claim authorship of your work and have your name or pseudonym credited (art. 24, I and II, LDA).

20. Right to keep the work unpublished and to withdraw it from circulation (art. 24, III and VI, LDA).

21. Aiming to ensure the integrity of the work before third parties, while at the same time giving the author the possibility of altering it even after it has been put into circulation (art. 24, IV and V, LDA).

22. WHITE, Sergio. *Copyright*. 1st ed. Rio de Janeiro: Editora FGV. 2009. p. 50. Available at: <https://repositorio.fgv.br/server/api/core/bitstreams/3df3edc6-9a6f-486d-bff8-c1a717da24b4/content> . Accessed on: July 13, 2024.

23. Given the possibility of transferring rights, the owner will not always be the author of the work, and he may assume original ownership of the work as a result of legal transactions, death or legal determination.

24. ABRAHAM, Eliane. *Copyright and related rights*. Sao Paulo: Ed. of Brazil, 2002.

performers, phonographic producers and broadcasting companies, with regard to the interpretation, performance or broadcasting of a work.

As is the case with copyright, holders of related rights are also granted the exclusive right to authorize or prohibit the recording, reproduction, performance and public communication of the work; the transmission, retransmission and fixation of interpretations/broadcasts; the provision to the public for access at any time and place; and any other form of use of their interpretations or performances.

Despite protecting the author of the work, even as a way of stimulating diversity and the creative economy, the rights and protection conferred by the LDA are not absolute, being mitigated from the perspective of public interest and the promotion of other fundamental rights (e.g. culture, accessibility, education), under the terms of articles 46, 47 and 48 of the law.

These provisions provide for situations in which a protected work may be used without prior authorization from the author/owner, without this implying a violation of the law or the rights of third parties. For example, it is permitted to quote short excerpts from a literary work in an academic book for the purposes of criticism or study, educational institutions may reproduce parts of works for exclusive use in teaching activities, the reproduction of news or informative articles in the press is authorized, paraphrases and parodies are permitted as long as they are not true reproductions of the original work and do not cause it to be discredited, etc.

In the context of copyright protection applied to the use, development and training of artificial intelligence systems, the interpretation of these limitations and their specificity is relevant.

Although it is not unanimous<sup>25</sup>, the extensive interpretation of legal limitations in light of the federal constitution has gained strength as a way of reflecting technological evolution, in order to encompass new forms of creation and overcome the apparent obsolescence of current legislation<sup>26</sup>.

To understand the provisions covered in “Section IV – Copyright and related rights” of the 4th amendment to Bill 2,338/23, it is also important to understand concepts such as: artificial intelligence system; AI developer and agent; and text and data mining process.

25. Authors such as Carlos Alberto Bittar and Plínio Cabral defend the restrictive interpretation of limitations.

26. SCHIRRU, Luca. *Copyright and artificial intelligence: authorship and ownership in AI products*. Thesis (PhD in Public Policies, Strategies and Development) - Institute of Economics, Federal University of Rio de Janeiro, Rio de Janeiro, 2020. P. 157. Available at: [https://www.ie.ufrj.br/images/IE/PPED/Teses/2020/Vers%C3%A3o%20final\\_Tese%20Luca\\_PDFa.pdf](https://www.ie.ufrj.br/images/IE/PPED/Teses/2020/Vers%C3%A3o%20final_Tese%20Luca_PDFa.pdf). Accessed on: July 13, 2024.

In the draft regulation an AI system is defined<sup>27</sup> as a machine-based system, with different degrees of autonomy, capable of inferring from sets of data and information and generating results such as predictions, recommendations or decisions.

In order to perform their functions, most artificial intelligence systems are made up of algorithms capable of learning from a database (*machine learning*)<sup>28</sup>, and can sometimes process this data in a similar way to neural networks (*deep learning*)<sup>29</sup>.

Regardless of how the system operates and learns, the success and accuracy of predictions, recommendations and decisions depends on a large volume of input data, used to train algorithms, identify significant patterns and improve system performance.

It is in this context that text and data mining (TDM)<sup>30</sup>, automated technique for extracting large volumes of data, directly or through other tools, to identify patterns and correlations<sup>31</sup>, becomes relevant, as it is from obtaining information extracted from immense amounts of data<sup>32</sup> that will be obtained *insights* for use in research, development or application in artificial intelligence systems.

From a copyright perspective, although there are those who defend the legality of text and data mining regardless of express legal provision, as it involves a non-expressive use from which factual elements and patterns are extracted<sup>33</sup> – not protected by copyright

27. Art. 4 [...] I – artificial intelligence system: machine-based system that, with different degrees of autonomy and for explicit or implicit purposes, infers, from a set of data or information it receives, how to generate results, in particular, prediction, content, recommendation or decision that may influence the virtual, physical or real environment; (BRAZIL. Federal Senate. Bill No. 2338, of 2023. Provides for the use of Artificial Intelligence. Brasília: Federal Senate, 2023. <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233> . Accessed on: November 29, 2024.)

28. In the original: “Machine Learning: algorithms that analyze data, learn from it, and then apply what they have learned to make informed decisions. They use features extracted from data by humans and improve with experience” (CERON, Rodrigo. *AI, machine learning and deep learning: What's the difference?* IBM, 5 Dec 2019, free translation). Available at: <https://www.ibm.com/blog/ai-machine-learning-and-deep-learning-whats-the-difference/> . Accessed on July 13, 2024.

29. In the original: “Deep Learning: neural network algorithms that learn by themselves about the relevant characteristics of the data. Able to adapt through repetitive training to discover hidden patterns and insights” (CERON, Rodrigo. *AI, machine learning and deep learning: What's the difference?* IBM, 5 Dec 2019, free translation). Available at: <https://www.ibm.com/blog/ai-machine-learning-and-deep-learning-whats-the-difference/> . Accessed on July 13, 2024.

30. Text and Data Mining.

31. Art. 4 [...] XIII - text and data mining: process of extraction and analysis with a high degree of automation of large amounts of data, carried out directly on primary data, or indirectly from another tool, from which patterns and correlations are extracted that will generate relevant information for research, development or use of artificial intelligence systems. (BRAZIL. Federal Senate. Bill No. 2338, of 2023. Provides for the use of Artificial Intelligence. Brasília: Federal Senate, 2023. <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233> . Accessed on: 29 Nov 2024)

32. ROCHA, Maria Victória. Text and data mining in the directive on copyright and related rights in the digital single market. *RRDDIS–Digital, Intellectual & Society Law Network Journal*, Curitiba, v. 2, n. 4, p. 99-164, 2022, p. 103. Available at: <https://revista.ioda.org.br/index.php/rrddis/article/view/76/45> . Accessed on July 16, 2024

33. SOUZA, Allan Rocha de. SCHIRRU, Luca. Alvarenga. MIGUEL BARROS. Text and data mining in health research: reflections on copyright. *Public Health Notebooks 2024*. Available at: <https://cadernos.ensp.fiocruz.br/ojs/index.php/csp/article/view/8597/19335> . Accessed on: July 27, 2024.

– considering that there is access to the database (article 7, XII, XIII, §2º LDA) and to protected works, an express normative provision regarding the applicable limitation is important to guarantee legal certainty.

In this scenario, reflecting international legislative experiences, such as the reforms in copyright legislation carried out in Japan<sup>34</sup>, in Singapore<sup>35</sup> and in Israel<sup>36</sup>, in Brazil, Bill 2,338/23 recognizes the insufficiency of the limitations of article 46 of the LDA, since even with an extensive interpretation, these limitations refer only to the reproduction of works for specific purposes, without covering other forms of use necessary for TDM. The Bill then proposes a specific limitation for this activity, seeking to balance and make the exclusivity of the copyright system more flexible in favor of the public interest.

In order to comply with the obligations of Bill 2,338/23, it is important to understand who the subjects to whom the law applies are. According to article 4, VIII of the 4th amendment to Bill 2,338/23, artificial intelligence agents, which may be natural or legal persons, of a public or private nature, are the developers (art. 4, V).<sup>37</sup>, distributors (art. 4, VI)<sup>38</sup> and the applicators (art. 4, VII)<sup>39</sup> who work in the value chain and internal governance of artificial intelligence systems.

Despite the current legislation, the dynamism in the development of AI technologies exposes gaps that raise doubts about the application and sufficiency of existing mechanisms for copyright protection. Recognizing these gaps, Bill 2,338/23 and the proposed amendments seek to build regulations that consider the new reality and balance public and private interests. To verify the compatibility of regulatory suggestions to promote the protection of authors without hindering technological advances, the next chapter will analyze the proposed legislative update from the perspectives of holders' rights, limitations on copyright, remuneration regime, duty of transparency and regulatory sandbox, and personality rights and use of image.

34. In Japan, copyright law has been adjusted to allow data mining for research purposes, including for the development of AI, without the need to obtain prior consent from rights holders.

35. In Singapore, the Copyright Act 2021 includes an exception for data mining, which allows the use of protected works for computational analysis, including the development of AI, without the need for prior authorization from rights holders.

36. Israel allows the use of data for AI under conditions that ensure privacy and security, but does not impose severe restrictions on the use of protected data for AI training purposes.

37. Those responsible for the development of the artificial intelligence system (from creation, training, implementation and improvement), directly or by order, with a view to placing it on the market or applying it in a service provided by it, under its own name or brand, whether for a fee or free of charge.

38. Responsible for making the AI system available and distributing it so that third parties can operate it for a fee or free of charge.

39. Responsible for the use or utilization, on its behalf or for its benefit, of the artificial intelligence system, including for the purposes of configuration, maintenance or support with the provision of data for the operation and monitoring of the AI system.

## 2. Copyright and related rights in light of the 4th amendment of the PL 2.338/23 and proposed amendments

Although the guidelines for aligning copyright with access to data for machine training and the development of artificial intelligence systems have been a concern since the final report of the CJUSBIA, converted into the initial text in Bill No. 2,338/2023, after the analysis of numerous amendments proposed on the subject, some relevant advances have already been made, so that the main “points” of Bill 2,338/23 affecting copyright will be presented in this work based on the wording of the articles of the 4th substitute, of November 28, 2024, which even began to recognize the protection of copyright as one of the foundations of the law, alongside intellectual property and commercial and industrial secrets.

### 2.1 Rights of holders and limitations on rights authorial

Articles 63 and 64 of the 4th amendment to Bill 2,338/23 deal with the limitations and main rights of copyright and related rights holders, such as prohibiting the use of content owned by them in the development of AI systems.<sup>40</sup>

As seen, considering that articles 46 to 48 of the LDA, although they can be interpreted extensively, do not bring clear limitations to copyright in text and data mining processes for the development, training and use of AI systems, in line with international practices and responding to the contemporary needs of research and technological development, art. 63 of the 4th substitute of PL 2,338/23 innovates by providing exceptions to copyright in which the right to prohibit use provided for in art. 64 is mitigated.

The exception, however, in order to preserve the interests (mainly economic) of the authors, is limited to situations in which the public interest prevails, with use being permitted by educational, research, and journalism organizations and institutions, museums, archives, and libraries.<sup>41</sup> provided that access was lawful (item I), and the use is not for commercial purposes

40. Art. 64. The holder of copyright and related rights may prohibit the use of content owned by him/her in the development of AI systems in cases not covered by art. 61 of this Law, in accordance with the regulation. Sole paragraph. The prohibition of the use of works and content protected in the databases of an AI system after the training process does not exempt the AI agent from liability for moral and material losses and damages, under the terms of the applicable legislation.

41. Art. 63. The automated use of protected content in text and data mining processes for the purposes of research or development of AI systems by research, journalism, museum, archive, library and educational organizations and institutions does not constitute an offense to copyright and related rights, provided that the following conditions are met:

(item II), the activity does not aim at the reproduction, exhibition or dissemination of the original work (item III), and the use is made only to achieve its objective, without harming the economic interests of the holders or competing with the normal exploitation of the protected works and content (item IV).

Of these requirements, perhaps the one that generates the most questions is the prohibition of commercial purposes arising from mining. As discussed by Miguel Bastos Alvarenga<sup>42</sup>, it is important to remember that even research activity can culminate in publications being put up for sale, so that linking the exception to a strictly non-commercial purpose could impact the dissemination of scientific works and compromise various research activities.

At this point, it is understood that the prohibition of commercial purposes deserves greater maturity, based on the assessment of the sufficiency of the prohibition of interference in the normal exploitation of the work to the detriment of the economic interests of the owner, especially because art. 46 of the LDA itself allows exceptions for profit purposes.<sup>43</sup>

In addition to these points, the legal device also includes security duties and adequacy of the storage period for any copies of protected content for use in training AI systems (§1) and extended application for the use of mining processes in the context of artificial intelligence systems to combat civil and criminal offenses against copyright and related rights (§3).<sup>44</sup>

Although the provisions provide for the possibility of using works for mining purposes and use by artificial intelligence in certain contexts, it is important to highlight that the Bill does not authorize such use broadly, granting the holders the right to oppose the use, even when there is no actual harm to their economic interests. Such a prohibition, stricter than in other international legislation, may represent a barrier to investment and technological advancement in the country, with impacts on competitiveness. For this reason, it is also considered important to further mature discussions and evaluate, for example, mandatory compensation mechanisms – to protect the interests of the holders – without the possibility of prohibiting the use.

42. BROWN, Michael. *Data Mining, Big Data and Copyright in Brazil*. Thesis (Master's in Public Policy, Strategies and Development) - Institute of Economics, Federal University of Rio de Janeiro, Rio de Janeiro, 2019. p. 92. Available at: [https://onda.org.br/resources/2020\\_Miguel%20ALVARENGA\\_Mest.pdf](https://onda.org.br/resources/2020_Miguel%20ALVARENGA_Mest.pdf). Accessed on July 27, 2024.

43. "Art. 46. The following do not constitute an offense to copyright: I - reproduction: (...) The use of literary, artistic or scientific works, phonograms and radio and television broadcasts in commercial establishments, exclusively for demonstration to customers, provided that these establishments sell the supports or equipment that allow their use."

44. It is understood that the requirements of the paragraphs of art. 63 do not apply to use for this purpose.

in cases where there is no harm to the economic interests of the holders or competition with the normal exploitation of the protected works<sup>45</sup>.

## 2.2 Remuneration

One of the biggest concerns raised by AI tools involves guaranteeing remuneration to holders due to the appropriation of their productions for the development and training of AI models.

Until the 2nd substitute of PL 2,338/23, of June 18, 2024, the remuneration of holders for the use of protected content for training and development of artificial intelligence systems was subject to the creation of an experimental regulatory environment (sandbox) for discussion of remuneration models.

Only with the wording of the 3rd substitute was the duty of remuneration made positive, with art. 65 of the 4th substitute stating that “the AI agent that uses content protected by copyright and related rights in mining processes, training or development of AI systems must remunerate the respective owners of such content by virtue of such use.”

Regarding the right to remuneration, it is important to mention the rejection, on 07/04/2024, of amendments 56<sup>46</sup>, 61<sup>47</sup> and 72<sup>48</sup>, which sought respectively (i) the prevalence of a final fixed-price offer to be set by the Sector Authority or the Private Arbitration Chamber in the event of unfeasibility of negotiation between AI agents and the holder of copyright and related rights; (ii) the suppression of provisions related to copyright; and (iii) the removal of prior authorization for the development of AI systems with the eventual right to remuneration to the holders, on the grounds that guaranteeing rights to the creative industry is important to encourage responsible innovation and the protection of the fruits of the human spirit.

Although some<sup>49</sup> argue that remuneration for the economic exploitation of protected works is already supported by the Federal Constitution of 1988<sup>50</sup>, and by the LDA, being redundant to address the issue in the legislation on artificial intelligence, PL 2.338/23 recognizes that there are specificities in the context of AI that do not fit into the modalities of use provided for in the

45. Hypothesis with the highest probability of configuration in cases involving generative AI systems.

46. Authored by Senator Weverton, presented on 06/18/2024.

47. Authored by Astronaut Senator Marcos Pontes, presented on 06/18/2024.

48. Authored by Astronaut Senator Marcos Pontes, presented on 06/18/2024.

49. Amendments 61 and 72 seeking to suppress articles that affect copyright are examples of this.

50. Art. 5, XXVII, of the Federal Constitution.

LDA<sup>51</sup>. Therefore, the provision of remuneration in these situations is crucial to prevent abuses arising from ambiguities and obsolescence of current legislation, in addition to elucidating how this right will be exercised in the new technological context, which involves the use of large volumes of data.

On this subject, the paragraphs and subparagraphs of art. 65 of the 4th amendment to the Bill provide that remuneration will be due to holders domiciled in Brazil or in countries that ensure reciprocity in protection (subparagraph V, items a and b), only in the event of commercial availability of AI systems (subparagraph IV), and with the possibility of a deferred term for payment by startups and small businesses (subparagraph VI), ensuring: (i) the ability to negotiate directly or collectively, for a fee or free of charge (subparagraph I), in the first case regardless of regulation (§2); (ii) that the value considers the economic power of the AI agent, the degree of use of the content and the competitive effects in relation to the original content, the complexity of the AI system, the economic realization cycle and the relative value of the work over time (subparagraph II); (iv) free negotiation, with the promotion of an environment for research and experimentation, without restrictions on the freedom of agreement (subparagraph III).

That is, subject to the limitations introduced by art. 63, as long as prior use of content owned by the owner is authorized, the owner must be remunerated by the AI agent that uses his works.

Although the provision responds to the creative industry's wishes, it is understood that the current wording is insufficient to guarantee the desired legal certainty, in particular because: it makes generic reference to the duty of "artificial intelligence agents", and it is important to define to what extent and on which agent the duty to pay will fall in order to dispel doubts that may arise from the involvement of multiple agents in the life cycle of AI systems; the criteria for calculating the remuneration are subjective, making practical application difficult, and it is important to establish more objective criteria to measure "economic power", "degree of use", "competitive effects", "complexity of the AI system", "economic realization cycle" and "value of the work over time", in order to guide negotiations, without ignoring the freedom of agreement.

In addition to these points, although the importance of providing mechanisms to protect copyright and related rights holders cannot be ignored, especially from an economic perspective and in the context of the use of works by generative AI systems – with greater potential for impacts of a con-

51. So much so that it creates an exception for the use of works for mining, training and development of AI systems.

and harm to the author's interests – the technical difficulty in controlling and obtaining prior authorization for the use of data raises concerns, including in view of the importance of training models with Brazilian content (to reflect nuances and ensure appropriate application in the country). From this perspective, even to preserve Brazil's competitiveness and sovereignty in the global AI scenario, it becomes relevant to mature discussions and evaluate alternatives such as the creation of collective compensation funds, mandatory licensing with a standard fee, etc.

### 2.3 Transparency and Regulatory Sandbox

To allow control by the holders and guarantee the effectiveness of the exercise of the rights to prohibit and remunerate the use of works, transparency is a crucial element.

Although Digital Rights Management (DRM), blockchain, digital trademarks and watermarks technologies can be used to control and monitor access to and use of works, assigning the burden of control and monitoring to the rights holders could make the full exercise of rights unfeasible. In this sense, art. 62 of the 4th amendment of Bill 2,338/23 determines that the AI developer that uses content protected by copyright and related rights must make public which content was used in the training processes of the AI systems, by publishing a summary on an easily accessible website or as provided for in the regulation.

Limitation of liability to the AI developer, due to the acceptance of amendment 44<sup>52</sup>, represents a significant step forward. It not only clarifies who must comply with the legal obligation, but also justifies the fact that, as the “creator” of the system, the developer is in the best position to monitor and report the use of copyrighted and related content. By simplifying the chain of responsibility, the device also reduces the costs associated with compliance with legal obligations by other AI agents, encouraging competitiveness and innovation.

Although the assignment of responsibility is unequivocal, the way in which this obligation will be implemented still raises numerous questions, especially regarding the technical feasibility of listing all accessed content and obtaining prior authorization for use (when the exceptions in art. 63 do not apply).

52. Authored by Senator Chico Rodrigues, proposed on 06/17/2024.

Precisely for this reason, the effectiveness of the device is conditioned on the regulation of the topic, which may take advantage of the experiences gathered in an experimental regulatory environment (sandbox) established by the National System of Regulation and Governance of Artificial Intelligence (SIA) and by the competent sectoral body.<sup>53</sup>, under Chapter X, Section I of the 4th substitute.

This environment, initially specifically referenced in Section IV of the Bill, dedicated to copyright and related rights, was originally intended to address both transparency and remuneration (until the 2nd amendment). In the 3rd amendment, its scope was reduced to address only transparency and, finally, in the 4th amendment, it was completely removed from this section.

In this context, although the creation of a *sandbox* regulatory framework to experiment and adapt rules, aiming to guarantee transparency in the use of protected works, is aligned with international experiences, it is crucial to consider the risk of abuse and violation of rights in this more flexible environment, which may have justified its exclusion from Section IV.

Without prejudice, the difficulty in implementing transparency measures and the uncertainties arising from the lack of specific regulation deserve attention, and it is essential that any discussion of the duty of transparency within the scope of an experimental regulatory environment be preceded by the clear delimitation of the parameters and limits of the sandbox, together with the implementation of robust supervision mechanisms and the involvement of all interested parties, to ensure that regulatory flexibility does not compromise the protection of copyright.

## 2.4 Personality rights and use of image

Article 66 of the 4th substitute of PL 2,338/23 provides that the use of images, audio, voice or videos that portray or identify people must respect personality rights, in accordance with the Civil Code and relevant legislation.

As a way of combating misinformation caused, for example, by *deep fakes*, also worth highlighting is art. 19, which provides for the need to indicate synthetic content generated from AI systems, in order to allow verification of authenticity and characteristics of its origin, modifications and transmission. This provision is a reflection of the incorporation of the discipline of generative artificial intelligence contemplated in Bill No. 3,592, of 2023; in Bill No. 145,

53. Before the 3rd amendment, the exclusive responsibility of the sectoral authority was defended, after hearing the competent central body, and of the SIA. In this sense, amendment 45, authored by Senator Chico Rodrigues, partially accepted, defended that decision-making within the scope of the *sandbox* by the sectoral authority would have its integrity compromised, since the authority, being composed of federal departments and bodies of direct administration, could suffer political interference.

of 2024; and in Bill No. 146, of 2024 – added to the text of Bill 2,338/23 to harmonize the various initiatives on the subject – and acceptance of amendment No. 4<sup>54</sup>.

Regarding the provisions related to personality rights, the Bill has been criticized due to the apparent redundancy with provisions of the Civil Code, the LDA and the LGPD.

In this sense, as can be seen from the grounds of amendment suggestions no. 61, 72, 109 and 128, some provisions of the new regulation would, in fact, be a reaffirmation of what is already dealt with in the Civil Code, specifically in articles 11 and 20.<sup>55</sup>, which protect personality rights, ensuring that the use of the image, voice and other personal attributes may only occur with authorization or in specific situations, such as the maintenance of public order.

Likewise, Brazilian copyright legislation already has mechanisms to protect authors' rights in relation to the use of their works by AI systems.<sup>56</sup>, since articles 29 and 31 provide that any use, transformation or adaptation of a work protected by copyright – such as the creation of content derived from generative AI – depends on the express authorization of the owner. These provisions, therefore, would be sufficient to address most of the problems raised by the use of AI related to the modification or generation of content derived from the use of protected works, such as images, voices or texts (even if used only for training the systems).

Furthermore, as pointed out by ANPD<sup>57</sup>, there are intersections between the PL 2,338/23 and the LGPD regarding the collection, use of personal data and exercise of rights by data subjects<sup>58</sup>, so the creation of a new regulatory authority responsible for overseeing the use of AI systems could generate regulatory fragmentation.

54. Authored by Senator Vanderlan Cardoso, presented on 04/18/2024, proposing the inclusion of identifying marks in content generated or manipulated by artificial intelligence.

55. Art. 11. Except in cases provided for by law, personality rights are non-transferable and irrevocable, and their exercise cannot be subject to voluntary limitation.

Art. 20. Unless authorized, or if necessary for the administration of justice or the maintenance of public order, the disclosure of writings, the transmission of speech, or the publication, exhibition or use of a person's image may be prohibited, at their request and without prejudice to any compensation that may be due, if they affect their honor, good name or respectability, or if they are intended for commercial purposes. Sole paragraph. In the case of a deceased or absent person, the spouse, ascendants or descendants are legitimate parties to request this protection.

56. See Technical Note No. 2/2024 of the General Coordination of Copyright Regulation of the Ministry of Culture. Available at: [https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md\\_pesq\\_documento\\_consulta\\_externa.php?yPDszXhdoNcWQHJaQIHJmJIqCNXRK\\_Sh2SMdn1U-tzNsXmaDPqth6TWQbVeqDsJUpXKCGrIfpqgd2LPweVifrVUs865P0Y\\_aohlycyNue-1ge1wXB9NIS-a8VWrNBh-Xw](https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQIHJmJIqCNXRK_Sh2SMdn1U-tzNsXmaDPqth6TWQbVeqDsJUpXKCGrIfpqgd2LPweVifrVUs865P0Y_aohlycyNue-1ge1wXB9NIS-a8VWrNBh-Xw). Accessed on 10/13/24.

57. See Technical Note No. 16/2023/CGTP/ANPD: Suggestions for legislative impact on bills on the regulation of Artificial Intelligence in Brazil, focusing on Bill No. 2338/2023.

58. For example, the right to information, explanation and request for review could be subject to simultaneous regulation and supervision.

From this perspective, seeking greater harmonization with current legislation, in order to avoid overlap and/or inconsistent application of the new standard, the delimitation of scenarios and inclusion of guidelines that specifically address the use of AI<sup>59</sup> in the context of copyright and personality rights, such as the inclusion of clear mechanisms for authorization and compensation of authors in the case of use of works for training models, is recommended.

## Final considerations

This work initially addressed the definitions from the legislation applicable to copyright and, subsequently, mapped the related provisions in Bill 2,338/23 to regulate copyright and related rights within the scope of AI. Through the analysis of legislative definitions, specialized doctrine, the text of the 4th substitute of the Bill and the amendments presented, four main points that the new regulation addresses were identified, in addition to problems that require greater maturity and possible adjustments to the current wording.

In conclusion, it is concluded that although Bill No. 2338/2023 is an important milestone in balancing the protection of authors' rights with the promotion of technological innovation and the integration of artificial intelligence, there are still significant uncertainties regarding the application and effectiveness of the proposed measures. The complexity of establishing the protection of authors' rights without making mining activities and the use of protected content for system development and training unfeasible highlights the challenges faced. Issues such as fair remuneration, transparency in uses, and the implementation of licensing models also depend on more detailed provisions for effective practical application.

In order to ensure that legislation keeps pace with technological innovations, without becoming an obstacle to the country's development and competitiveness and, at the same time, promote a robust inspection system capable of guaranteeing respect for copyright and related rights,  
- it is essential that debates on the rights of holders, limitations on copyright, guarantees of transparency and remuneration continue to

59. Contrary to the delimitation of specific situations, it is worth mentioning the rejection, due to the limitation, in the PL, of the discipline of artificial intelligence in the aspect of Civil Law and with a general and principled nature, of amendments no. 20, 102, 103 and 112 which dealt, respectively, with the typification of *deep fakes* as a crime in the Penal Code, the indication of the use of AI in advertising pieces, rules for the use of the image and audio of the deceased person through AI for commercial purposes, the exclusion of indication of generation of synthetic content for artistic and literary works created for cultural purposes in a context in which there is editorial responsibility.

mature, with multisectoral and equitable participation of stakeholders and observance of international experiences. The topic, when brought to the debate, enriches the legislative process, allowing the collection of diverse points of view and the mapping of controversies.

Given that the PL is still under discussion, this work remains open for further development, making it possible, for example, to compare the final text of the approved regulation with the wording currently being analyzed.

## References

ABRAHAM, Eliane. *Copyright and related rights*. Sao Paulo: Ed. of Brazil, 2002.

BROWN, Michael. *Data Mining, Big Data and Copyright in Brazil*. Thesis (Master's in Public Policies, Strategies and Development) – Institute of Economics, Federal University of Rio de Janeiro, Rio de Janeiro, 2019. p. 92. Available at: [https://onda.org.br/resources/2020\\_Miguel%20ALVARENGA\\_Mest.pdf](https://onda.org.br/resources/2020_Miguel%20ALVARENGA_Mest.pdf). Accessed on July 27, 2024.

BITTAR, CA *Copyright*. 5th ed. rev. updated and expanded by Eduardo CB Bittar. Rio de Janeiro: Forense, 2013.

WHITE, Sergio. *Copyright on the Internet and the use of other people's works*. Rio de Janeiro: Lumen Juris, 2007. Available at: <https://repositorio.fgv.br/items/9d286b3c-c77e-46f2-ad95-1bc48debd48c> . Accessed on: July 13, 2024.

WHITE, Sergio. *Copyright*. 1st ed. Rio de Janeiro: Editora FGV. 2009. p. 50. Available at: <https://repositorio.fgv.br/server/api/core/bitstreams/3df3edc6-9a6f-486d-bff8-c1a717da24b4/content> . Accessed on: July 13, 2024.

BRAZIL. National Data Protection Authority. *Preliminary analysis of Bill No. 2338/2023, which provides for the use of Artificial Intelligence*. Brasilia, 2023. Available at: [https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338\\_2023-formatado-ascom.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf) . Accessed on: July 27, 2024.

BRAZIL. National Data Protection Authority. *Technical Note No. 16/2023/CGTP/ANPD: Suggestions for legislative impact on bills on the regulation of Artificial Intelligence in Brazil, focusing on Bill No. 2338/2023*. Brasilia, 2023. Available at: [https://www.gov.br/anpd/pt-br/issues/news/Technical\\_Note\\_16ANPDIA.pdf](https://www.gov.br/anpd/pt-br/issues/news/Technical_Note_16ANPDIA.pdf) . Accessed on: July 27, 2024.

BRAZIL. Chamber of Deputies. *Bill No. 21 of 2020*. Establishes principles, rights and duties for the use of artificial intelligence in Brazil, and contains other provisions. Brasília: Chamber of Deputies, 2020. Available at: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340&fichaAmigavel=nao> . Accessed on: July 20, 2024.

BRAZIL. Coordination of Special, Temporary and Parliamentary Commissions of Inquiry. *Final Report of the Commission of Jurists responsible for supporting the preparation of a substitute on artificial intelligence in Brazil*. Available at: <https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4> . Accessed on: July 20, 2024.

BRAZIL. Federal Senate. *Bill No. 5691, 2019*. Institutes the National Policy on Artificial Intelligence, with the objective of stimulating the creation of an environment favorable to the development of technologies in Artificial Intelligence. Brasília: Senado Federal, 2019. Available at: <https://www25.senado.leg.br/web/atividade/materias/-/materia/139586> . Accessed on: July 20, 2024.

BRAZIL. Federal Senate. *PBill No. 5051, of 2019*. Establishes the principles for the use of Artificial Intelligence in Brazil. Brasília: Senado Federal, 2019. Available at: <https://www25.senado.leg.br/web/atividade/materias/-/materia/138790> . Accessed on: July 20, 2024.

BRAZIL. Federal Senate. *Bill No. 872, 2021*. Provides for the use of Artificial Intelligence. Brasília: Federal Senate, 2019. Available at: <https://www25.senado.leg.br/web/atividade/materias/-/materia/147434> . Accessed on: July 20, 2024.

BRAZIL. Federal Senate. *Bill No. 2338, of 2023*. Provides for the use of Artificial Intelligence. Brasília: Federal Senate, 2023. <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233> . Accessed on: 29 Nov 2024.

CABRAL, Plinio. *A New Copyright Law*. 4th Edition. Harbra Publishing. 2003.

CANTALI, Fernanda Borghetti. Artificial intelligence and copyright: disruptive technology requiring reconfiguration of legal categories. *Journal of Law, Innovation, Intellectual Property and Competition*. Porto Alegre. v. 4. p. 1–21. Jul/Dec. 2018. Available at: <https://www.indexlaw.org/index.php/revistadipic/article/view/4667/pdf> . Accessed on: July 20, 2024.

CARBONI, William. *Copyright, Diversity of Cultural Expressions and Plurality of Authorship*. In: *Intellectual Property Law, Vol II: studies in honor of Father Jorge Hammes* (Org. by Luiz Gonzaga Silva Adolfo and Marcos Wachowicz). Curitiba: Juruá. 2014.

CERON, Rodrigo. *AI, machine learning and deep learning: What's the difference?* IBM, December 5, 2019. Available at: <https://www.ibm.com/blog/ai-machine-learning-and-deep-learning-whats-the-difference/> . Accessed on July 13, 2024.

EUROPEAN PARLIAMENT NEWS. *What is artificial intelligence and how is it used?* Sep 4, 2020. Available at: <https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used> . Accessed on July 13, 2024.

CONSUMER DEFENSE INSTITUTE (IDEC). *Idec's contribution to the CTIA Substitute for Bill 2,338/2023 (Artificial Intelligence)*. May, 2024. Available at: [https://idec.org.br/sites/default/files/2024\\_idec\\_-\\_analise\\_do\\_substituto\\_ao\\_pl\\_2338\\_23\\_-\\_inteligencia\\_artificial\\_08.05.2024\\_.docx.pdf](https://idec.org.br/sites/default/files/2024_idec_-_analise_do_substituto_ao_pl_2338_23_-_inteligencia_artificial_08.05.2024_.docx.pdf) . Accessed on: July 13, 2024.

PUBLIC POLICY AND INTERNET LABORATORY (LAPIN). *Bill No. 2338/2023 – Technical Note*. August, 2023. Available at: <https://direitosnarede.org.br/2023/08/23/coalizao-rights-on-the-network-releases-technical-note-on-pl-2338-2023-which-seeks-to-regulate-it/> . Accessed on: October 13, 2024.

MINISTRY OF CULTURE – GENERAL COORDINATION FOR COPYRIGHT REGULATION CGREG/DIREG/SDAI/GM/MinC. *Technical Note No. 2/2024*. Available at: [https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md\\_pesq\\_documento\\_consulta\\_externa.php?yPDSzXhdoNcWQHJa-QIHJmJIqCNXRK\\_Sh2SMdn1U-tzNsXmaDPqth6TWQbVeqDsJUpxKCGrIfpqqd2LPweVjfrVUs-865P0Y\\_aohlycNue1qe1wXB9NIS-a8VWrNBh-Xw](https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDSzXhdoNcWQHJa-QIHJmJIqCNXRK_Sh2SMdn1U-tzNsXmaDPqth6TWQbVeqDsJUpxKCGrIfpqqd2LPweVjfrVUs-865P0Y_aohlycNue1qe1wXB9NIS-a8VWrNBh-Xw) . Accessed on October 13, 2024.

ROCHA, Maria Victória. Text and data mining in the directive on copyright and related rights in the digital single market. *RRDDIS – Digital, Intellectual & Society Law Network Magazine*, Curitiba, v. 2, n. 4, p. 99-164, 2022, p. 103. Available at: <https://revista.ioda.org.br/index.php/rrddis/article/view/76/45> . Accessed on July 16, 2024.

SCHERER, Matthew U. Regulating Artificial Intelligence Systems: risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, vol, 29, nº 2, 2016, p. 354-400. Available at: <https://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf> . Accessed on July 13, 2024.

SCHIRRU, Luca. *Copyright and artificial intelligence: authorship and ownership in AI products*. Thesis (PhD in Public Policies, Strategies and Development) – Institute of Economics, Federal University of Rio de Janeiro, Rio de Janeiro, 2020. Available at: [https://www.ie.ufrj.br/images/IE/PPED/Teses/2020/Vers%C3%A3o%20final\\_Tese%20Luca\\_PDFA.pdf](https://www.ie.ufrj.br/images/IE/PPED/Teses/2020/Vers%C3%A3o%20final_Tese%20Luca_PDFA.pdf) . Accessed on: July 13, 2024.

SOUZA, Allan Rocha de. Author's moral rights. *Civilistica.com*. Rio de Janeiro, a. 2, n. 1, Jan.-Mar./2013. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/73/53> . Accessed on: July 27, 2024.

SOUZA, Allan Rocha de. SCHIRRU, Luca. Alvarenga. MIGUEL BARROS. Text and data mining in health research: reflections on copyright. *Public Health Notebooks 2024*. Available at: <https://cadernos.ensp.fiocruz.br/ojs/index.php/csp/article/view/8597/19335> . Accessed on: July 27, 2024.

STAUT JUNIOR, Sergio Said. *Copyright: between social relations and legal relations*. Mill of the Verb. Curitiba. 2006.

TURING, AM Computing Machinery and Intelligence. *Mind*, v. 59, n. 236, p. 433-460, Oct. 1950. Available at: <https://academic.oup.com/mind/article/LIX/236/433/986238> . Accessed on: July 13, 2024.

**Algorithmic Originality: there is  
originality in the outputs  
of artificial intelligence  
generative?**

Taís Bigarella Lemos

Summary: Introduction. 1. Concept of originality for copyright law. 2. But how does artificial intelligence work? 3. Metrics for evaluating the originality of *outputs* generated by artificial intelligence. Final considerations. References. Annex I.

## Introduction

The topic of artificial intelligence is increasingly in vogue, not only in academic and professional circles, but also in more informal settings, in people's daily lives. Therefore, there is sometimes an incorrect perception of what it means, including the idea that artificial intelligence would be linked to robots and futuristic items, such as flying cars. Artificial intelligence, however, is characterized by being a field of study known for the development and use of machines capable of performing tasks that would normally require human intelligence.<sup>2</sup>

The development of artificial intelligence involves "*machine learning*" and "*deep learning*". The "*machine learning*" is a branch of artificial intelligence and computer science that studies the use of data and algorithms to enable artificial intelligence to mimic the way humans learn, to improve its accuracy.<sup>3</sup> Now the "*deep learning*" is characterized by using multilayer neural networks to simulate the complex decision-making process of the human mind.<sup>4</sup>

Artificial intelligence thus consists of different models of "*machine learning*", what differentiates them is the way they use and understand data.<sup>5</sup> You *softwares* Artificial intelligence is becoming increasingly complex, producing work never before performed by computers.<sup>6</sup> For example, the latest generation of generative artificial intelligence, which

1. Master in Law from the Federal University of Rio Grande do Sul (2022). Bachelor in Legal and Social Sciences from the Federal University of Rio Grande do Sul (2018). Advisor to a Judge at the Court of Justice of Rio Grande do Sul. E-mail: taisbigarella@gmail.com .

2. FEINGOLD, S. What is artificial intelligence—and what is it not?. World Economic Forum, 2023. Available at:<https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning> . Accessed on: August 2, 2024.

3. IBM. What is machine learning?. IBM, 2024. Available at:<https://www.ibm.com/topics/machine-learning> . Accessed on: August 2, 2024.

4. HOLDSWORTH, J.; SCARPICCHIO, M. What is deep learning?. IBM, 2024. Available at:<https://www.ibm.com/topics/deep-learning> . Accessed on: August 2, 2024.

5. FEINGOLD, S. What is artificial intelligence – and what is it not?. World Economic Forum, 2023. Available at:<https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning> . Accessed on: August 2, 2024.

6. NAQVI, Zack. Artificial Intelligence, Copyright, and Copyright Infringement. *Marquette Intellectual Property Law Review*, vol. 24, no. 1, Winter 2020, p. 16. Accessed via HeinOnline.

has been surprising the population and raising new questions, especially with the launch of ChatGPT, which can learn and synthesize not only human language, but other data, such as images and videos.<sup>7</sup> These systems are a type of artificial intelligence model, called a large-scale language model, usually called by their English name "*Large Language Model*" or simply by the acronym "LLM", and are capable of performing various language understanding and text generation tasks at an unprecedented level.<sup>8</sup> To train these models to think and act, some strategies can be used, including document selection, linking to search engines and training question answering systems.<sup>9</sup> They are placed "*inputs*" in the system, which result in "*outputs*".

These new technologies challenge the legal system and, among these challenges, are those involving the protection of copyright, both of the documents used to train the system, and of those results obtained by the system, the "*outputs*". Regarding the data used for learning models, there has been much discussion about the possibility of using works protected by copyright, especially due to a well-known case in which The New York Times sued OpenAI and Microsoft due to the use of their articles for training artificial intelligence.<sup>10</sup>

Another topic in vogue is whether artificial intelligence could be the author of an intellectual work, considering the understanding that only natural persons would have such capacity, as they are the only ones capable of creating a work.<sup>11</sup> However, there is an essential aspect for a creation to be protected by copyright that seems to be little observed when analyzing artificial intelligence products, even though, without it, there is no copyright protection: originality.

7. IBM. What is artificial intelligence?. IBM, 2024. Available at:<https://www.ibm.com/topics/artificial-intelligence> . Accessed on: August 2, 2024.

8. MIALON, Grégoire; DESSI, Roberto; LOMELI, Maria; NALMPANTIA, Christoforos; PASUNURU, Ram; RAILEANU, Roberta; ROZIÈRE, Baptiste; SCHICK, Timo; DWIVEDI-YU, Jane; CELIKYILMAZ, Asli; GRAVE, Edouard; LECUN, Yann; and SCIALOM, Thomas. *Augmented Language Models: a Survey*. arXiv, 2023, <https://doi.org/10.48550/arXiv.2302.07842> 2302.07842. p. 2.

9. MIALON, Grégoire; DESSI, Roberto; LOMELI, Maria; NALMPANTIA, Christoforos; PASUNURU, Ram; RAILEANU, Roberta; ROZIÈRE, Baptiste; SCHICK, Timo; DWIVEDI-YU, Jane; CELIKYILMAZ, Asli; GRAVE, Edouard; LECUN, Yann; and SCIALOM, Thomas. *Augmented Language Models: a Survey*. arXiv, 2023, <https://doi.org/10.48550/arXiv.2302.07842> 2302.07842. p. 17.

10. POPE, A. NYT v. OpenAI: The Time's About-Face. Harvard Law Review, 2024. Available at:<https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/> . Accessed on: August 6, 2024.

11. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. *The Minimum Contribution in Intellectual Property: Inventive Activity, Originality, Distinguishability and Minimum Margin*. Rio de Janeiro: Lumen Juris, 2010. p. 434.

Only those creations that have *something more*, so that they can do justice to the quality of the work.<sup>12</sup> Whether it is called originality, creativity, individuality or minimum contribution, it is necessary that this something extra exists for there to be copyright protection. And, in this sense, before even thinking about the authorship of the *outputs* of artificial intelligence, it seems essential to analyze whether these results would have this *something more*, authorizing copyright protection. Now, if the “creation” is not considered a protected intellectual work, there is no reason to debate who would have the rights as its author, since it would not even be subject to protection.

Thus, the research problem of the present work is to analyze whether there is originality in the results/*outputs* obtained by users of generative artificial intelligence systems, considering the copyright doctrine.

To this end, the concept of originality for copyright law will be analyzed in the first chapter, followed by an examination in the second chapter of how artificial intelligence works, and the third and final chapter will conclude with metrics for assessing the originality of *outputs* and understandings of other legal systems on the subject.

## 1. Concept of originality for copyright law

Understanding the scope of copyright is complex, raising many questions in the analysis of specific cases. Unlike those rights protected by Industrial Property,<sup>13</sup> the Copyright Law, No. 9,610/98,<sup>14</sup> hereinafter referred to by its acronym, LDA, is broader in defining the object of its protection, requiring an analysis of each creation, in order to verify whether it meets the requirements for protection.

Starting with the legislative analysis, the *caput* Article 7 of the LDA defines protected intellectual works as “creations of the mind, expressed by any means or fixed in any tangible or intangible medium, known or that can be

12. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. *The Minimum Contribution in Intellectual Property: Inventive Activity, Originality, Distinguishability and Minimum Margin*. Rio de Janeiro: Lumen Juris, 2010. p. 307.

13. The Industrial Property Law (No. 9,279/96) protects intellectual property rights with less broad characteristics and more requirements, including the need for registration with the National Institute of Industrial Property (INPI), such as patents, industrial designs and trademarks. Therefore, it is very common to understand that, when a product/creation does not fit into any of these rights, there is an attempt to classify it as a creation protectable by copyright.

14. BRAZIL. *Law No. 9,610 of February 19, 1998*. Amends, updates and consolidates the legislation on copyright and contains other provisions. Available at: <[https://www.planalto.gov.br/ccivil\\_03/leis/l9610.htm](https://www.planalto.gov.br/ccivil_03/leis/l9610.htm)>.

invent in the future, such as” the examples given in its thirteen paragraphs.<sup>15</sup> Among them, we can highlight the texts of literary, artistic or scientific works, audiovisual works, musical compositions, illustrations and drawings.

The legal provision is, as can be seen from the content of the *caput* of the article, quite broad, the list of its paragraphs being merely illustrative,<sup>16</sup> so that other intellectual works, not listed, may be subject to protection, as long as they meet the other legal requirements. At this point, it is important to highlight that copyright arises from a protection policy, attempting to balance society's access to works and the incentive to the author,<sup>17</sup> through the granting of the monopoly right over the work.

Therefore, it is of utmost importance to first analyze whether the creation has the necessary attributes to be subject to copyright protection, under penalty of even influencing this balance between access to society and the monopoly granted to the author. And, in this sense, it is essential to examine whether there is originality in a creation so that it is entitled to protection. This is because originality, also referred to by the doctrine as “minimum contribution” or creativity, is the only filter existing in the Brazilian legal system and which serves as a stimulus for the author, the subject, to express his creative spirit, creating something different from what preceded it.<sup>18</sup>

There is, however, no unanimity on what characterizes originality. Traditionally, there is a distinction between the interpretation of the term in countries with a tradition of *common law*, which adopt the *copyright*,<sup>19</sup> as the Es-

15. Art. 7º Intellectual works protected are creations of the spirit, expressed by any means or fixed in any support, tangible or intangible, known or invented in the future, such as:

I - the texts of literary, artistic or scientific works;

II - conferences, speeches, sermons and other works of the same nature; III - dramatic and dramatic-musical works;

IV - choreographic and pantomimic works, the stage performance of which is recorded in writing or in any other form; V - musical compositions, whether or not they have lyrics;

VI - audiovisual works, with or without sound, including cinematographic works;

VII - photographic works and those produced by any process analogous to photography; VIII - works of drawing, painting, engraving, sculpture, lithography and kinetic art;

IX - illustrations, geographical maps and other works of the same nature;

X - projects, sketches and plastic works concerning geography, engineering, topography, architecture, landscaping, scenography and science;

XI - adaptations, translations and other transformations of original works, presented as new intellectual creations; XII - computer programs;

XIII - collections or compilations, anthologies, encyclopedias, dictionaries, databases and other works which, due to their selection, organization or arrangement of their content, constitute an intellectual creation.

16. ABRÃO, Eliane Yachouh. *Copyright and Related Rights*. 1st ed. New York: Routledge, 2002. p. 97.

17. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. *The Minimum Contribution in Intellectual Property: Inventive Activity, Originality, Distinguishability and Minimum Margin*. Rio de Janeiro: Lumen Juris, 2010. p. 309.

18. BARBOSA, Pedro Marcos Nunes. Originality in Crisis. *Brazilian Journal of Civil Law*, vol. 15, 2018, p. 38-39. Accessed via HeinOnline.

19. The origin of *copyright* took place in England, with the Statute of Queen Anne, later influencing the United States of America, with a perspective of being aimed at society, to promote the dissemination of works. For more information on the subject, see GINSBURG, Jane C. A Tale of Two Copyrights: Literary Property in Revolutionary France and America. *Tulane Law Review*, vol. 64, no. 5, May 1990. p. 991 -1031.

United States of America, which employed the “*sweat of the brow doctrine*”, and then move on to the theory of creativity *de minimis*, and those of Romano-Germanic tradition or of *civil law*, which use the idea of the doctrine of creativity.<sup>20</sup>

The “*sweat of the brow doctrine*”, translated as the sweat on the brow theory, is the one that understands that work and industry, even without any creativity, could be sufficient to meet the originality requirement for the *copyright*.<sup>21</sup> THE *copyright* arises from the idea of a certain materialization of copyright, since, as the name itself says, its objective was to protect the “copy right”, that is, the basis of the right was the copyable work. Thus, in this system, the original idea is that the economic utility of the copy would be more relevant than the creativity of the material,<sup>22</sup> so the theory of sweat on the forehead arises within this context, in which less importance was really given to the creativity involved in creation.

The doctrine of creativity, in turn, understands that a *quantum* minimum level of creativity for copyright protection to exist, even if it is modest, as well as requiring that the work is not a copy of another. In this reasoning, the mere compilation of information without a minimum level of creativity could not be subject to protection.<sup>23</sup>

In the United States of America, in 1991, with the trial of the Feist case<sup>24</sup>, the application of the theory was dismissed “*sweat of the brow*”, the understanding being established that, to meet the originality requirement, the work must demonstrate a minimum level of creativity.<sup>25</sup> In this case, it was a compilation and it was understood that the selection, coordination and organization of the compilation did not satisfy the constitutional minimum for protection by *copyright*, as they were common, only with the listing in alphabetical order. Thus, it is understood that the theory of creativity was applied *de minimis*.

Moving on to the Brazilian context, the LDA is not clear about which theory was adopted, however, Brazil being a country that is part of the tradition

20. BRIDGES, Leonardo Machado. *Copyright: the theory of the dichotomy between idea and expression*. Belo Horizonte: Arraes Publisher, 2012. p. 43.

21. BRIDGES, Leonardo Machado. *Copyright: the theory of the dichotomy between idea and expression*. Belo Horizonte: Arraes Publisher, 2012. p. 44.

22. ASCENSÃO, José de Oliveira. Copyright without author and without work. *Stvdia Ivridica*, Ad Honorem-3, Bulletin of the Faculty of Law, University of Coimbra, 1991. p. 88.

23. BRIDGES, Leonardo Machado. *Copyright: the theory of the dichotomy between idea and expression*. Belo Horizonte: Arraes Publisher, 2012. p. 45.

24. UNITED STATES OF AMERICA. US Supreme Court. Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc., 499, US 340. Appellant: Feist Pubs. Inc.. Respondent: Rural Tel. Svc. Co., Inc. Rapporteur: Justice Sandra Day O'Connor, March 27, 1991. Available at: <https://supreme.justia.com/cases/federal/us/499/340/>. Accessed on: July 27, 2024.

25. As part of the opinion in the Feist case, which states: “Originality requires only that the author make the selection or arrangement independently (*ie*, without copying that selection or arrangement from another work), and that it displays some minimal level of creativity”. Available at: <https://supreme.justia.com/cases/federal/us/499/340/>. Accessed on: July 27, 2024.

Roman-Germanic, there is a tendency towards the theory of creativity.<sup>26</sup> Furthermore, based on the provisions of the Berne Convention and TRIPs, Leonardo Pontes explains that, in Brazilian legislation:

the term “intellectual creation” will be more correctly interpreted in the sense of *creativity doctrine*, insofar as, through this doctrine, the law would not protect compilations of *productions*, since these *do not represent anything more than trivial or mechanical in nature*.<sup>27</sup>

Barbosa, Souto Maior and Tinoco explain that it seems to be part of the collective consciousness, both of Brazilian doctrine and jurisprudence, that the presence of “*something more*”, that is, a minimum contribution, so that a creation can be considered a work. The term used to identify this contribution may vary in the doctrine, with the use of different terms such as “creativity”, “originality”, “individuality” and similar terms.

José de Oliveira Ascensão, for example, when conceptualizing creativity, states that the work must have a minimum of creativity or originality, explaining that, when we move from creation to description, when it is the object that commands, instead of the predominant role being the author's vision, we are no longer within the scope of authorial guardianship.<sup>28</sup>

In this work, the expression “originality” is used in the sense of the doctrine of creativity, understanding the need for the work to present a minimum degree of creativity, a minimum contribution, for copyright protection. Furthermore, the choice of the term “originality” is due to it being the term considered most popular to designate this attribute of authorial creation, including because it is an expression commonly used in the English language.<sup>29</sup> and which is therefore more interesting for the case, which focuses on originality in artificial intelligence.

Having established the concept of originality for copyright law, we move on to the analysis of artificial intelligence and possible metrics for assessing the originality of *outputs*.

26. BRIDGES, Leonardo Machado. *Copyright: the theory of the dichotomy between idea and expression*. Belo Horizonte: Arraes Publisher, 2012. p. 49.

27. BRIDGES, Leonardo Machado. *Copyright: the theory of the dichotomy between idea and expression*. Belo Horizonte: Arraes Publisher, 2012. p. 51.

28. ASCENSION, José de Oliveira. *Copyright*. 2nd ed., ref. and ampl. Rio de Janeiro: Renovar, 1997. p. 57.

29. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. *The Minimum Contribution in Intellectual Property: Inventive Activity, Originality, Distinguishability and Minimum Margin*. Rio de Janeiro: Lumen Juris, 2010. p. 311.

## 2. But how does artificial intelligence work?

As already mentioned in the introduction, artificial intelligence is a group of techniques or instructions that aim to simulate biological cognition, human intelligence, using machines. Currently, most artificial intelligence uses the technique of "*machine learning*" which, as already mentioned, uses algorithms that can "learn" or improve performance for specific tasks, based on programmed instructions. However, it can be understood that artificial intelligence would be a "black box", since the programmer only sees what he puts to "feed" the system, the "*input*", and the result, the "*output*", without being able to specifically observe the machine learning process.<sup>30</sup>

In this work, the focus of the analysis is on generative artificial intelligences, which generate in their *output*, or result, creations that could be considered subject to copyright protection. As mentioned in the chapter above, article 7 of the LDA lists some hypotheses of creations that could be protected and, among the hypotheses brought by its clauses,<sup>31</sup> stand out-

- if, for the purposes of this analysis, the texts of literary works and illustrations.

This is because, currently, there are artificial intelligences capable, apparently, of generating these types of creations. The most famous of the tools is ChatGPT, a *chatbot* able to create coherent paragraphs by predicting what the most likely next word in a sentence would be.<sup>32</sup> This tool is capable of creating complete texts, which could, at first glance, be considered literary works. ChatGPT is a large-scale language model, commonly referred to in English as a "*Large Language Model*" or LLM, built based on training with a massive amount of documents/texts. The models incorporate the information obtained from the dataset and thus learn word patterns for a given context, a process that allows the user to obtain the most likely combination of words as a result, generating a more natural language.<sup>33</sup>

In Annex I of this work, a response given by the tool is demonstrated, when asked to "Write a literary work of romance, of

30. NAQVI, Zack. Artificial Intelligence, Copyright, and Copyright Infringement. *Marquette Intellectual Property Law Review*, vol. 24, no. 1, Winter 2020, p. 19. Accessed via HeinOnline.

31. See footnote 14.

32. FEINGOLD, S. What is artificial intelligence—and what is it not?. World Economic Forum, 2023. Available at: <https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning> . Accessed on: August 2, 2024.

33. POPE, A. NYT v. OpenAI: The Time's About-Face. *Harvard Law Review*, 2024. Available at: <https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-times-about-face/> . Accessed on: August 6, 2024.

four paragraphs, portraying a love story with a happy ending”. From the result, it is confirmed that, from a first analysis, it would even be intuitive for the reader to understand that this text is a literary work, even more so without knowing its origin, that is, that it is the result of artificial intelligence.

Another very interesting tool, also using generative artificial intelligence, is DALL-E, from the same developer as ChatGPT, the company OpenAI. This tool does not generate texts, but, as explained in its *website*, is a system capable of creating realistic images or art based on the description given by the user.<sup>34</sup>In the same way as mentioned for ChatGPT, its result, at first glance, can also be understood as subject to copyright protection, for creating illustrations and visual works.

Both of these systems are protected by the Brazilian legal system through the Law of *Software* (Law No. 9,609/98), which protects the computer program, as “an expression of an organized set of instructions in natural or coded language, contained in a physical medium of any nature, for use in automatic information processing machines, devices, instruments or peripheral equipment, based on digital or analogous techniques, to make them function in a specific way and for specific purposes”<sup>35</sup>. However, as the legislator rightly states, this protection is for the expression of the organized set of instructions, that is, for the model itself used, and not necessarily for the products obtained from it. The protection of the *software* in itself, of the codes used by artificial intelligence, which seems peaceful to be covered by the Law of *Software*, and of your *outputs*, which is debated as to whether they could be subject to copyright protection.

It is therefore essential to analyze what is provided for in the Terms of Use of the aforementioned platforms, ChatGPT and DALL-E, regarding the ownership and protection of the results obtained by them. The Terms of Use of both are the same, as they are services offered by the same company, OpenAI.<sup>36</sup>The first clarification given is that the Terms of Use constitute an agreement between the user and OpenAI, including important provisions for the resolution of disputes and that, by using the services, the user is agreeing to these Terms. Also, the existence of other Terms of Use for residents of the Union is reserved.

34. According to information in: OpenAI. DALL-E 2. OpenAI, 2024. Available at:<https://openai.com/index/dall-e-2/>. Accessed on: August 3, 2024.

35. According to art. 1 of Law nº 9.609/98. BRAZIL. *Law No. 9,609 of February 19, 1998*. Provides for the protection of intellectual property of computer programs, their commercialization in the country, and other provisions. Available at:[https://www.planalto.gov.br/ccivil\\_03/leis/l9609.htm](https://www.planalto.gov.br/ccivil_03/leis/l9609.htm).

36. Terms of use are available at: OpenAI. Terms of use. OpenAI, 2024. Available at:<https://openai.com/policies/terms-of-use/>. Accessed on: August 4, 2024.

European, Swiss and United Kingdom, which will not be analyzed in this work, as the focus is on Brazilian regulation.

That said, as it specifically relates to *outputs*, the Terms of Use state that the *inputs and outputs*, together, are referred to as “content”. Ownership of the content, in turn, is provided in the sense that, to the extent permitted by applicable law, the user holds ownership rights over the *input* placed and, still, is the owner of the *output*. This is what the item provides:

**Content ownership.** As between you and OpenAI, to the extent permitted by applicable law, you (a) retain your ownership rights in the *input* and (b) is the owner of the *output*. We hereby assign to you all of our rights, titles and interests, if any, in and to the *output*.<sup>37</sup>

Specifically regarding the existence of copyright over these results, there is no mention in the Terms of Use, which only contains a part referring to the possibility of the user sending a notification, if he/she understands that his/her right to *copyright* is being infringed by the platform. It is interesting, however, to point out that there is a section in the Terms that lists the activities that cannot be carried out by the user (“*What you cannot do*”) and, among them, is to present the *outputs* as human-generated, when it was not.<sup>38</sup>

It can be seen that there is, therefore, at least in the Terms of Use, no express intention by the company to understand that the results obtained would be protected by copyright and, even if they were, the rights over these works are attributed to the users, with the caveat, however, that these results cannot be presented as generated by human beings, as they were not.

It seems to make sense that the Terms of Use do not presume the existence of copyright protection over these results. This is because, as already mentioned, for a creation to be protected by copyright, it must meet different requirements, among which is originality, the subject of this work, which is why we move on to the analysis of metrics for assessing the originality of these results. *outputs*.

37. Free translation by the author of: “**Ownership of content.** As between you and OpenAI, and to the extent permitted by applicable law, you (a) retain your ownership rights in Input and (b) own the Output. We hereby assign to you all our right, title, and interest, if any, in and to Output.” Available at: OpenAI. Terms of use. OpenAI, 2024. Available at: <https://openai.com/policies/terms-of-use/> . Accessed on: August 4, 2024.

38. In the original, the item is written as follows: “Represent that Output was human-generated when it was not”. OpenAI. Terms of use. OpenAI, 2024. Available at: <https://openai.com/policies/terms-of-use/> . Accessed on: August 4, 2024.

### 3. Metrics for assessing the originality of outputs generated by Artificial Intelligence

To assess whether there is a *quantum* minimum level of originality or creativity to justify copyright protection, also known by the doctrine as minimum contribution, it is first essential to think about the definition of a work, since it is not possible to say that a creation is a work if there is not a minimum level of creativity present in its realization.<sup>39</sup> To identify a creation as a work, the doctrine understands that one must, first, look at its creator, and it can only be a work if its intellectual creator is a human person who has an impact on its final result. After that, it is still necessary to identify whether the creation was externalized, is not among the legal prohibitions and, finally, presents a minimum contribution.<sup>40</sup>

The minimum contribution, in turn, is characterized by the minimum creativity necessary for the existence of a work and, in fact, helps to separate the works, so that, if the minimum contribution exists, there is no plagiarism.<sup>41</sup> At this point, it is important to understand that if there is a minimum contribution to differentiate one work from another, even if the first was based on the second, it is understood that there is a work; however, these works are called derivative works. Derivative works are works such as translation and adaptation and, therefore, require authorization from the owner of the original work, but they are attributed original ownership, as they are an intellectual creation, with sufficient creativity, independent of the rights of the authors of the pre-existing works, which remain intact.<sup>42</sup>

Now for the measurement of the *quantum* of creativity or originality necessary for the protection of the work as copyright, Leonardo Machado Pontes suggests the use of three criteria: (i) the person responsible for the composition of the work and its right to development must be the author, as opposed to the person who simply follows orders to execute the work; (ii) the greater the mechanical participation in the process of the work, the more the author must demonstrate that he deserves protection; and (iii) authorship is equivalent to originality and creativity.<sup>43</sup>

39. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. *The Minimum Contribution in Intellectual Property: Inventive Activity, Originality, Distinguishability and Minimum Margin*. Rio de Janeiro: Lumen Juris, 2010. p. 446.

40. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. *The Minimum Contribution in Intellectual Property: Inventive Activity, Originality, Distinguishability and Minimum Margin*. Rio de Janeiro: Lumen Juris, 2010. p. 449.

41. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. *The Minimum Contribution in Intellectual Property: Inventive Activity, Originality, Distinguishability and Minimum Margin*. Rio de Janeiro: Lumen Juris, 2010. p. 470.

42. COSTA NETTO, José Carlos. *Copyright in Brazil*. Coordination Hélio Bicudo. São Paulo: FTD, 1998. p. 63.

43. BRIDGES, Leonardo Machado. *Copyright: the theory of the dichotomy between idea and expression*. Belo Horizonte: Arraes Publisher, 2012. p. 88-94.

As for the first criterion, it lies in the differentiation between the author of the work and the one *mere executor*, which merely complies with third party orders, without any improvement. The second criterion deals with the need, even when the work is created with the help of machines, to follow *a standard*, even if low, in order to demonstrate the expression of creativity, even if minimal. Protection would only exist when it is identified that the work is not *automatic production of a machine*, but there is an expression from an author.<sup>44</sup> Finally, the third and final criterion refers to the finding that, in the end, for copyright protection to exist, originality and creativity only mean that the creation needs to come from the author's work, not being *copy of another work*.<sup>45</sup>

Thus, to assess whether there is originality or creativity, even in *quantum* minimum, in the *output* of generative artificial intelligence, it is necessary to analyze whether they meet these three criteria. Based on the premises established in the previous topics, it is known that the artificial intelligences currently being studied work in such a way that, when a request is made by the user (*input*), obtained a result or *output* which may, superficially, appear to be a copyrighted work.

However, analyzing the criteria necessary to recognize the originality of the work, to authorize its protection, it seems that none of them would be present in the creations carried out by these artificial intelligences.

Starting with the first requirement, it seems difficult to interpret that artificial intelligence is not a mere executor of orders, since it only predicts what would be the most coherent response based on the learning it has obtained and the request made by the user.<sup>46</sup> Thus, the result obtained by the system seems more like the automatic production of a machine, which also violates the second criterion mentioned, since the machine is taught to reason, to make inferences based on the training it received. In this sense, the more interactivity there is between the machine and the user, the greater the chance of obtaining a better result, or *output*.<sup>47</sup>

44. BRIDGES, Leonardo Machado. *Copyright: the theory of the dichotomy between idea and expression*. Belo Horizonte: Arraes Editora, 2012. pp. 88-89 and 91.

45. BRIDGES, Leonardo Machado. *Copyright: the theory of the dichotomy between idea and expression*. Belo Horizonte: Arraes Publisher, 2012. p. 93.

46. According to FEINGOLD, S. What is artificial intelligence—and what is it not? World Economic Forum, 2023. Available at: <https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning>. Accessed on: August 2, 2024. Explains that ChatGPT is a *chatbot* that is able to predict the most likely next word in a sentence, based on numerous and relatively accurate predictions.

47. MIALON, Grégoire; DESSI, Roberto; LOMELI, Maria; NALMPANTIA, Christoforos; PASUNURU, Ram; RAILEANU, Roberta; ROZIÈRE, Baptiste; SCHICK, Timo; DWIVEDI-YU, Jane; CELIKYILMAZ, Asli; GRAVE, Edouard; LECUN, Yann; and SCIALOM, Thomas. *Augmented Language Models: a Survey*. arXiv, 2023, <https://doi.org/10.48550/arXiv.2302.07842>. p. 9.

Furthermore, with regard to the third and final criterion, it is interesting to reflect on whether, considering that the results obtained in these systems are based on the data entered into them, responsible for their learning and which teach them to reason, this would not be, in a certain way, a form of plagiarism.

As already mentioned, for there to be a separation between the works and for them to be understood as distinct and, therefore, not be a case of plagiarism, there must be a minimum contribution from the author. In the case of generative artificial intelligence, the use of images and articles to teach the system, in order to obtain the most accurate result possible, leads to the conclusion that the result obtained when, for example, Chat-GPT is asked to write a text, is, in the end, a result of the combination of these different data that were input to “teach” the model. Even if it is not, therefore, a direct copy of those documents that feed the system, the *outputs* are only possible and present the desired precision also because of them.

At this point, it is interesting to highlight the lawsuit filed by The New York Times against OpenAI and Microsoft, for the alleged unauthorized use of Times articles to train the large-scale language model of ChatGPT and BingChat (or Copilot). The Times argues that the problem of unauthorized use of articles would be aggravated by two reasons: the large-scale language model memorizes part of the works and can, therefore, eventually generate results that are reproductions of the works; and, further, it produces “synthetic” search results and may end up allowing readers to read Times articles that would not be available without paying for the newspaper’s subscription, harming its business model.<sup>48</sup>

These arguments are interesting for the analysis carried out now because they reflect on the originality of the *output* of these artificial intelligence models, which may even incur evident plagiarism, when reproducing articles used to train the language model.

In this sense, it is important to reflect that when creating, human beings invariably have other works as a basis and inspiration, however, they are capable of reasoning, thinking, making connections and using this information in different ways. Differently, artificial intelligence systems do not have “intelligence” per se, but they make predictions, given the improvement in the machines’ ability, with increasing precision and achieving the desired result. However, it is not comparable to human intelligence, which can obtain the

48. POPE, A. NYT v. OpenAI: The Time’s About-Face. Harvard Law Review, 2024. Available at: <https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/>. Accessed on: August 6, 2024.

information from a source and use it in multiple ways, being transferable, unlike the “intelligence” of machines.<sup>49</sup> Furthermore, to avoid committing plagiarism, the human author also needs to indicate his/her sources, a characteristic that is not observed in the results obtained from artificial intelligence.

In the same sense, the tendency of legal systems seems to be to recognize the lack of sufficient creativity in the results of artificial intelligence to obtain copyright protection. This is because machines have no internal awareness and sensitivity of what they are doing, they are not inspired at a subconscious level,<sup>50</sup> requirements normally required to characterize a protected work, as can be seen from the decision in the Feist case, already mentioned, in which the Supreme Court of the United States of America indicated the need for the author to prove the “existence of these facts of originality, intellectual production, thought and conception”.<sup>51</sup>

It is also possible to identify this same interpretation in other legal systems, such as Japan's 2016 Strategic Plan for Intellectual Property, which indicates that products created automatically by artificial intelligence are not eligible for copyright protection under the current legal system, and it is also possible to deduce from French decisions that, although it is possible to protect results produced by humans with the help of machines, it denies that machines can replace humans and perform the work independently.<sup>52</sup>

However, China's understanding has been the opposite. Since 2019, Chinese courts have been stating that products generated by artificial intelligence constitute works protected by copyright.<sup>53</sup> Chinese law does not specifically address the issue, but the courts' understanding affirms the possibility of protection, due to four factors: (i) adoption of a broader interpretation of human participation, considering that the

49. FEINGOLD, S. What is artificial intelligence—and what is it not? World Economic Forum, 2023. Available at: <https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning>. Accessed on: August 2, 2024.

50. ZURTH, Patrick. Artificial Creativity? A Case against Copyright Protection for AI-Generated Works. *UCLA Journal of Law and Technology*, vol. 25, no. 2, Spring 2021, p. 11. Accessed via HeinOnline.

51. As per UNITED STATES OF AMERICA. US Supreme Court. Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc., 499, US 340. Appellant: Feist Pubs. Inc. Respondent: Rural Tel. Svc. Co., Inc. Rapporteur: Justice Sandra Day O'Connor, March 27, 1991. Available at: <https://supreme.justia.com/cases/federal/us/499/340/>. Accessed on: 27 July. 2024. Free translation by the author of: “the importance of requiring an author who accuses another of infringement to prove “the existence of those facts of originality, of intellectual production, of thought, and conception.”.

52. DAI, Zhe; and JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. *Legal Tribune*, vol. 13, no. 2, June 2023, p. 243-244. Accessed via HeinOnline.

53. DAI, Zhe; and JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. *Legal Tribune*, vol. 13, no. 2, June 2023, p. 245. Accessed via HeinOnline.

requirement that human participation be only at the preparation stage, prior to the operations of artificial intelligence; (ii) lack of distinction between machine assistance and the results generated by artificial intelligence; (iii) adoption of a *standard objective* for the concept of originality, which can be fulfilled even if there is no human participation, since it is understood that the content generated by artificial intelligence reflects selection, judgment and analysis of relevant data, which would be sufficient to satisfy the requirement of originality; and, finally, what can be understood as the main reason for the difference between the Chinese understanding and that of other countries, (iv) the strong utilitarian principles of its copyright law. The value of human participation is less relevant in Chinese legislation, with the issue of protection being less focused on the creator and more on the analysis of whether protection is in the social interest.<sup>54</sup>

Although the analysis of the Chinese understanding is interesting, it seems that its adoption by other countries is unlikely considering their current copyright laws, especially those of the Romano-Germanic family, which adopt the theory of creativity, as they place more emphasis on human characteristics and the connection between the author and his work, on what only humans could do. In any case, the debate is inevitable, as generative artificial intelligence models have been gaining more and more space and prominence, even economically, showing that it is essential to understand how to regulate them and what protection they will receive, including with regard to their *outputs*, to the results produced by them.

## Final considerations

Artificial intelligence, although no longer a novelty, has become increasingly present and a protagonist in people's daily lives. Among the various challenges that this technology imposes on the legal system are those related to the copyright protection of its *outputs*, of their results, while they may appear, at first glance, to be works protected by copyright, such as literary texts and illustrations.

However, for a creation to be eligible for copyright protection, it must be original and present a *quantum* minimum level of creativity that differentiates it from those creations already carried out by third parties and justifies the author's monopoly, that only he has rights over that

54. DAI, Zhe; and JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. *Legal Tribune*, vol. 13, no. 2, June 2023, p. 249-254. Accessed via HeinOnline.

work. It does not seem, however, that the *outputs* of artificial intelligence have this characteristic, since these models appear to be mere executors of orders and, in turn, their result would constitute an automatic production of the machine, which would not give it the characteristic of being original.

Furthermore, the fact that the results obtained by these models are based on the data inputted into them, which are sometimes texts and images protected by copyright, leads to the conclusion that they do not have sufficient originality to be understood as autonomous works that deserve copyright protection, but, on the contrary, could even incur plagiarism, by merely reproducing protected works that they use for their learning.

Thus, it is concluded that the *outputs* of artificial intelligence systems do not, as a rule, present sufficient originality to be subject to copyright protection.

## References

ABRAM, Eliane Yachouh. *Copyright and Related Rights*. 1st ed. New York: Routledge, 2002.

ASCENSION, Jose de Oliveira. *Copyright*. 2nd ed., ref. and ampl. Rio de Janeiro: Renovar, 1997.

ASCENSÃO, José de Oliveira. Copyright without author and without work. *Stvdia Ivridica*, Ad Honorem – 3, Bulletin of the Faculty of Law, University of Coimbra, 1991.

BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. *The Minimum Contribution in Intellectual Property: Inventive Activity, Originality, Distinguishability and minimum margin*. Rio de Janeiro: Lumen Juris, 2010.

BARBOSA, Pedro Marcos Nunes. Originality in Crisis. *Brazilian Journal of Civil Law*, vol. 15, 2018, p. 33-48. Accessed via HeinOnline.

BRAZIL. *Law No. 9,609 of February 19, 1998*. Provides for the protection of intellectual property of computer programs, their commercialization in the country, and other provisions. Available at: <[https://www.planalto.gov.br/ccivil\\_03/leis/l9609.htm](https://www.planalto.gov.br/ccivil_03/leis/l9609.htm)>.

BRAZIL. *Law No. 9,610 of February 19, 1998*. Amends, updates and consolidates the legislation on copyright and contains other provisions. Available at: <[https://www.planalto.gov.br/ccivil\\_03/leis/l9610.htm](https://www.planalto.gov.br/ccivil_03/leis/l9610.htm)>.

COSTA NETTO, Jose Carlos. *Copyright in Brazil*. Coordination Hélio Bicudo. São Paulo: FTD, 1998.

DAI, Zhe; and JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. *Legal Tribune*, vol. 13, no. 2, June 2023, pp. 241-260. Accessed via HeinOnline.

UNITED STATES OF AMERICA. US Supreme Court. *Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc.*, 499, US 340. Appellant: Feist Pubs. Inc. Respondent: Rural Tel. Svc. Co., Inc. Rapporteur: Justice Sandra Day O'Connor, March 27, 1991. Available at:<https://supreme.justia.com/cases/federal/us/499/340/> . Accessed on: July 27, 2024.

FEINGOLD, S. What is artificial intelligence—and what is it not? World Economic Forum, 2023. Available at:<https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning> . Accessed on: August 2, 2024.

HOLDSWORTH, J.; SCARPICCHIO, M. What is deep learning? IBM, 2024. Available at:<https://www.ibm.com/topics/deep-learning> . Accessed on: August 2, 2024.

IBM. What is artificial intelligence? IBM, 2024. Available at:<https://www.ibm.com/topics/artificial-intelligence> . Accessed on: August 2, 2024.

IBM. What is machine learning? IBM, 2024. Available at:<https://www.ibm.com/topics/machine-learning> . Accessed on: August 2, 2024.

OpenAI. DALL-E 2. OpenAI, 2024. Available at:<https://openai.com/index/dall-e-2/> . Accessed on: August 3, 2024.

OpenAI. Terms of use. OpenAI, 2024. Available at:<https://openai.com/policies/terms-of-use/> . Accessed on: August 4, 2024.

BRIDGES, Leonardo Machado. *Copyright: the theory of the dichotomy between idea and expression*. Belo Horizonte: Arraes Publishing, 2012.

POPE, A. NYT v. OpenAI: The Time's About-Face. Harvard Law Review, 2024. Available at:<https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/> . Accessed on: August 6, 2024.

MIALON, Grégoire; DESSI, Roberto; LOMELI, Maria; NALMPANTIA, Christoforos; PASUNURU, Ram; RAILEANU, Roberta; ROZIÈRE, Baptiste; SCHICK, Timo; DWIVEDI-YU, Jane; CELIKYILMAZ, Asli; GRAVE, Edouard; LECUN, Yann; and SCIALOM, Thomas. *Augmented Language Models: a Survey*. arXiv, 2023, <https://doi.org/10.48550/arXiv.2302.07842> 2302.07842.

NAQVI, Zack. Artificial Intelligence, Copyright, and Copyright Infringement. *Marquette Intellectual Property Law Review*, vol. 24, no. 1, Winter 2020, pp. 15-52. Accessed via HeinOnline.

ZURTH, Patrick. Artificial Creativity? A Case against Copyright Protection for AI-Generated Works. *UCLA Journal of Law and Technology*, vol. 25, no. 2, Spring 2021, pp. i-18. Access via HeinOnline.

# Annex I – ChatGPT Response



The screenshot shows a ChatGPT interface with a dark theme. At the top left, it says "ChatGPT 4o mini" with a dropdown arrow. At the top right, there are buttons for "Entrar" and "Cadastrar". The main content area contains a prompt in a rounded rectangle: "Escrever uma obra literária de romance, de quatro parágrafos, retratando uma história de amor com final feliz." Below the prompt, the AI response is displayed in four paragraphs, each preceded by a small circular icon. The response describes a romance in a coastal town between Ana and Lucas. At the bottom, there is a text box with a copy icon, a download icon, and a warning message: "Não compartilhe informações confidenciais. Os chats podem ser revisados e usados para treinar nossos modelos. Saiba mais". Below the text box is a "Mensagem ChatGPT" input field with an upward arrow icon. At the very bottom, a small disclaimer reads: "ChatGPT pode cometer erros. Considere verificar informações importantes." and a question mark icon.

ChatGPT 4o mini Entrar Cadastrar

Escrever uma obra literária de romance, de quatro parágrafos, retratando uma história de amor com final feliz.

Em uma pequena cidade costeira, onde o mar e o céu se fundem em um azul profundo, vivia Ana, uma jovem que passava seus dias na livraria do avô. Era um local encantador, repleto de histórias e segredos, e Ana se perdia entre as páginas de romances antigos, sonhando com um amor que parecia tão distante quanto as estrelas. Um dia, enquanto rearrumava as prateleiras, ela encontrou um livro antigo, empoeirado e com uma capa desgastada, que chamou sua atenção de uma maneira inexplicável.

No mesmo dia, Lucas, um artista que havia se mudado recentemente para a cidade em busca de inspiração, entrou na livraria. Seus olhos brilhavam com uma curiosidade genuína e, ao esbarrar na prateleira, fez com que o livro caísse diretamente em suas mãos. Ana, curiosa, se aproximou e uma conversa fluida e encantadora começou entre os dois. Descobriram que, apesar de suas vidas serem diferentes, compartilhavam uma paixão por histórias e uma sede por aventuras.

Com o tempo, Ana e Lucas se encontraram frequentemente, explorando os cantos pitorescos da cidade e criando memórias em cada encontro. Entre passeios pela praia e tardes na livraria, eles começaram a se apaixonar, descobrindo uma conexão profunda que transcendia as palavras e as páginas dos livros. O amor deles era uma mistura perfeita de amizade e romance, um conto que parecia ter sido escrito pelos próprios deuses do destino.

Finalmente, em uma tarde dourada de verão, Lucas preparou uma surpresa para Ana. Ele a levou a uma pequena galeria onde exibiu suas pinturas inspiradas na beleza da cidade e na magia dos momentos que passaram juntos. Em meio às obras, uma pintura especial retratava o exato instante em que se conheceram na livraria. Com um sorriso no rosto e lágrimas de felicidade nos olhos, Lucas pediu a Ana que passasse o resto de sua vida ao seu lado. Ela aceitou com um beijo suave e um abraço apertado, e assim, com o final feliz que ambos haviam sonhado, eles começaram a escrever seu próprio capítulo eterno.

📄 ↓

Não compartilhe informações confidenciais. Os chats podem ser revisados e usados para treinar nossos modelos. [Saiba mais](#)

Mensagem ChatGPT ↑

ChatGPT pode cometer erros. Considere verificar informações importantes. ?

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

8

**The challenges involved in use  
and regulation  
of artificial intelligence in the  
face of discrimination  
algorithmic**

Maria Fernanda Longato Maturana

Summary: Introduction. 1. The ways in which artificial intelligence learns and the core of the problem surrounding algorithmic discrimination. 2. The challenges involved in regulating artificial intelligence to ensure the promotion of equality and avoid discrimination. 3. New horizons in internet networks in light of bill no. 2,338/2023. Final considerations. References.

## Introduction

In view of the constant evolution of the modern world, artificial intelligence has established itself as one of the most transformative technologies with the greatest projection of use in the modern era, enabling innovative, fast and relevant transformations and solutions in various areas, from health to the vastest areas of agribusiness.

The purpose of using artificial intelligence technology is to “humanize” this machine, so that its responses can be relevant to society, given that the machine becomes a reflection of it. This thinking has enabled several technological advances, but at the same time, the use of artificial intelligence algorithms brings to light complex and worrying issues for society, especially with regard to algorithmic discrimination, given that artificial intelligence aims to reflect the thinking of a society, which also includes its imperfections.

Algorithmic discrimination occurs when artificial intelligence systems reproduce or even amplify discriminatory stereotypes combined with existing prejudices within a society, resulting in biased decisions and creations that negatively affect certain groups of people who are already subject to structural discrimination.

The problem of algorithmic discrimination arises in many ways and from many sources, including training data biased by discriminatory stereotypes, poor design choices, and even a lack of diversity among AI developers. These challenges not only compromise fairness and justice in automated decision-making, but also reveal structural problems present in society. It is therefore crucial to understand and address these challenges to ensure that

1. Postgraduate student in Digital Law at the State University of Rio de Janeiro (UERJ) in partnership with the Institute of Technology and Society (ITS). Lawyer at the Abramides e Gonçalves law firm. E-mail: mariafernandalm@icloud.com

artificial intelligence is used to help society by promoting inclusion and equity, instead of perpetuating inequalities.

The research in this article aims to explore the various aspects of algorithmic discrimination, analyzing the matrix of its causes, its impacts on society, and possible solutions. Initially, an overview of the fundamental concepts related to artificial intelligence learning will be provided, highlighting the sensitive points that enable algorithmic discrimination by demonstrating real cases where these problems have manifested themselves, highlighting the social and ethical consequences. Then, the ethical challenges involved in artificial intelligence data science will be discussed. Finally, strategies and best practices to mitigate algorithmic discrimination will be examined, promoting a healthy development for this technology.

## 1. The ways in which intelligences learn artificial and the core of the problem involved algorithmic discrimination

There is much discussion about algorithmic discrimination, however, to understand the core of this discussion it is necessary to understand how the different ranges of artificial intelligences learn.

Artificial intelligence learning is a technique, a complex process, where in a short explanation, we can say that a variety of cases are analyzed and a relationship is made between all of them. In this way, artificial intelligence analyzes a diverse range of data and acquires knowledge through these data patterns.

The algorithms and all systems involved in artificial intelligence are extremely volatile, constantly adapting to achieve goals. This phenomenon is only possible through the machine learning technique, popularly known as *machine learning*, which allows systems to learn and improve their performance through a set of data, in order to enable the performance of various actions without having been explicitly programmed to do so.<sup>2</sup>

Simply put, machine learning, or *machine learning*, is based on a set of data. Calculated by the machine through

2. JANIESCH, C.; ZSCHENCH, P.; HEINRICH, K. Machine learning and deep learning. arXiv.org, Springer, [2331-8422], 2021. Available at: <https://arxiv.org/pdf/2104.05314>. Accessed on: July 17, 2024.

through various repetition training, it begins to find patterns, generating responses that help in the most diverse fields of human activity, from disease prognosis, through fraud detection and even in popular facial recognition and voice recognition.

Arthur Samuel discusses the topic<sup>3</sup>“Machine learning is the field of study that gives computers the ability to learn without being explicitly programmed.”

Based on the questions presented and the availability of data, there are several ways to implement the *machine learning*. Authors Lloyd, Mohseni and Rebentrost posit three types of machine learning.<sup>4</sup>

The first model presented is known as supervised learning, where algorithms are trained based on labeled data sets, through which the machine is trained to classify predictions from this data, where each input example is associated with a desired output. The objective of this learning is for the machine to interactively classify various features to ultimately achieve the desired result based on the classified features.

The second model presented is unsupervised learning, unlike the first model, in this one the algorithms are trained to work with unlabeled data, and seek to discover hidden patterns or structures in the data, it is commonly used in situations where it is necessary to use large-scale data learning, the popular *big data*, so that the use of this model allows for greater segmentation within the customer portfolio, generating more effective communication with the system operator's target audience.

The third model is known as reinforcement learning, being the most different among those mentioned. In this context, the dynamics of the algorithms work based on the use of rewards and penalties for the action performed, through which the objective is to learn a policy that maximizes the reward accumulated over time. Its use is commonly focused on games.<sup>5</sup>

Given the availability of all these technologies, the market has been advancing more and more, the use of artificial intelligence has become increasingly

3. SAMUEL, A. Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development*, vol. 3, n. 3, p. 210-229, 1959. Available at: <https://people.csail.mit.edu/brooks/idocs/Samuel.pdf> . Accessed on: July 17, 2024.

4. LLOYD, S.; MOHSENI, M.; REBENTROST, P. Quantum algorithms for supervised and unsupervised machine learning. Available at: <https://arxiv.org/pdf/1307.0401> . Accessed on: July 17, 2024.

5. LLOYD, S.; MOHSENI, M.; REBENTROST, P. *Quantum algorithms for supervised and unsupervised machine learning*. Available at: <https://arxiv.org/pdf/1307.0401> . Accessed on: July 17, 2024.

more dynamic, reaching different groups of consumers of this product in various areas of society. With the popular dissemination of the most diverse artificial intelligences, the mistaken idea was created that such technology is taken from a neutral point of view, so that all its decisions would be made from a totally neutral point of view, this understanding highlights the core of the problem to be discussed in this article.

Safiya Umoja Noble says on the subject: "Algorithms are not neutral; they reflect the priorities, values and judgments of those who have the power to shape them."<sup>6</sup>

The world forgets that the functionality of artificial intelligence is closely linked to the way it was programmed and the database used in its programming, so that its results will always be related to the data provided to that machine. It is important to emphasize that this data is not neutral; quite the opposite, it can be closely related to various discriminatory biases of its programmers and of an entire society.

It is important to emphasize that human society is far from being an ideal society, and is increasingly dominated by prejudices. In this context, the core of the issue surrounding algorithmic discrimination begins with the algorithms themselves, which may be imbued with ideological biases from their own programmers. Such transmission of these biases is not necessarily linked to a bad intention to pass on such prejudices, and may be linked to a human error that was transmitted to the programming without further perception. However, in any case, such transmission will directly affect the results of the tool's decisions.

However, even if algorithms are not influenced by the ideological biases of their programmers, they may still have discriminatory biases that are embedded in their own data sets, so that these algorithms can generate clearly prejudiced results when fed with completely distorted concepts and values.

It is important to emphasize that artificial intelligences replicate what they have been taught, so they learn from the biases of the data that has been made available to them, making it very easy for their programmers to create artificial intelligences that are driven by completely discriminatory data.

6. NOBLE, SU *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press, 2018.

so that all their decisions will be made by these same biases, further propagating these prejudices. In today's society, such discriminatory thoughts are on the rise, so that artificial intelligences built on the basis of distorted and discriminatory data are becoming increasingly common.

Once these questions have been clarified, we can conclude that the machine itself is not prejudiced, it does not have discriminatory biases, but the human beings behind its development can cause these distorted biases to be inserted into its learning process, affecting all its decisions.<sup>7</sup>

Algorithmic discrimination works like a mathematical formula. Whenever a system is fed with data containing discriminatory biases, its algorithmic decisions will replicate these same biases, resulting in even more discrimination and, consequently, a serious violation of human rights. As an example of such a statement, it is possible to analyze the use of algorithms in the policing system based on explicitly biased crime statistics. The decisions of this policing system tendentiously perform greater monitoring in neighborhoods with a higher concentration of immigrants. In this way, this system suggests the deployment of a greater number of police officers to these locations, so that all police incidents are recorded, suggesting that neighborhoods with a higher concentration of immigrants have a high crime rate. This finding, however, is not true. What ends up happening is that because of the greater number of police officers, all incidents are recorded, unlike other neighborhoods that, because they have a smaller number of police officers deployed, consequently have fewer incidents recorded and, therefore, a lower crime rate. This type of predictive policing needs to be analyzed and used with extreme caution, given that it can create a cycle of extremely biased and dangerous results, where prejudiced human decisions are amplified, resulting in new decisions that exalt discriminatory positions and, consequently, seriously offend human rights.<sup>8</sup>

7. WEST, Sarah Myers; WHITTAKER, Meredith; CRAWFORD, Kate. Discriminating systems: gender, race and power in AI. New York: New York University, AI Now Institute, 2019. Available at: <https://ainowinstitute.org/discriminatingystems.pdf>. Accessed on: July 22, 2024.

8. BORGESIU, FJZ. Strengthening legal protection against discrimination by algorithms and artificial intelligence. The International Journal of Human Rights, vol. 24, no. 10, p. 1572-1593, 2020. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3561441](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561441). Accessed on: July 18, 2024.

On the subject, Frank Pasquale explains that “The algorithm is a mirror: it reflects our priorities and prejudices, but amplified and made invisible.”<sup>9</sup>

Given everything that has been presented, it can be concluded that algorithmic discrimination in the context of artificial intelligence begins even before the decisions of such technologies are inserted into the real world. Thus, it is demonstrated that the basis for algorithmic discrimination lies in machine learning itself, showing that the core of this entire issue is centered on the moment in which artificial intelligence is being developed. It is therefore indicated that the monitoring of these artificial intelligences should begin at the time of the creation of such technology.

Regarding the discussion, Joy Buolamwini and Timnit Gebru highlight that “The danger of algorithmic discrimination is that it can escalate at a pace and scale that surpasses human capabilities for monitoring and intervention.”<sup>10</sup>

Elucidating this statement, it is clear that the issue of algorithmic discrimination requires attention. The world of technology is immeasurable and the consequences of this world have the same proportions, which will not necessarily be positive.

The speeches by Joy Boulamwini and Timnit Gebru highlight the theme that has been discussed in this chapter: that algorithmic discrimination needs to be discussed when creating artificial intelligence. Considering that from the moment that data with discriminatory biases feeds artificial intelligence, the results of the decisions of this technology are immeasurable, in a way that constitutes a serious attack on human rights and the constitution and exalts the discriminatory principles wrongly inserted for many years in society.<sup>11</sup>

## **2. The challenges involved in regulating intelligence artificial to ensure the promotion of equality and avoid discrimination.**

There is a consensus on the need to regulate artificial intelligence; however, the difficulty in implementing this regulation is

9. PASQUALE, F. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015. Available at: <https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf> . Accessed on: July 18, 2024.

10. BUOLAMWINI, J.; GEBRU, T. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. *Proceedings of Machine Learning Research*, vol. 81, p. 1-15, 2018. Available at: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> . Accessed on: July 15, 2024.

11. *Ibid.*

evident. This technology is among the situations that urgently require regulation, but little is known about how to implement truly effective regulation.

The regulation of artificial intelligence involves several topics from the world of law, but it is clear that the topic concerning algorithmic discrimination requires greater attention in view of the recent high-profile cases involving such technology.

Although there is no specific legislation regulating artificial intelligence and its effects, it is important to highlight that Brazilian legislation guarantees the promotion of equality among all and punishes any and all conduct with a discriminatory bias.

The Federal Constitution expressly provides that “Art. 5 All are equal before the law, without distinction of any nature, guaranteeing Brazilians and foreigners residing in the country the inviolability of the right to life, liberty, equality, security and property.”<sup>12</sup>

Law No. 7,716, popularly known as the Racial Crime Law, states in its first article that “Crimes resulting from discrimination or prejudice based on race, color, ethnicity, religion or national origin will be punished in accordance with this Law.”<sup>13</sup>

Law No. 7,716, mentioned above, also regulates that any practice of any discriminatory act is a crime and will be punishable, further highlighting that any discriminatory act carried out on the world wide web is also a crime and aggravates the punishment:

Art. 20. Practice, induce or incite discrimination or prejudice based on race, color, ethnicity, religion or national origin.

Penalty: imprisonment of one to three years and a fine.

§ 2 If any of the crimes provided for in this article are committed through the media, publication on social networks, the world wide web or publication of any nature.

Penalty: imprisonment of two to five years and a fine.<sup>14</sup>

12. BRAZIL. Constitution (1988). *Constitution of the Federative Republic of Brazil: promulgated on October 5, 1988*. Brasília, DF: Federal Senate: Graphic Center, 1988. Available at: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm) . Accessed on: July 19, 2024

13. BRAZIL. Law No. 7,716, of January 5, 1989. Defines crimes resulting from racial or color prejudice. *Official Gazette of the Union: section 1*, Brasília, DF, p. 240, January 6, 1989. Available at: [https://www.planalto.gov.br/ccivil\\_03/leis/l7716.htm](https://www.planalto.gov.br/ccivil_03/leis/l7716.htm) . Accessed on: July 19, 2024.

14. *Ibid.*

Having clarified these issues and highlighting the idea already mentioned, there is a consensus on the need to advance in the search for algorithmic justice, especially to mitigate the risks of direct (unequal treatment) and indirect (unequal impact) discrimination in algorithmic decisions. However, there is still no answer as to how this regulation will be carried out. It is believed that one possibility to mitigate these risks is by investing in research that clarifies the nature of ethical risks, providing solid and transparent guidelines for the governance of algorithmic design and the use of technology.<sup>15</sup>

Tsamados' idea is extremely relevant, but it once again involves the problem that all these strategies never left the world of ideas, so that regulation is becoming increasingly distant and discrimination involving artificial intelligence is expanding more and more. In this way, the regulation of such discriminatory acts ends up going in the opposite direction to what seems to be the solution to the issue.

As long as there is no legislation regulating artificial intelligence, the effects of the misuse of this technology will continue to exist, so that the root cause of this problem lies in the lack of transparency of the mechanisms and data linked to artificial intelligence, resulting in the lack of protection of individual rights.<sup>16</sup>

Regarding the lack of transparency of mechanisms and data linked to artificial intelligence, it is worth highlighting that this information does not have a clear author. There is no person responsible for the data used to make these decisions, so this lack of transparency makes it extremely difficult to find the source to hold such discrimination accountable, given the discriminatory biases of the algorithms.<sup>17</sup>

Transparency is essential to prevent discriminatory biases and avoid a scenario of insecurity for users of such technology. On this subject, it is highlighted:

15. TSAMADOS, A.; AGGARWAL, N.; COWLS, J.; MORLEY, J.; ROBERTS, H.; TADDEO, M.; FLORIDI, L. The ethics of algorithms: key problems and solutions. *AI & SOCIETY*, v. 37, p. 215-230, 2022. Available at: <https://link.springer.com/article/10.1007/s00146-021-01154-8>. Accessed on: July 22, 2024.

16. AZEVEDO, Ingrid Borges de. Facial recognition and law: proposals for an anti-discriminatory AI. 2021. 65 p. Course Conclusion Work (Undergraduate Degree in Law)-University of Brasília, Brasília, 2021. Available at: <https://bdm.unb.br/handle/10483/29805>. Accessed on: July 22, 2024.

17. BONA, Celito de; SCHONS, Eduarda Arruda; LOPES-FLOIS, Luiza. Artificial intelligence: is there ethics in the implementation of algorithms? *Applied Social Sciences in Review*, [SL], v. 25, n. 45, p. 225-246, Aug. 18, 2023. Western Paraná State University -UNIOESTE. Available at: <https://e-revista.unioeste.br/index.php/csaemrevista/article/view/31510/22369>. Accessed on: July 21, 2024.

This lack of regulation, accountability, auditing and transparency in the use of AI has been generating harmful consequences from a legal and social perspective, as it perpetuates and increases the discrimination and selectivity that permeates criminal control and the agencies that comprise it. And all under the illusory impression that it is based on impartial, precise and objective mathematical models. In truth, the results are loaded with subjectivity and racist biases that tend to catalyze well-defined social sectors for marginalization and discrimination.<sup>18</sup>

Regarding the topic presented in light of the difficulty of regularization, a new discussion arises regarding the responsibility of the company or programmer who developed the artificial intelligence.

The main issue to be analyzed regarding the liability of the company or programmer is the intention of this developer agent, analyzing whether he had any intention of generating discriminatory results or if he had any possibility of monitoring these results. Thus, if it is demonstrated that the developer agent had clear influence or intention in the discriminatory results, he must be held responsible.

In this regard, the problem of lack of regulation arises again, given that the only way to analyze the intention and monitoring of the developer agent is through the traceability of the algorithm used by the machine. This information is only available to the developer agent, so that, due to the lack of regulation on the subject, the information becomes inaccessible and consequently undermines the accountability of the subjects involved in the discriminatory results of artificial intelligence.

The regulation of artificial intelligence in Brazil seems to be increasingly distant from reality, but there is already a law that regulates the processing of personal data: Law No. 13,709/2018, the General Data Protection Law (LGPD). This law regulates the processing of personal data in Brazil, both online and offline, by individuals or legal entities, under public or private law. Its main objectives are to protect the fundamental rights of freedom and privacy, as well as the free development of the natural person's personality.

18. CHAVES JUNIOR, Airto; GUASQUE, Bárbara; PÁDUA, Thiago Santos Aguiar de. Racial segregation and algorithmic biases: racist machines in the context of criminal control. *Brazilian Journal of Law*, [SL], v. 19, n. 2, p. 1-30, Sep 22, 2023. Meridional Higher Education Complex SA Available at:<https://doi.org/10.18256/2238-0604.2023.v19i2.4768>. Accessed on: July 22, 2024.. *Brazilian Law Journal*, [SL], v. 19, n. 2, p. 1-30, September 22, 2023. Meridional Higher Education Complex SA Available at:<https://doi.org/10.18256/2238-0604.2023.v19i2.4768>. Accessed on: July 22, 2024.

The General Data Protection Law represents an important milestone in the protection of personal data in Brazil, but it distances itself from data regulation in the sense of avoiding algorithmic discrimination, so that this law and its articles do not solve the problems announced in this chapter. It is possible to use some articles of the legal diploma as a basis for specific legislation on the subject, however, it is clear that there is a need for complementary regulation to the General Data Protection Law.

The diploma of Art.6 of the General Data Protection Law ratifies issues regarding data discrimination:

Art. 6 Personal data processing activities must observe good faith and the following principles:

(...)

VIII – prevention: adoption of measures to prevent the occurrence of damages due to the processing of personal data;

(...)

IX–Non-discrimination: impossibility of carrying out processing for unlawful or abusive discriminatory purposes;<sup>19</sup>

The aforementioned article 6 clarifies that personal data cannot be used for unlawful or abusive discriminatory purposes, but this legislation remains incomplete, given that there is a clear prohibition on this discriminatory practice involving the use of data. However, there is no punishment for such conduct, so it is up to everyone to understand that even though such conduct is prohibited, if it is practiced, it will not be punished.

There is currently a lot of talk about algorithmic justice, and the topic is being studied worldwide in light of the regulation of artificial intelligence, but no predictive analysis can reliably indicate that there will be no discriminatory risk from artificial intelligence systems.<sup>20</sup>

Therefore, it is clear that the only way to begin an attempt to eradicate algorithmic discrimination will begin when developers of such technology and governments start working together to ensure that artificial intelligence is used in an ethical and fair manner, in which technology must be regulated by a legislative framework with a

19. BRAZIL. Law No. 13,709 of August 14, 2018. Provides for the protection of personal data and amends Law No. 12,965 of April 23, 2014 (Civil Rights Framework for the Internet). Official Gazette of the Union: section 1, Brasília, DF, p. 1, Aug. 15, 2018. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm) . Accessed on: July 22, 2024.

20. HUPFFER, Haide Maria; SANTANNA, Gustavo da Silva. Artificial intelligence and algorithmic discrimination: regulatory frameworks and ethical parameters. Available at: <http://www.guaritadigital.com.br/casaleirialivros/iasq/iasq.4.pdf> . Accessed on: July 15, 2024

set of rules that must be followed by the tool, so that it recognizes discriminatory acts and data and does not spread them.<sup>21</sup>

In a society where technology is used on a large scale, the creation of a law to regulate artificial intelligence is essential to protect the individual rights of citizens, especially the most vulnerable populations. Regulations must be based on ethical precedents so that algorithmic decisions are transparent and non-discriminatory.

### 3. New horizons in internet networks in light of the Project of Law No. 2338/2023

Considering all the themes discussed in this article, it is easy to analyze that the regulation of artificial intelligence is necessary, but it is also necessary to understand that even with all the regulation on the subject, there will only be significant changes in the scope of algorithmic discrimination when there is social awareness regarding the entire issue of discrimination, not only in the digital world, but in the entire real world.

Society is constantly trying to combat all discriminatory and prejudiced acts, but this fight is far from ideal. Even with so many advances in society, discriminatory culture is still widespread throughout the world and the internet is not exempt from this wave of dissemination, so it is necessary to seek new horizons in the networks to combat these acts.

To face all these ethical challenges, society's awareness needs to be aligned with strong regulations, which in turn need to be developed by experts in the field in order to enable these regulations to have real effects, moving beyond the world of ideas to regulate the issue and punish those who disseminate acts with discriminatory biases.

The United Nations (UN) clarifies the need for new horizons in the world of artificial intelligence regulation:

Artificial intelligence promises to drive advances in several sectors, but its deployment must be carefully managed to avoid adverse impacts on human rights and social values.

21. SINGAPORE. Personal Data Protection Commission. Model AI Governance Framework. Available at: <https://www.p.gov.sg/ajuda-e-recursos/2020/01/model-ai-vai-estrutura>. Accessed on: July 17, 2024

Regulatory measures must be implemented to ensure that AI technologies are developed and used in ways that promote inclusion and equity. This involves creating policies that require AI systems to be assessed for bias and their potential effects on different demographic groups. In addition, transparency in AI decision-making processes and accountability mechanisms must be established to build public trust and prevent abuse. It is essential that the benefits of AI are broadly shared and that safeguards are in place to protect against unintended consequences.<sup>22</sup>

In line with the UN's position, the OECD (Organization for Economic Cooperation and Development) takes the following position:

AI governance must be grounded in principles that emphasize inclusion, transparency, and accountability. Regulatory frameworks need to be forward-looking, anticipating the rapid evolution of AI technologies and their potential societal impacts. Policies should encourage the responsible development and deployment of AI by ensuring that it is aligned with democratic values and human rights. This involves creating mechanisms for ongoing monitoring and evaluation of AI systems, as well as fostering international cooperation to address the global challenges posed by AI. By taking a holistic approach to AI regulation, we can harness its transformative potential while safeguarding against risks and ensuring that its benefits are equitably distributed. (OECD, 2019)<sup>23</sup>

According to these positions, the whole world has been understanding the importance of regulating artificial intelligence and has been starting the regulatory movement, ushering in a new era of horizons in networks. Currently, Brazil is very behind in this matter in relation to other countries in the world. For this statement, we can cite the European Union, which as a global reference in May 2024 enacted the Artificial Intelligence Law, which regulates the entire subject and emphasizes the fight against algorithmic discrimination.

22. UNITED NATIONS. The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation. 2019. Available at:<https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf> . Accessed on: July 17, 2024.

23. OECD.Principles on Artificial Intelligence. 2019. Available at:<https://www.oecd.org/going-digital/ai/principles/> . Accessed on: July 17, 2024.

In Brazil, there are more than 46 bills for the regulation of artificial intelligence, and although the range of projects is extensive, the country is still far from effective regulation. Among the 46 projects, the one that is most advanced is Bill (PL) No. 2338/2023, reported by Senator Eduardo Gomes (PL-TO). Although the project in question is most advanced, this progress is still small, considering that its vote was postponed for the third time on July 9, 2024.

Specifically regarding bill (PL) n° 2338/2023, its text has some clear objectives, such as the promotion of technological innovation in the face of the sustainable development of artificial intelligence, the establishment of guidelines for transparency regarding the explainability of artificial intelligence systems and, most importantly for this article, the guarantee of respect for fundamental rights, human dignity and privacy.

Bill (PL) No. 2338/2023 extols the principle of transparency in the world of artificial intelligence, which is an essential principle for combating algorithmic discrimination, given that AI systems must be designed in a transparent manner, allowing people to understand how they work and how decisions are made. Transparency also requires the disclosure of information about the data used and the criteria adopted for automated decisions, making it possible to understand how possible discriminatory decisions would be generated and, as a consequence, allows the punishment of agents who use such technologies to promote discriminatory acts.

Article 5 of bill (PL) n° 2338/2023 highlights non-discrimination in the world of artificial intelligence:

Art. 5. Persons affected by artificial intelligence systems have the following rights, to be exercised in the manner and under the conditions described in this Chapter:

(...)

V-right to non-discrimination and to the correction of direct, indirect, illegal or abusive discriminatory biases; (BRAZIL, Bill No. 2338, 2023).

24

Still in its article 19 it informs that there will be adoption of measures to combat algorithmic discrimination:

24. BRAZIL. National Congress. Bill No. 2338, of 2023. Provides for the regulation of artificial intelligence. Available at: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1720798347645&disposition=inline> . Accessed on: July 24, 2024

Art. 19. Artificial intelligence agents shall establish governance structures and internal processes capable of guaranteeing the security of the systems and the fulfillment of the rights of affected persons, under the terms provided for in Chapter II of this Law and the relevant legislation, which shall include, at least:

(...)

III—adequate data management measures to mitigate and prevent potential discriminatory biases; (BRAZIL, Bill No. 2338, 2023).<sup>25</sup>

Bill (PL) n° 2338/2023 highlights the attempt to combat algorithmic discrimination, in a way that would initiate the necessary regulation on the subject in order to eliminate discrimination within digital technologies.

Bill (PL) n° 2338/2023 has several criticisms regarding its content and its way of operation, according to Thiago Marcílio's idea, the aforementioned bill does not reflect the true needs of regulating artificial intelligence and even becomes controversial with the General Data Protection Law (LGPD) itself, however it opens up new horizons for networks in Brazil, in a way that it needs to be understood as an advance towards the ideal in the world of networks.<sup>26</sup>

Although these proposals represent a normative ideal, their effective implementation in Brazil remains distant. The country still lacks a robust and effective legal framework to regulate artificial intelligence, which prevents these objectives from being achieved in the near future. However, from an optimistic perspective, the mere creation of a strong bill, albeit with several problems, is already evidence of the beginning of a path towards the ideal.

## Final considerations

Algorithmic discrimination represents a critical challenge in the growing use of AI technologies, reflecting and amplifying existing biases and prejudices in society. This phenomenon does not arise from the technology itself, but rather from the way data is collected and processed, as well as from the bias choices of its own developers. Therefore,

25. Ibid.

26. MARCÍLIO, Thiago. Four controversies about the project that regulates artificial intelligence. Legal Consultant, São Paulo, February 29, 2024. Available at: <https://www.conjur.com.br/2024-fev-29/quatro-polemicas-sobre-o-projeto-que-regula-a-inteligencia-artificial/>. Accessed on: October 14, 2024

Artificial intelligence, if not properly regulated and monitored, can perpetuate and intensify algorithmic discrimination, perpetuating discriminatory guidelines that are ingrained in society.

To effectively combat algorithmic discrimination, it is essential that AI regulation is robust and effective. In Brazil, although the Constitution and the Racial Crime Law already establish the prohibition of discriminatory acts, there is still a significant gap in specific legislation that addresses the unique challenges presented by AI. The lack of transparency and the difficulty in tracking responsibility for the data and algorithms used make it difficult to apply punishments and ensure algorithmic justice.

Regulation of AI must be developed with great care and transparency, so that those who perpetuate algorithmic discrimination can be held accountable. This requires collaboration between technology developers and policymakers to create a legal framework that ensures the protection of individual rights and promotes equity.

The global movement towards the regulation of intelligence, exemplified by the recent European Union Artificial Intelligence Act, highlights the urgency and importance of this effort. In Brazil, Bill No. 2338/2023 represents a significant step forward, but there is still a long way to go.

In conclusion, algorithmic discrimination is a reflection of society's thinking, making it a complex issue that requires a multifaceted approach, involving legislation, monitoring and broader social awareness. Only through a coordinated and continuous effort across society will it be possible to ensure that artificial intelligence contributes to a more just and inclusive society, rather than perpetuating the inequalities that are rooted in today's society.

## References

AZEVEDO, Ingrid Borges de. *Facial recognition and law: proposals for anti-discriminatory AI*. 2021. 65 p. Final Course Work (Undergraduate Degree in Law)–University of Brasília, Brasília, 2021. Available at: <https://bdm.unb.br/handle/10483/29805> . Accessed on: July 22, 2024.

BONA, Celito de; SCHONS, Eduarda Arruda; LOPES-FLOIS, Luiza. Artificial intelligence: is there ethics in the implementation of algorithms? *Applied Social Sciences in Review*, [SL], v. 25, n. 45, p. 225-246, Aug. 18, 2023. Western Paraná State University–UNIOESTE. Available at:

<https://e-revista.unioeste.br/index.php/csaemrevista/article/view/31510/22369> . Accessed on: July 21, 2024.

BORGESIUS, FJZ Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, v. 24, n. 10, p. 1572-1593, 2020. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3561441](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561441) . Accessed on: July 18, 2024.

BRAZIL. National Congress. *Bill No. 2338, of 2023*. Provides for the regulation of artificial intelligence. Available at: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1720798347645&disposition=inline> . Accessed on: July 24, 2024.

BUOLAMWINI, J.; GEBRU, T. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research*, v. 81, p. 1-15, 2018. Available at: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> . Accessed on: July 15, 2024.

CHAVES JUNIOR, Airto; GUASQUE, Bárbara; PÁDUA, Thiago Santos Aguiar de. Racial segregation and algorithmic biases: racist machines in the context of criminal control. *Brazilian Journal of Law*, [SL], v. 19, n. 2, p. 1-30, 22 Sep. 2023. Meridional Higher Education Complex SA Available at: <https://doi.org/10.18256/2238-0604.2023.v19i2.4768> . Accessed on: July 22, 2024.

HENRIQUES, Isabella Vieira Machado; *Algorithmic discrimination and inclusion in artificial intelligence systems – a reflection from the perspective of children's rights in the digital environment*. Available at: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5993/pdf> . Accessed on: July 19, 2024.

HUPFFER, Haide Maria; SANTANNA, Gustavo da Silva. *Artificial intelligence and algorithmic discrimination: regulatory frameworks and ethical parameters*. Available at: <http://www.guaritadigital.com.br/casaleialivros/iasq/iasq.4.pdf> . Accessed on: July 15, 2024.

JANIESCH, C.; ZSCHENCH, P.; HEINRICH, K. Machine learning and deep learning. arXiv.org, *Springer*, [2331-8422], 2021. Available at: <https://arxiv.org/pdf/2104.05314> . Accessed on: July 17, 2024.

LLOYD, S.; MOHSENI, M.; REBENTROST, P. *Quantum algorithms for supervised and unsupervised machine learning*. Available at: <https://arxiv.org/pdf/1307.0401> . Accessed on: July 17, 2024.

MARCÍLIO, Thiago. Four controversies about the project that regulates artificial intelligence. *Legal Consultant*, São Paulo, February 29, 2024. Available at: <https://www.conjur.com.br/2024-fev-29/quatro-controversias-about-the-project-that-regulates-artificial-intelligence/> . Accessed on: October 14, 2024.

UNITED NATIONS. The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation. 2019. Available at: <https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf> . Accessed on: July 17, 2024.

NOBLE, SU *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press, 2018.

OECD. *OECD Principles on Artificial Intelligence*. 2019. Available at: <https://www.oecd.org/going-digital/ai/principles/> . Accessed on: July 17, 2024.

PASQUALE, F. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015. Available at:<https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf> . Accessed on: July 18, 2024.

RESMINI, Carol; PAGLIARINI, Eduarda; MORAES, Júlia D'Alascio Rangel de; LANDMEIER, Laura Vardanega. *Social challenges in the era of artificial intelligence: a focus on the racial equity gap*. Available at:<https://ojs.sites.ufsc.br/index.php/avant/article/view/7661/6164> . Accessed on: July 17, 2024.

SAMUEL, A. Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development*, v. 3, n. 3, p. 210-229, 1959. Available at:<https://people.csail.mit.edu/brooks/idocs/Samuel.pdf> . Accessed on: July 17, 2024.

SINGAPORE. *Personal Data Protection Commission. AI Governance Framework Model*. Available at:<https://www.p.gov.sg/ajuda-e-recursos/2020/01/model-ai-vai-estrutura> . Accessed on: July 17, 2024

TSAMADOS, A.; AGGARWAL, N.; COWLS, J.; MORLEY, J.; ROBERTS, H.; TADDEO, M.; FLORIDI, L. The ethics of algorithms: key problems and solutions. *AI & SOCIETY*, v. 37, p. 215–230, 2022. Available at:<https://link.springer.com/article/10.1007/s00146-021-01154-8> . Accessed on: July 22, 2024.

WEST, Sarah Myers; WHITTAKER, Meredith; CRAWFORD, Kate. *Discriminating systems: gender, race and power in AI*. New York: New York University, AI Now Institute, 2019. Available at:<https://ainowinstitute.org/discriminatingystems.pdf> . Accessed on: July 22, 2024.

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

9

**A critical analysis  
about discriminatory  
algorithmization in the context of  
criminal law**

Luisa Amelia

Summary: Introduction. 1. Artificial Intelligence: concept, evolution and developments. 2. Algorithmic discrimination and its effects. 3. Critical analysis on the use of discriminatory algorithms in criminal law. Final considerations. References.

## Introduction

Modern society, called the information society<sup>2</sup>, is driven by data of the most varied levels, which fall on people, their habits and their characteristics and only after a few years of evolution of the collecting technologies, it became possible to mine and understand it, called processing. In this scenario, it is a fact that everything we do and even what we don't do, like when we open a sales page but decide not to buy something *online*, for example, remains recorded and is considered navigation data.

In this context, it is worth noting that data has always been an important asset, but the ways of interpreting it, even with computational resources, have not always been so assertive. However, this has been changing with the rise of data processing technologies and, more recently, with the rise of Artificial Intelligence.

In this way, activities that were considered hypercomplex have become simple because they can be performed with precision by systems, so that their use has advanced to areas such as medicine and law. In Brazil, for example, the STF allows the use of AI to analyze filed appeals, in order to identify repetitive appeals in their matters, which has proven to be an efficient solution from the point of view of procedural speed and economy.

However, despite the relevance of this type of technology for global scientific progress, its use and rise is accompanied by concerns about its social, ethical and legal implications, given that these

1. Associate lawyer at Peter Fernandes and Marihá Viana Advogados Associados. She holds a bachelor's degree in Law from the University Center of Brasília (UniCEUB) and a master's degree in Criminology with a specialization in Criminal Policy from the University of Barcelona/Spain. She is currently studying a postgraduate degree in Digital Law at the Institute of Technology and Society (ITS), in partnership with the State University of Rio de Janeiro (UERJ) and the Center for Studies and Research in Legal Education (CEPED).

2. WEBSTER, Frank. *Theories of the information society*. London: Routledge, 1995.

systems should not place themselves above people's rights<sup>3</sup>. This highlights the need to discuss the ethical, transparent and responsible use of AI, as well as its necessary regulation. However, in this discussion, we cannot lose sight of the need for continuous technological progress to coexist as an effective protection of citizens' rights.

Thus, this research aims to carry out a critical analysis of the risks of discriminatory decisions led by Artificial Intelligence in the context of Criminal Law, as well as its implications and possible proposals to circumvent the situation. It is worth noting that the study was carried out using the dialectical deductive method, through bibliographic research in scientific articles, books and legislation related to the subject and was structured in three chapters.

The first chapter provides an analysis of Artificial Intelligence, specifically in relation to its concept, uses and dynamics of discussion in Brazil. It also addresses the impressions listed in the literature, competition and ethical issues, as well as regulatory proposals and what is expected from efficient regulation on the subject in Brazil.

In turn, the second chapter addressed the issue of algorithmic discrimination, considering the risks associated with AI decision-making. Given the possible biased resolutions with negative human prejudices and preconceptions, an assessment of the ethical limits and legal assumptions in this regard was proposed.

Finally, in the third chapter, based on the hypothesis of using Artificial Intelligence in the context of Criminal Law, it was demonstrated, by the literature related to the subject, that its use can perpetuate racist and segregationist decisions. For this reason, the proposal that was reached to overcome the problem was to prevent the use of systems that may present discriminatory biases, in accordance with what is already provided for in Resolution No. 332 of the National Council of Justice (CNJ)<sup>4</sup> and new draft Resolution developed by the Working Group on Artificial Intelligence in the Judiciary (GTIA) of the CNJ<sup>5</sup>, as well as the importance of including human participation in AI decision-making processes.

3 MOURÃO, Licurgo; INDUSTRIAL, Revolution. Regulation of artificial intelligence in Brazil. *Intellegentiae artificialis, imperium et civitatem*, p. 73-89, 2022. Available at: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Accessed on July 27, 2024.

4. National Council of Justice. *Resolution No. 332, of August 21, 2020*. Available at: [https://atos.cnj.jus.br/atos/deta\\_lhar/3429](https://atos.cnj.jus.br/atos/deta_lhar/3429). Accessed on: July 29, 2024.

5 NATIONAL COUNCIL OF JUSTICE (CNJ). *Draft proposal for resolution 332*. Brasília: CNJ, 2024. Available at: <https://www.cnj.jus.br/wp-content/uploads/2024/09/minuta-proposta-resolucao-332-cnj-rev.pdf>. Accessed on: October 13, 2024.

In the final considerations, it was highlighted that the use of automated systems in actions involving criminal law is risky, as it is already a discriminatory system in itself.

## 1. Artificial Intelligence: concept, evolution and developments

The scientific community defines the term “artificial intelligence” as “the reasoning capacity of machines that reproduces the functioning of the human mind”<sup>6</sup>, as has been done by ChatGPT<sup>7</sup>(*Generative Pre-Trained Transformer*), one software developed by OpenAI.

It is considered a hot topic in social, political, legal debate and in the world's mainstream media. This is due, in particular, to the promise of transforming the way society is organized, marking the peak of technological development on a global scale. As a result, there is a development race, disputed by countries that want to be the protagonists in the development and use of AI, which has been concentrated, by the way, between already known powers such as the United States and China.<sup>8</sup>

This rapid development, combined with its transformative potential, has served as a basis for understanding that the planet is facing a new era. These technologies truly have great transformative potential, to the point of raising questions about whether some professions will soon be replaced. It is clear, therefore, that AI is transforming social structures, including the way humans deal with technology, which has led the literature to consider the rise of a fourth Industrial Revolution.<sup>9</sup>

So much so that the Organization for Economic Cooperation and Development (OECD), when evaluating the transformative and modifying potential of this type of technology, drew attention to the need to define ethical limits regarding its use, especially due to the competitive and democratic implications that they can cause, as Mourão explains:

6. MOURÃO, Licurgo. Regulation of artificial intelligence in Brazil. *Intellegentiae artificialis, imperium et civitatem*, p. 73, 2022. Available at: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitem.pdf?sequence=1#page=74>. Accessed on July 27, 2024.

7. ChatGPT “works from an updated knowledge base that allows it to decode words to offer textual responses to people. It is a model trained from text data available on the internet” (FIA, 2024).

8. PARENTONI, Leonardo Netto; VALENTINI, Rômulo Soares; ALVES, Tárík César Oliveira E. Overview of the Regulation of Artificial Intelligence in Brazil: with emphasis on PL's No. 5,051/2019. *Electronic Journal of the Law Course at UFSM*, v. 15, n. 2, p. 2, 2020.

9. MOURÃO, Licurgo; INDUSTRIAL, Revolution. Regulation of artificial intelligence in Brazil. *Intellegentiae artificialis, imperium et civitatem*, p. 73, 2022. Available at: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitem.pdf?sequence=1#page=74>. Accessed on July 27, 2024.

[...] the Organization for Economic Cooperation and Development (OECD), recognizing that artificial intelligence is transforming societies, economic sectors and the future of work and that it has the potential to contribute to solving the main global challenges, highlighted that the transformations brought about by technological advances can affect societies and economies unequally, especially with regard to competition, transitions in the labor market, inequalities and implications for democracies and human rights, privacy and data protection and digital security.

In this scenario, there is growing global concern about defining ethical standards and limits for the use of artificial intelligence, seeking to regulate the use of new technologies in order to safeguard citizens' rights.<sup>10</sup>

In a short period of time, it is clear that artificial intelligence has developed in such a way that it can make decisions autonomously, that is, without human intervention in the phases following the formulation of the algorithm, which was made possible through the use of mechanisms of *machine learning* (machine learning) added to the techniques of *deep learning* (deep learning). This happened in such a surprising way that, in 2024, a certain artificial intelligence system already has the ability to create another, in addition to being able to integrate with others, aiming to improve results.<sup>11</sup>

In Brazil, for example, since 2020, the Federal Supreme Court (STF) has been using models of *machine learning* for the analysis of appeals received by the Court that deal with topics of general relevance.<sup>12</sup>

This mechanism used by the Brazilian Supreme Court allowed the insertion of “speed and accuracy in the analysis of a significant number of processes and situations, contemplating relevant principles of speed, efficiency and economy”<sup>13</sup>. This shows the advantage of using systems like this, as they facilitate human activity and can

10. MOURÃO, Licurgo. Regulation of artificial intelligence in Brazil. *Intellegentiae artificialis, imperium et civitatem*, p. 75-76, 2022. Available at: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Accessed on July 27, 2024.

11. REQUIÃO, Maurício; COSTA, Diego. Algorithmic discrimination: affirmative actions as a combat strategy. *Civilistica.com*, v. 11, n. 3, p. 3, 2022. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Accessed on: July 24, 2024.

12 MAIA FILHO, Mamede Said; JUNQUILHO, Tainá Aguiar. Victor Project: perspectives on the application of artificial intelligence to law. *Journal of Fundamental Rights and Guarantees*, v. 19, n. 3, p. 218, 2018.

13 PEIXOTO, Fabiano Hartmann. Victor Project: report on the development of artificial intelligence in the general repercussion of the Supreme Federal Court. *Brazilian Journal of Artificial Intelligence and Law-RBIAD*, v. 1, n. 1, p. 18. Available at: <https://www.rbiad.com.br/index.php/rbiad/article/view/4/4>. Accessed on: July 25, 2024.

deliver a positive result to society. However, as previously mentioned, a positive result in this sense does not eliminate the need to deal with the issue with the care it requires and does not exclude the urgency of regulation that defines ethical and legal criteria, so that its development continues to occur in strict compliance with the legislation.

Regarding this last point, in Brazil, the General Law on the Protection of Personal Data (Law No. 13,709/2018 – LGPD) opened the doors to regulation of the matter by providing for the possibility of the holder of personal data requesting the review of automated decisions, in accordance with art. 20.<sup>14</sup>. However, the respective law, far from regulating the matter, only highlighted the need for careful treatment of the matter, given that its impact covers not only personal data, but a range of other rights and social issues.

In 2020, Resolution No. 332/2020 of the National Council of Justice<sup>15</sup> dealt with the establishment of rules regarding ethics, transparency and governance for the use of artificial intelligence by the Judiciary<sup>16</sup>. This legislation was truly an important milestone for the treatment of the subject within the Brazilian judiciary, especially due to the alarming data on biased decisions of a discriminatory and even racist nature, which will be specifically addressed later in this study. Currently, there is a new draft of a Resolution developed by the Working Group on Artificial Intelligence in the Judiciary (GTIA) of the CNJ.<sup>17</sup>

The Federal Executive also intends to make efforts to outline a “Brazilian Artificial Intelligence Strategy” (EBIA), established by MCTI Ordinance No. 4,617/2021 and has as its premise “to guide the actions of the Brazilian State in favor of the development of actions, in their various aspects, that stimulate research, innovation and development of solutions in Artificial Intelligence, as well as its conscious, ethical use and in favor of a better future”<sup>18</sup>.

14. Art. 20. The data subject has the right to request a review of decisions taken solely on the basis of automated processing of personal data that affect his or her interests, including decisions intended to define his or her personal, professional, consumer and credit profile or aspects of his or her personality.

15. National Council of Justice. *Resolution No. 332, of August 21, 2020*. Available at: <<https://atos.cnj.jus.br/atos/detail/3429>>. Accessed on: July 29, 2024.

16 MOURÃO, Licurgo; INDUSTRIAL, Revolution. Regulation of artificial intelligence in Brazil. *Intellegentiae artificialis, imperium et civitatem*, p. 82, 2022. Available at: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74> . Accessed on July 27, 2024.

17 NATIONAL COUNCIL OF JUSTICE (CNJ). *Draft proposal for resolution 332*. Brasilia: CNJ, 2024. Available at: <https://www.cnj.jus.br/wp-content/uploads/2024/09/minuta-proposta-resolucao-332-cnj-rev.pdf> . Accessed on: October 13, 2024.

18 BRAZIL. Ministry of Science, Technology and Innovation. *Artificial intelligence*. Available at: <<https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial>> . Accessed on: July 29, 2024.

It is revealed that the EBIA represents a notable movement by the Federal Executive Branch, within the scope of the Ministry of Science and Technology, for having allowed a transversal discussion of the topic since the opening of a public consultation, in which it allowed the participation of several actors of society, until the publication of its scope covering several axes. However, the literature says that it is far from being a strategy, resembling more a mere letter of intent due to the generic propositions and without a pragmatic bias.<sup>19</sup>

In this sense, it is clear that the few movements seen in practice by the Brazilian State still do not correspond to a legitimate expectation of regulation of the matter, despite its urgency and indispensability.

It is also important to highlight that several Bills are currently being processed in the National Congress (CN) with the aim of regulating the matter. In this context, attention is drawn to Bill 2,338/2023, initiated by Senator Rodrigo Pacheco (PSD/MG), which has presented a propositional scope and is guided by the centrality of the human person as a foundation (art. 2, item I of the Bill), and which also proposes free enterprise as a premise (art. 2, item VII), with a bias clearly guided by Economic Freedom. Therefore, after a long process by several committees in the CN, the scenario in the second half of 2024 still differs from a consensus in the legislative house regarding the scope of the topic.

Thus, most of the discussions in the National Congress focus on finding a balance between the centrality of the human person, with the respective protection of their dignity and fundamental rights, and the continuation of technological and scientific development.

In this scenario of governing the structure of regulation for Artificial Intelligence, Mourão considers that:

In view of the challenges observed in the use of artificial intelligence, the main regulatory principles that should guide the drafting of laws on the subject stand out: a) general interest, ensuring inclusion and equity, since the public authorities cannot aim to satisfy private interests to the detriment of the public interest; b) human rights, since fundamental rights, such as individual freedoms, equality and diversity, must be respected, combating discriminatory practices.

19. GASPAR, Walter Britto; MENDONÇA, Yasmin Curzi de. Artificial Intelligence in Brazil still needs a strategy. *Getulio Vargas Foundation*, Rio de Janeiro, 2021. Available at: <<https://diretorio.fgv.br/sites/default/files/2022-08/ebia-pt-br.pdf>>. Accessed on: July 27, 2024.

used by artificial intelligence systems; c) transparency, in order to ensure understanding of how they work (regarding algorithms, data, tests and validations carried out, in addition to the list of areas that use such technologies).<sup>20</sup>

The importance of the general interest, human rights and transparency is therefore particularly important. However, we cannot lose sight of the need to ensure technological progress in order to develop increasingly suitable solutions. In other words, AI regulation should not be seen as a barrier to its progress; on the contrary, it should serve to ensure that its development occurs in accordance with justice and ethics, and this balance is called the high point of regulation.

## 2. Algorithmic discrimination and its effects

The use of artificial intelligence in everyday processes has advantages, such as optimizing time, parameterizing choices and facilitating various activities. There are even opinions in the scientific community that the reason for resorting to automated decision-making<sup>21</sup> would be linked to its neutrality, due to its objectivity and the use of mathematical criteria, which could, in theory, solve problems related to human decision-making, which is endowed with flaws and cognitive biases.<sup>22</sup>

However, as already explained, there are several difficulties observed in practice, depending on the form of use. In this context, it is noted that AI has several characteristics, including:

“i) opacity, which often means that not even developers know for sure the reasons why the algorithms reached their conclusions” and, furthermore, the “ii) quality of the data used to “run” the algorithms, which can bring with them implicit biases in the programming or acquire them later through network interaction, making automated decisions a fertile ground for discrimination, especially against more vulnerable groups” can be questioned.<sup>23</sup>

20. MOURÃO, Licurgo; INDUSTRIAL, Revolution. Regulation of artificial intelligence in Brazil. *Intellegentiae artificialis, imperium et civitatem*, p. 79, 2022. Available at: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Accessed on July 27, 2024.

21. Algorithmic or automated decision refers to decisions made by the algorithm without human intervention.

22. REQUIÃO, Maurício; COSTA, Diego. Algorithmic discrimination: affirmative actions as a combat strategy. *Civilistica.com*, v. 11, n. 3, p. 3, 2022. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Accessed on: July 24, 2024.

23. REQUIÃO, Maurício; COSTA, Diego. Algorithmic discrimination: affirmative actions as a combat strategy. *Civilistica.com*, v. 11, n. 3, p. 2, 2022. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Accessed on: July 24, 2024.

See Costa Requião's explanation in which he details the algorithm's discriminatory bias:

[...] AI and algorithmic processes are not only incapable of correcting subjective human error, but can also replicate and even reinforce existing prejudices in society, causing distinctions, preferences or exclusions capable of affecting equal treatment between individuals, especially vulnerable groups. This is what is called discriminatory bias of the algorithm or, simply, algorithmic discrimination.<sup>24</sup>

The author further explains that algorithmic discrimination can occur in two ways: “i) when algorithms reflect human prejudices (conscious or not) embedded in their programming; ii) when they come into contact with databases containing prejudicial biases, which causes the algorithm to “learn” to discriminate”.<sup>25</sup>

On this topic, Mendes and Matiuzzo make an interesting point:

[. . .] the term “algorithmic discrimination” is used in this article to encompass both scenarios involving statistically inconsistent statements and scenarios in which the statements, although statistically logical, somehow treat the individuals who are the object of them not as an effectively individualized form, but only as part of a group. This is because, in our view, a classification, even if consistent from a statistical point of view, may in some cases prove to be unfair.

<sup>26</sup>

In this article, the authors also highlight 4 (four) types of algorithmic discrimination, without excluding other types. They therefore support “discrimination by statistical error”, which refers to technical errors, that is, flaws in the algorithm code that can lead to incorrect data analysis, for example. They also point out “discrimination by generalization”, which occurs when the algorithm takes generalization as

24. REQUIÃO, Maurício; COSTA, Diego. Algorithmic discrimination: affirmative actions as a strategy to combat it. *Civilistica.com*, v. 11, n. 3, p. 4, 2022. Available at: <<https://civilistica.emnuvens.com.br/redc/article/view/804/650>>. Accessed on: July 24, 2024.

25. REQUIÃO, Maurício; COSTA, Diego. Algorithmic discrimination: affirmative actions as a combat strategy. *Civilistica.com*, v. 11, n. 3, p. 4, 2022. Available at: <<https://civilistica.emnuvens.com.br/redc/article/view/804/650>>. Accessed on: July 24, 2024.

26. MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithmic discrimination: concept, legal basis and typology. *Public Law*, v. 16, n. 90, p. 51, 2019. Available at: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>>. Accessed on: July 24, 2024.

absolute truth disregarding variations and exceptions, which in the context of probability is an error.<sup>27</sup>

The third type consists of “discrimination due to the use of sensitive information”, which refers to the use of data such as health or religion to make decisions, in the sense that it involves data that should not be used for certain purposes and is prohibited by Brazilian law. Finally, “discrimination that limits the exercise of rights”, which arises when the relationship between the information used and the right is so direct that it ends up restricting or impairing a person’s ability to exercise a certain right.<sup>28</sup>

From this understanding, it is clear that its occurrence weakens important fundamental rights, such as equality and isonomy, by restricting rights and benefits to individuals through generalizations. Furthermore, the use of these generalizations as a basis for decision-making processes “can have side effects, that is, discrimination against certain groups in society can be intensified”.<sup>29</sup>

Wimmer and Doneda consider, in this regard, that AI systems are, in themselves, predisposed to failure, especially because they make choices based on mechanisms that are neither precise nor neutral, which can result in unacceptable results, resulting, for example, from the internalization of cultural biases, racial and gender stigmas, in addition to harming individuals belonging to specific ethnic and social groups.<sup>30</sup>

It was noted, therefore, from the analysis of generalizations and data feeding that AI decisions express the *status quo* human, making predictions and perpetuating patterns of inequality, “worse, they are capable of reinforcing them even further: by deliberately ignoring the structural inequalities of the data they use, they end up exacerbating them”<sup>31</sup>.

Thus, it is clear that, for the digital system to function cohesively, there must be, at the very least, a large number of

27. MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithmic discrimination: concept, legal basis and typology. *Public Law*, v. 16, n. 90, p. 52-53, 2019. Available at: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>>. Accessed on: July 24, 2024.

28. MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithmic discrimination: concept, legal basis and typology. *Public Law*, v. 16, n. 90, p. 52-53, 2019. Available at: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>>. Accessed on: July 24, 2024.

29. MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithmic discrimination: concept, legal basis and typology. *Public Law*, v. 16, n. 90, p. 54, 2019. Available at: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>>. Accessed on: July 24, 2024.

30. WIMMER, Miriam and DONEDA, Danilo. “AI Failures” and Human Intervention in Automated Decisions: Parameters for Legitimation through Humanization, *Public Law Journal*, Brasília, Vol. 18, n. 100, p. 380, Oct./Dec. 2021.

31. BEZERRA, Arthur Coelho; COSTA, Camila Mattos. Black skin, white algorithms: information and racism in sociotechnical networks. *Liinc in Review*, Rio de Janeiro, v. 18, n. 2, p. 6, e6043, Nov. 2022.

data generation<sup>32</sup>(*data mining*), as they are the ones that feed and guide the functioning of applications and artificial intelligence solutions.

As for this dynamic, it should be said in passing, several protocols must be adopted, mainly due to the fact that much of the data routinely used by technology is sensitive and has more incisive protection.

### 3. The use of discriminatory algorithms in the context of criminal law

Given the discriminatory phenomenon in some algorithms, a brief analysis of the application of artificial intelligence in the then branch of Brazilian criminal law, also a perpetrator of segregation, is extremely relevant, as black, brown and people with low education are the majority of the prison population, according to the 2023 Criminal Information Report.<sup>33</sup>

As mentioned, this area of public law has several complexities linked to discrimination that results in social labeling and criminal selectivity.

Regarding social labeling, Howard S. Becker highlights that:

Because deviance is, among other things, a consequence of the reactions of others to a person's act, students of deviance cannot assume that they are dealing with a homogeneous category when they study people who have been labeled deviant. That is, they cannot assume that these people have actually committed a deviant act or broken some rule, because the labeling process may not be infallible; some people may be labeled deviant without having actually broken a rule. Furthermore, they cannot assume that the category of those labeled will contain all those who have actually broken a rule, because many offenders may escape detection and thus fail to be included in the population of "deviants" they study.<sup>34</sup>

32. Data mining refers to the process of exploring large data sets to discover meaningful patterns, trends, and relationships (Gropp, Motta, 2020).

33. SENAPEN – National Secretariat for Penal Policies. *National Criminal Information System*. 15th SISDEPEN Cycle. Period July to December 2023. Criminal Information Report. Brasília, 2024. Available at: <<https://www.gov.br/senappen/pt-br/servicos/sisdepen/relatorios>>. Accessed on: July 3, 2024.

34 BECKER, Howard. *Outsiders*. Translation by Maria Luiza X. de Borges; technical review by Karina Kuschnir. Rio de Janeiro: Zahar, 2008, p. 22.

According to this criminological approach, it is clear that, for a certain conduct to be considered a crime, it goes through a labeling process in which that action, carried out by a certain person, must be characterized as such. In this sense, in accordance with the cited excerpt, numerous people can carry out behaviors considered criminal, but not be considered deviant, as well as vice versa.

In other words, the identity of the individual matters much more than the conduct itself. Thus, in an intertwined way and as a logical consequence, penal selectivity emerges.

In the context of criminalization, referring to this process of selectivity, Vera Batista points out:

[...] it is much more accurate to call registered crime criminalization, because the operative selectivity of the penal system, qualitatively and quantitatively shaping the final result of secondary criminalization – that is, who and how many will be registered – makes it a procedure that configures social reality. We may or may not believe that the number of cars that exceeded the speed limit (criminality) is identical to the number of fines imposed for this reason by traffic authorities (criminalization); but it is only in this second number, in truth a human construct (dependent on factors as distinct as the moods of the police officer, the location of the surveillance camera, etc.) that we can study the incidence of transgressions.<sup>35</sup>

In this sense, it is emphasized, once again, that the labeling that exists in society is reflected in the prison population, as Luisa Silva explains:

Selectivity demonstrates the existence of a preferential profile of the public subjected to prison in Brazil. It consists of filtering between latent criminality and persecuted criminality, which occurs both in the context of primary and secondary criminalization. The reasons for this are issues such as social level, education, ethnicity, way of dressing, communicating and behaving, the last three of which reveal to which class the individual belongs in relation to the first two, among other cleavage mechanisms. It must also be considered that, since state control agencies do not have the necessary means to effectively process each and every typical fact that occurs, they

35. BATISTA, Vera Malaguti. *Critical introduction to Brazilian criminology*. 2nd edition. Rio de Janeiro: Revan, 2012, p. 22.

select the quality of attention given to those who come to their attention.<sup>36</sup>

It turns out that this phenomenon of selectivity is a problem, *per se*, carried out in the racist and classist context of modern society. It is aggravated, however, when automated decision-making systems, fed by data consistent with social reality, reproduce stigmas and prejudiced biases through generalizations and the reproduction of human prejudices.

Many of those who defend the use of AI in justice systems, especially in Criminal Law, argue that the automation of processes can bring benefits such as savings and procedural speed. However, such benefits end up occurring at the cost of sacrifices to human rights and human dignity, as Piló and Brasil explain.<sup>37</sup>

That said, Bichara, Cascardo Junior and Perazzoni explain that:

Using AI to analyze crime-related data carries the risk of exacerbating stereotypes and prejudices already present in society. Algorithms used to predict crimes or identify suspects tend to replicate existing biases in the data used, resulting in the continuation of racial and social inequalities.<sup>38</sup>

Thus, Santos, Torres and Celestino, when carrying out an analysis on the use of AI in criminal justice, found that the chances of incarcerating black people were greater than white people, which occurred due to the generalization carried out by the machine.<sup>39</sup>

The authors further explain when discussing the police security service:

In the criminal justice sector, there is an argument that since the predictions of machine learning-based algorithms depend on the quality of the training data, the public police security service of different regions may be affected at least

36. SILVA, Luisa Cypriano Moreira da. *Brazilian prison system: an analysis of the profile of prisoners based on theories of penal selectivity and social labeling*. 2019, p. 20. Federal University of Ouro Preto. Department of Law. Monograph. Available at: <[https://monografias.ufop.br/bitstream/35400000/2399/7/MONOGRRAFIA\\_SistemaCarcer%-c3%a1rioBrasileiro.pdf](https://monografias.ufop.br/bitstream/35400000/2399/7/MONOGRRAFIA_SistemaCarcer%-c3%a1rioBrasileiro.pdf)>. Accessed on: July 29, 2024.

37 PILÓ, Xenofontes Curvelo; BRASIL, Deilton Ribeiro. The use of artificial intelligence in criminal law and its impact on fundamental rights and guarantees. *EJEF Magazine*, n. 1, p. 294-295, 2022.

38 BICHARA, Anderson Andrade; CASCARDINO JR, Agostinho Gomes; PERAZZONI, Franco. Algorithmic racism, reinforcement of prejudices and use of AI: perspectives and challenges for digital criminal investigation. *IBCCRIM Bulletin*, v. 32, n. 379, p. 24, 2024.

39. SANTOS, Adriane de Almeida; TORRES, Marck de Souza; CELESTINO, Victor. Algorithmic discrimination and the intensification of structural racism: a scoping review. *Integrated Scientific Journal*, v. 7, n. 1, p. 5, e202415-e202415, 2024. Available at: <<https://revistas.unaerp.br/rci/article/view/3233/2422>>. Accessed on: July 24, 2024.

in two distinct ways: (1) communities with a history of a damaged relationship with the police may underreport criminal activity in their region and once this data is used in algorithmic decision-making systems, the system may decide that these regions have a level of crime and security that is not consistent with reality and not direct adequate police resources and assistance; (2) Algorithmic systems that are not trained based on data that incorporate racial stereotypes related to crime may indicate that regions with greater police pressure than regions with a higher population density of black people receive greater police pressure than regions with a predominantly white population. The combination of both algorithmic practices contributes to the concentration of security resources in privileged regions predominantly inhabited by white people while peripheral territories with a black majority receive police coercion, further demarcating racial disparities.<sup>40</sup>

In the case described, the potential for segregation that algorithmic decisions have is evident, as it can range from the articulation of the strategy for dealing with the problem to the action itself in the specific case.

It is important to consider, therefore, the risk of allowing AI to adopt a more punitive stance directed at specific groups to the detriment of others. In other words, what is also seen in Brazilian forensic practice can be aggravated in the context of an AI, which uses this type of metric to rationalize patterns through generalization.

In this context, there are already explicit cases of discriminatory algorithmization in AIs operated in Brazilian criminal law. This is the case, for example, of the facial recognition system, which is being widely used by police authorities to identify potential criminals. Although the use of this type of technology is proving to be problematic in countries such as the USA, where racist and segregationist bias has been proven, in addition to low accuracy in identifying people, Brazil imported this model to assist in the arrest of individuals wanted by the police.<sup>41</sup>

However, the same result is occurring in Brazil, according to the literature on the subject:

40 SANTOS, Adriane de Almeida; TORRES, Marck de Souza; CELESTINO, Victor. Algorithmic discrimination and the intensification of structural racism: a scoping review. *Integrated Scientific Journal*, v. 7, n. 1, p. 5, e202415-e202415, 2024. Available at: <<https://revistas.unaerp.br/rci/article/view/3233/2422>>. Accessed on: July 24, 2024.

41. CHAVES JUNIOR, Airto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Racial segregation and algorithmic lives: racist machines in the context of penal control. *Brazilian Journal of Law*, v. 2, p. 19, 2023. Available at: <<https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768>>. Accessed on: August 5, 2024.

[...] after about a year of use, statistics regarding the model's bias have already begun to appear. A survey carried out by the Security Observatory Network found that, of the 151 arrests made using the easy recognition system that took place in the country, 90% were of black people (Chaves Jr., Guasque, De Pádua, 2023, p. 20).

It is interesting to note that, on the international scene, there is a growing movement of cases that denounce algorithmic discrimination in the facial identification process, some of which are even proposing the banning of this type of technology. In turn, in Brazil, on the contrary, there is the promotion of the use of this type of tool by member states, with funding from the federal government, as a form of public security policy.<sup>42</sup>

Catiane Steffen explains that one of the means with the greatest potential for discrimination by algorithms that use AI is criminal law.<sup>43</sup> The author mentions the functionality of techniques that, in a first analysis, could, in theory, help authorities confirm the authorship and materiality of crimes, while optimizing the production of evidence. However, she explains that:

[...] at the same time as the State's preventive and punitive capacity increases, the possibility of violating citizens' rights over their personal data stored – with or without their consent – in State public security databases is opened up. Another of the many possibilities of violating rights is the creation of criminal profiles that conclude an individual's potential for harm based on physical, emotional and social characteristics, increasing the State's action on groups that are already stigmatized or discriminated against in a given society.<sup>44</sup>

Given all the setbacks demonstrated, Resolution No. 332 of the CNJ was an important milestone in the treatment of the matter discussed here, by regulating its use within the Judiciary. Mourão, in fact, clarifies the solution presented by the norm for cases in which the AI system may present discriminatory biases, saying that:

42. CHAVES JUNIOR, Airto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Racial segregation and algorithmic lives: racist machines in the context of penal control. *Brazilian Journal of Law*, v. 2, p. 20, 2023. Available at: <<https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768>>. Accessed on: August 5, 2024.

43. STEFFEN, Catiane. Artificial intelligence and criminal proceedings: the use of technology in the violation of rights. *EMERJ Magazine*, v. 25, n. 1, p. 112, 2023.

44 STEFFEN, Catiane. Artificial intelligence and criminal proceedings: the use of technology in the violation of rights. *EMERJ Magazine*, v. 25, n. 1, p. 113, 2023.

The Resolution requires that the development, implementation and use of artificial intelligence comply with fundamental rights and that the use of technologies must seek to guarantee legal certainty and equality. To this end, it provided that, before being implemented, the system must be approved in order to identify whether prejudices or generalizations influenced its development, leading to discriminatory tendencies in its operation. If the discriminatory bias cannot be remedied, the model cannot be used.<sup>45</sup>

In this case, the CNJ has already anticipated the need for approval and carrying out tests capable of measuring the discriminatory bias of an AI so that it can be permitted and then used within the scope of the Judiciary, covering decisions on criminal law.

The resolution in question dealt with the issue specifically in the criminal context in its article 23, as follows:

Art. 23. The use of Artificial Intelligence models in criminal matters should not be encouraged, especially with regard to the suggestion of predictive decision models.

§ 1 The provisions of the caput do not apply when it comes to the use of computational solutions intended for automation and the provision of subsidies for the calculation of penalties, prescription, verification of recidivism, mapping, classification and screening of records for the purposes of collection management.

§ 2 Artificial Intelligence models intended to verify criminal recidivism must not indicate a conclusion that is more prejudicial to the defendant than the one that the judge would reach without their use. (BRAZIL, 2020).

Chaves Júnior, Guasque, De Pádua attest that the lack of regulation on the matter poses risks to all spheres, especially to the indiscriminate use by criminal justice. For the authors:

This lack of regulation, accountability, auditing and transparency in the use of AI has been generating harmful consequences from a legal and social perspective, as it perpetuates and expands the discrimination and selectivity that permeates criminal control and the agencies that comprise it. And all under the illusory impression that it is based on impartial, precise and objective mathematical models.

45. MOURÃO, Licurgo; INDUSTRIAL, Revolution. Regulation of artificial intelligence in Brazil. *Intellegentiae artificialis, imperium et civitatem*, p. 81, 2022. Available at: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Accessed on July 27, 2024.

you. In truth, the results are loaded with subjectivity and racist biases that tend to catalyze well-defined social sectors for marginalization and discrimination.<sup>46</sup>

The specialized legal literature has also offered as a solution to the types of problems highlighted here, the limitation of the obtaining and processing of sensitive personal data, as well as drawing attention to the use of algorithm governance tools provided for in the LGPD, such as the auditing of machine decisions. However, such activity, by itself, is still not sufficient to solve the issue, given that “in a scenario of interaction with the *big data*, in which all data is potentially sensitive, only to ensure “algorithmic neutrality” and control a *posteriori* algorithm is not enough to mitigate the occurrence of discrimination”.<sup>47</sup>

Requião and Costa, in this scenario, highlight:

According to specialized doctrine, to solve the problem of opacity, it is necessary to strictly follow the principle of transparency, viewing it through the right to explanation of algorithmic decisions. Based on this principle, it is necessary to ensure that all steps of the algorithm can be explained in a way that a non-specialist individual can understand. In addition, algorithm creators must always maintain the ability to provide transparency regarding the entire algorithmic process involved and explanations for the decisions and results achieved.<sup>48</sup>

However, this solution alone is not sufficient, as the discussion is not restricted to the principle of non-discrimination, transparency and explanation, due to the high complexity and autonomy that AIs are endowed with.<sup>49</sup>

Thus, Wimer and Doneda consider the need for human participation in machine decision-making, especially given the fact that

46. CHAVES JUNIOR, Airto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Racial segregation and algorithmic lives: racist machines in the context of penal control. *Brazilian Journal of Law*, v. 2, p. 20, 2023. Available at: <<https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768>>. Accessed on: August 5, 2024.

47. REQUIÃO, Maurício; COSTA, Diego. Algorithmic discrimination: affirmative actions as a combat strategy. *Civilistica.com*, v. 11, n. 3, p. 2-3, 2022. Available at: <<https://civilistica.emnuvens.com.br/redc/article/view/804/650>>. Accessed on: July 24, 2024.

48. REQUIÃO, Maurício; COSTA, Diego. Algorithmic discrimination: affirmative actions as a combat strategy. *Civilistica.com*, v. 11, n. 3, p. 6, 2022. Available at: <<https://civilistica.emnuvens.com.br/redc/article/view/804/650>>. Accessed on: July 24, 2024.

49. REQUIÃO, Maurício; COSTA, Diego. Algorithmic discrimination: affirmative actions as a strategy to combat it. *Civilistica.com*, v. 11, n. 3, p. 6-7, 2022. Available at: <<https://civilistica.emnuvens.com.br/redc/article/view/804/650>>. Accessed on: July 24, 2024.

Many of the mistakes they make occur due to the lack of critical understanding of the situation being assessed.<sup>50</sup>

Therefore, the importance of human interference is evident, given the presence of discriminatory algorithms in AI tools. However, it cannot be ignored that the data entered into the systems are a reflection of society. Thus, with regard specifically to criminal law, the use of artificial intelligence has not yet been demonstrated to be cohesive until there is effective regulation, as it represents a systemic risk to human dignity.

## Final considerations

After analyzing the literature, including observing specific cases, it was concluded that there is an alarming risk in the use of artificial intelligence in everyday practice in criminal law, which is already, *per se*, endowed with selectivity, stigmas and prejudices.

In other words, the use of artificial intelligence in criminal law is extremely risky, due to the evidence regarding the discriminatory bias that technology can assume and the consequences of its generalization model. Such actions contribute to reinforcing social stigmas and perpetuating injustices related to the criminalization of black and low-income people.

In this sense, the use of AI in the criminal sphere is premature, both due to the discriminatory risks of the algorithm and the margins of error that the technology offers, as well as the disincentive to the use of automated systems in the criminal law sphere is understood to be correct by Resolution No. 332 of the CNJ, which highlights the sensitivity of the issue and the risks to people.

It was also clear that, if they are used, there is a need for human participation in decision-making phases, without there being any autonomous deliberations on the part of these technologies, especially when there is some impact on individual and collective fundamental rights. This interference is justified under the pretext of ensuring compliance with ethical limits.

Finally, after the study, the importance of an educational basis for training with themes such as structural racism, criminology, is demonstrated to be relevant.

50. WIMMER, Miriam and DONEDA, Danilo. "AI Failures" and Human Intervention in Automated Decisions: Parameters for Legitimation through Humanization, *Public Law Journal*, Brasília, Vol. 18, n. 100, p. 382, Oct./Dec. 2021.

among others, aimed at developers of artificial intelligence programs so that they can interrupt the racist reflex in society.

Thus, the technology can be developed taking into account ethics, human dignity and all other fundamental rights guaranteed by the Constitution. This would represent a preventive approach with a security protocol at the beginning of the development of the technologies and would avoid problems during use.

## References

BAPTISTA, Vera Malaguti. *Critical introduction to Brazilian criminology*. 2nd edition. Rio de Janeiro: Revan, 2012.

BECKER, Howard. *Outsiders*. Translation by Maria Luiza X. de Borges; technical review by Karina Kuschnir. Rio de Janeiro: Zahar, 2008.

BEZERRA, Arthur Coelho; COSTA, Camila Mattos. Black skin, white algorithms: information and racism in sociotechnical networks. *Liinc in Review*, Rio de Janeiro, v. 18, n. 2, e6043, Nov. 2022.

BICHARA, Anderson Andrade; CASCARDO JR, Agostinho Gomes; PERAZZONI, Franco. Algorithmic racism, reinforcement of prejudices and use of AI: perspectives and challenges for digital criminal investigation. *IBCCRIM Bulletin*, v. 32, no. 379, p. 23-26, 2024.

BRAZIL. Ministry of Science, Technology and Innovation. *Artificial intelligence*. Available at: <https://www.gov.br/mcti/pt-br/acomprae-o-mcti/transformacaodigital/inteligencia-artificial> . Accessed on: July 29, 2024.

\_\_\_\_\_. National Council of Justice. *Resolution No. 332, of August 21, 2020*. Available at: <https://atos.cnj.jus.br/atos/detalhar/3429> . Accessed on: July 29, 2024.

NATIONAL COUNCIL OF JUSTICE (CNJ). *Draft proposal for resolution 332*. Brasília: CNJ, 2024. Available at: <https://www.cnj.jus.br/wp-content/uploads/2024/09/minuta-proposta-resolucao-332-cnj-rev.pdf>. Accessed on: October 13, 2024.

\_\_\_\_\_. Presidency of the Republic. *Law No. 13,709, of August 14, 2018*. Provides for the protection of personal data and amends Law No. 12,965 of April 23, 2014 (Marco Civil da Internet). Brasília, DF: Presidency of the Republic, 2018. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm) . Accessed on: July 31, 2024.

\_\_\_\_\_. Federal Senate. *Bill No. 2338, of 2023*. Provides for the use of Artificial Intelligence. Brasília, DF: Senado Federal, 2023. Available at: <https://www25.senado.leg.br/web/activity/material/-/material/157233> . Accessed on: July 31, 2024.

CHAVES JUNIOR, Aírto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Racial segregation and algorithmic lives: racist machines in the context of penal control. *Brazilian Journal of Law*, v. 2, p. 4768, 2023. Available at: <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768> . Accessed on: August 5, 2024.

FIA – Administration Institute Foundation. *ChatGPT: what it is, how it works and how to use the tool*. Available at: <https://fia.com.br/blog/chat-gpt/> . Accessed on: July 25, 2024.

GASPAR, Walter Britto; MENDONÇA, Yasmin Curzi de. Artificial Intelligence in Brazil still needs a strategy. *Getulio Vargas Foundation*, Rio de Janeiro, 2021. Available at: <https://rightorio.fgv.br/sites/default/files/2022-08/ebia-pt-br.pdf> . Accessed on: July 27, 2024.

MOURÃO, Licurgo. Regulation of artificial intelligence in Brazil. *Intellegentiae artificialis, imperium et civitatem*, p. 73-89, 2022. Available at: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74> . Accessed on: July 27, 2024.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithmic discrimination: concept, legal basis and typology. *Public Law*, v. 16, n. 90, 2019. Available at: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766> . Accessed on: July 24, 2024.

MAIA FILHO, Mamede Said; JUNQUILHO, Tainá Aguiar. Victor Project: perspectives on the application of artificial intelligence to law. *Journal of Fundamental Rights and Guarantees*, v. 19, no. 3, p. 218- 237, 2018.

PARENTONI, Leonardo Netto; VALENTINI, Rômulo Soares; ALVES, Tárík César Oliveira E. Overview of the Regulation of Artificial Intelligence in Brazil: with emphasis on PL's No. 5,051/2019. *Electronic Journal of the Law Course at UFSM*, v. 15, n. 2, 2020.

PEIXOTO, Fabiano Hartmann. Victor Project: report on the development of artificial intelligence in the general repercussion of the Supreme Federal Court. *Brazilian Journal of Artificial Intelligence and Law-RBIAD*, v. 1, n. 1, p. 1-22, 2020. Available at: <https://www.rbiad.com.br/index.php/rbiad/article/view/4/4> . Accessed on: July 25, 2024.

PILÓ, Xenofontes Curvelo; BRASIL, Deilton Ribeiro. The use of artificial intelligence in criminal law and its impact on fundamental rights and guarantees. *EJEF Magazine*, n. 1, p. 269-299, 2022.

REQUIÃO, Maurício; COSTA, Diego. Algorithmic discrimination: affirmative actions as a combat strategy. *Civilistica.com*, v. 11, n. 3, p. 1-24, 2022. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/804/650> . Accessed on: July 24, 2024.

SANTOS, Adriane de Almeida; TORRES, Marck de Souza; CELESTINO, Victor. Algorithmic discrimination and the intensification of structural racism: a scoping review. *Integrated Scientific Journal*, v. 7, n. 1, p. e202415-e202415, 2024. Available at: <https://revistas.unaerp.br/rci/article/view/3233/2422> . Accessed on: July 24, 2024.

SENAPEN–National Secretariat for Penal Policies. *National Criminal Information System*. 15th SISDEPEN Cycle. Period July to December 2023. Criminal Information Report. Brasília, 2024. Available at: <https://www.gov.br/senappen/pt-br/servicos/sisdepen/relatorios> . Accessed on: July 3, 2024.

SILVA, Luisa Cypriano Moreira da. *Brazilian prison system: an analysis of the profile of prisoners based on theories of penal selectivity and social labeling*. 2019. Federal University of Ouro Preto. Department of Law. Monograph. Available at: [https://monografias.ufop.br/bitstream/35400000/2399/7/MONOGRRAFIA\\_SistemaCarcer%c3%a1rioBrasileiro.pdf](https://monografias.ufop.br/bitstream/35400000/2399/7/MONOGRRAFIA_SistemaCarcer%c3%a1rioBrasileiro.pdf) . Accessed on: July 29, 2024.

STEFFEN, Catiane. Artificial intelligence and criminal proceedings: the use of technology in the violation of rights. *EMERJ Magazine*, v. 25, no. 1, p. 105-129, 2023.

WEBSTER, Frank. *Theories of the information society*. London: Routledge, 1995.

WIMMER, Miriam and DONEDA, Danilo. "AI Failures" and Human Intervention in Automated Decisions: Parameters for Legitimation through Humanization, *Public Law Journal*, Brasilia, Vol. 18, n. 100, p. 374-406, Oct./Dec. 2021.

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

10

**Between Brain  
and Computer: Dialogues  
on Neurorights and  
Artificial intelligence**

Henry Segolin Molina

Summary: Introduction; 1. How neurotechnologies and AI are influencing the creation of new rights; 2. Paths and proposals for the implementation of Neurorights; 2.1. Analysis of laws and regulations around the world; 2.3. The Chilean Case: Girardi vs Emotiv Inc.; Final Considerations; Bibliographic References

## Introduction

The human brain is unlike any other organ, as it generates all of our mental and cognitive activities, to such an extent that we can consider it the most complex and powerful computer in the world.<sup>2</sup>

The search for new ways to understand and expand the limits of our mental capabilities has been the subject of research and development for some decades, and is at the epicenter of the field of Neuroscience and invasive technologies, allowing machines to interact directly with regions of the brain.

In 1924, Hans Berger performed the first electroencephalogram (EEG) on humans, a feat that represented a true revolution for its time. Using silver electrodes and a galvanometer, Berger was able to capture and record the first brain waves, now known as alpha and beta waves. This historic moment not only proved the feasibility of recording and analyzing the electrical activity of the human brain, but also launched a new and promising field of scientific research.

Later, the invention of cochlear implants in 1957 was a crucial point in the development of neurotechnologies with the aim of controlling electrical devices, such as lamps, using electrodes that can measure and react to brain signals, consisting of what we call today Brain-Computer Interfaces (BCIs).<sup>3</sup>

Normally, when we want to interact with an object in our environment, our nervous system goes through several neurological stages prior to sending nerve impulses, which, consequently, will allow a certain interaction to occur. BCIS, in turn, shorten this path

1. Postgraduate student in Digital Law and New Technologies at the Rio de Janeiro Institute of Technology and Society (ITS RIO), in partnership with the State University of Rio de Janeiro (UERJ). Graduated from the Pontifical Catholic University of São Paulo (PUC-SP). Lawyer.

2. MARR, B. *AI's next frontier: are brain-computer interfaces the future of communication?* Forbes Innovation, 2023. Available at: <https://www.forbes.com/sites/bernardmarr/2023/08/11/ais-next-frontier-are-brain-computer-interfaces-the-future-of-communication/>. Accessed on: June 10, 2024.

3. LOTTE, F. NAM, CS *Introduction: Evolution of Brain-Computer Interfaces*. Hal Open Science: Brain-Computer Interfaces Handbook: Technological and Theoretical Advance, Taylor & Francis (CRC Press), p.1-11, 2018. Available at: <https://inria.hal.science/hal-01656743/document>. Accessed on: June 10, 2024.

nho, since they use software and technologies that identify the intended action and execute it promptly and, for this reason, have potential applications in various fields.

On the subject, in mid-2017, Brazilian neuroscientist Miguel Nicolelis expressed an optimistic and provocative view about the potential of BCIs to transform not only medicine, but also the way we interact with the world around us:

**In the coming decades**, by combining this relativistic view of the brain with our growing technological ability to hear and decode increasingly complex neural symphonies, **neuroscience will eventually expand human capacity to almost unimaginable limits, which will begin to express itself far beyond the boundaries and limitations imposed by both our fragile primate bodies and our sense of self.**[...] Surprisingly **Future applications of BCIS promise to go far beyond the boundaries of medicine.**In a few generations, its technological development will enable our descendants to perform actions and experience sensations that few will be able to imagine a way to verbalize today. **BCISs can transform the way we interact with the tools we build to engage with the world around us, the way we communicate with each other, and how we interact with the distant environment.**and other worlds. To understand what this future might hold, you would first need to **imagine how dramatically our lives would change if some of our most routine tasks could be performed directly under the control of our brain's electrical activity, freely disseminated through the air in the same way that radio waves travel today**[...] The prospect of this wonderful freedom, which today may still sound to some like magic, miracle or alchemy, no longer belongs to the realm of science fiction.. **This world of the future is beginning to take shape, before our eyes, here and now..** (gn)<sup>4</sup>

At present, we can say that we are in the “second machine age”<sup>5</sup>, in which new discoveries occur simultaneously in the most diverse areas, in a complete fusion between the most advanced technology and the physical, digital, biological domains<sup>6</sup>and neuroscientists.

4. NICOLELIS, M. *Beyond our selves: the new neuroscience that unites brain and machines – and how it can change our lives*. 1st ed. 25-28 p.

5. MCAFEE, A. BRYNJOLFSSON, E. *The second machine age*. New York: Routledge, 2014.

6. SCHWAB, K. *The fourth industrial revolution*–New York: Routledge, 2016. 115 p.

It should be noted that, when mentioning that future applications of such tools could go beyond the frontiers of medicine, Nicoletti sensed that these technologies would open doors to experiences and actions that, at the time, would be difficult to conceive, but are now already capable, largely due to the integration of Artificial Intelligence (AI) in this field.<sup>7</sup>, due to the algorithmic ability to analyze large amounts of data and identify underlying patterns, thus improving the accuracy and efficiency of BCIs in interpreting neural data.<sup>8</sup>

This incorporation has enabled the growth of large-scale, high-quality data sets, contributing to the expansion of applications for brain-machine interfaces, which now, in addition to helping people with disabilities, also improve human capabilities by expanding our understanding of the complex functioning of the brain, as well as promoting the emergence of new markets.

One of the *players* best known in this scenario is the *Neuralink*, the subject of news around the globe, due to its advanced stage, considering that, on January 28, 2024, the company successfully performed its first brain implant, allowing a man named Noland Arbaugh, after living with paralysis for eight years, to regain the ability to perform tasks that, for him, were inaccessible<sup>9</sup>

Another company that is bringing products to market in this space is *NextMind*. In addition to creating tools that allow computers to be controlled with brain signals, the company hopes to create a device that can translate visual imagination into digital signals; that is, any image you imagine will be recreated on a computer screen – something similar to the image generation model used by AI applications including DALL-E and Midjourney.<sup>10</sup>

However, while there is great enthusiasm for advances in BCIs, as these technologies continue to mature, questions arise regarding their ethical and responsible development and use. These questions need to be addressed so that their application improves lives without causing unanticipated and potentially serious harm, including considering that

7. KUMAR, B. Integration of AI and Neuroscience for Advancing Brain-Machine Interfaces: A Study. *International Journal of New Media Studies (IJNMS)*, Volume 9 Issue 1, January-June, 2022. Available at: [https://www.researchgate.net/profile/BharathKumarNagaraj/publication/380785142\\_Integration\\_of\\_AI\\_and\\_Neuroscience\\_for\\_Advancing\\_Brain-Machine\\_Interfaces\\_A\\_Study/links/664e2edfbc86444c72f79492/Integration-of-AI-and-Neuroscience-for-Advancing-Brain-Machine-Interfaces-A-Study.pdf](https://www.researchgate.net/profile/BharathKumarNagaraj/publication/380785142_Integration_of_AI_and_Neuroscience_for_Advancing_Brain-Machine_Interfaces_A_Study/links/664e2edfbc86444c72f79492/Integration-of-AI-and-Neuroscience-for-Advancing-Brain-Machine-Interfaces-A-Study.pdf) . Accessed on: June 11, 2024.

8. KAWALASTE-STERNIUK, A. BROWASKA, N. Summary of over Fifty Years with Brain-Computer Interfaces-A Review. *Brain Sciences* 2021 Jan 3;11(1):43. doi: 10.3390/brainsci11010043. PMID: 33401571; PMCID: PMC7824107. Available at: <https://doi.org/10.3390/brainsci11010043> . Accessed on: June 11, 2024.

9. DREW, L. *Elon Musk's Neuralink brain chip: what scientists think of firsts human trial*. *Nature*, 2024. Available at: <https://www.nature.com/articles/d41586-024-00304-4> . Accessed on: June 11, 2024.

10. AR -SNAP AR. *Welcome Nextmind*. Available at: <https://ar.snap.com/welcome-nextmind> . Accessed on: June 11, 2024

Many of the threats associated with BCIs are already manifesting themselves in the way that neural data is exploited by technology companies on a daily basis.<sup>11</sup>

According to Adrian Carter, the use of Artificial Intelligence tools and algorithms, which interpret eye movements and detect changes in skin color and temperature, are already being used to read the results of brain activity and, from there, predict and influence behaviors, making certain companies profit billions from the use of this data.<sup>12</sup>

Furthermore, neural data from these activities is, by its very nature, extremely sensitive information, as it has the capacity to reveal very intimate elements about consumers.

In this regard, in a very recent study carried out by Jared Genser, Stephen Damianos, and Rafael Yuste, the authors pointed out that one of the most pressing concerns of these advances is the mining of neural data for commercial purposes, since, according to them, as consumers increasingly use neurotechnology devices, companies are building larger databases of brain images and other neural data, which, like genetic material and fingerprints, could lead to the immediate identification of individuals.

Advances in AI are rapidly increasing the ability to decode information, providing companies with unprecedented levels of insight into consumers' cognitive states and inner worlds, as well as helping to predict personality traits, addictions, mental health, and various disorders, according to the study.<sup>13</sup>

It is therefore not difficult to imagine how this data could be misused by corporations, which in turn poses complex challenges, particularly in terms of developing these tools and protecting privacy, user autonomy – especially where users have limited control over implanted brain-machine interfaces and the data they produce – and data and device security challenges.

Faced with such a scenario, foreseeing the growing capacity of Neuroscience and neurotechnology to access and influence human mental processes, Marcello Ienca and Roberto Andorno pointed out the need to determine

11. GENSER, J., DAMIANOS, S., YUSTE, R. *Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies*. Neurorights Foundation, 2024. Available at: [https://www.perseus-strategies.com/wp-content/uploads/2024/04/FINAL\\_Consumer\\_Neurotechnology\\_Report\\_Neurorights\\_Foundation\\_April-1.pdf](https://www.perseus-strategies.com/wp-content/uploads/2024/04/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf). Accessed on: 12. Jul. 2024.

12. WILD, K. 'Our notion of privacy will be useless': what happens if technology learns to read our minds? The Guardian, 2021. Available at: <https://www.theguardian.com/technology/2021/nov/07/our-notion-of-privacy-will-be-useless-what-happens-if-technology-learns-to-read-our-minds>. Accessed on: June 17, 2024.

13. GENSER, J., DAMIANOS, S., YUSTE, R. **Op cit**; 17-18 p.

what rights individuals should exercise in relation to their own mental dimension, in order to protect integrity, privacy and autonomy, as well as to ensure that people have control over their own thoughts, memories and decisions, as well as being protected against possible abuse or manipulation, arising from these advances. In particular, they advocated the creation of new human rights, which they called “Neurorights”<sup>14</sup>.

Thus, considering that brain-computer interfaces represent technological advances that, despite being potentially transformative in a positive way, already face non-technical obstacles that may limit their use – if there is no broad and sophisticated understanding of how to develop them – this article aims to analyze the ethical and regulatory challenges of advances arising from the intersection between BCIs and AI, focusing on:

**(i)** in the pressing need for consent; and **(ii)** in safeguarding the Neurorights of individuals, in the face of the processing of neural data.

To achieve this objective, among the traditional scientific methods, the methodology adopted will be the hypothetical-deductive one. In the legal field, in turn, the study will employ the hermeneutic, empirical and argumentative methods, in addition to adopting a critical-methodological approach. These dimensions will encompass descriptive research, with a reflective analysis of the academic and doctrinal production on the topics addressed, as well as a detailed analysis of the applicable regulations and proposals, if any.

## 1. How Neurotechnologies and AI are influencing the creation of new rights?

To begin, we can cite the report by the World Health Organization (WHO), according to which one in six people, approximately 16% of the global population, faces some type of significant disability.<sup>15</sup> In Brazil, the population with disabilities was estimated at 18.6 million people, and the survey data also shows that these individuals are less included in the job market and in schools – and, as a result, have more difficult access to income.<sup>16</sup>

14. IENCA, M.. ANDORNO, R.. *A new category of human rights: neurorights*. BMC, 2017. Available at: <https://blogs.biomed-central.com/bmcblog/2017/04/26/new-category-human-rights-neurorights/> . Accessed on July 15, 2024.

15. WHO -World Health Organization. *Global report on health equity for persons with disabilities*. Geneva: WHO, 2022. Available at: <https://www.who.int/publications/i/item/9789240063600> Accessed on July 31, 2024.

16. BRAZIL, Ministry of Human Rights and Citizenship. *Brazil has 18.6 million people with disabilities, according to research released by IBGE and MDHC*. Gov.br, 2023. Available at: <https://www.gov.br/mdh/pt-br/assuntos/noticias/2023/julho/brasil-tem-18-6-milhoes-de-pessoas-com-deficiencia-indica-pesquisa-divulgada-pelo-ibge-e-mdhc> . Accessed on July 31, 2024.

Although there are already several neurotechnology techniques applied in everyday life, such as electroencephalograms, functional magnetic resonance imaging, as well as techniques to stimulate the brain in order to mitigate symptoms of diseases such as Parkinson's or epilepsy, the most interesting and controversial innovations have emerged in their relationship with cognitive technologies.

The interaction between BCIs and data obtained on brain functions through machine learning (*machine learning*) and deep learning (*deep learning*), as well as natural language processing are used to generate what are called “artificial neural networks”, which are radically transforming AI applications.

With the help of a brain-computer interface, a person can control and operate external electronic devices with just their thoughts, communicate through synthesized speech, move prosthetic limbs, operate a computer, and perform other important functions that improve the quality of life for people with disabilities.<sup>17</sup>

In this context, as Rafael Yuste and Sara Goering rightly observe:

**Technological advances indicate that we are moving towards a world in which it will be possible to decode people's mental processes and directly manipulate the brain mechanisms underlying their intentions, emotions and decisions.**; where individuals could communicate with others simply by thinking; and where powerful computer systems linked directly to people's brains would aid their interactions with the world in such a way that their **mental and physical abilities would be greatly enhanced[...]**Such advances could revolutionize the treatment of many conditions, from brain injuries and paralysis to epilepsy and schizophrenia, **and transform the human experience for the better. But technology could also exacerbate social inequalities and give corporations, hackers, governments, or anyone else new ways to exploit and manipulate people.** And it could profoundly alter some fundamental human characteristics: private mental life, individual autonomy, and the understanding of individuals as entities limited by their bodies (gn)<sup>18</sup>

17. ZHANG, X. MA, Z. ZHENG, H. *et al.* The combination of brain-computer interfaces and artificial intelligence: applications and challenges. *Ann Transl Med.* 2020 Jun;8(11):712. doi: 10.21037/atm.2019.11.109. PMID: 32617332; PMCID: PMC7327323. Available at: <https://doi.org/10.21037/atm.2019.11.109> . Accessed on: June 18, 2024.

18. YUSTE, R. GOERING, S. *et al.* Four ethical priorities for neurotechnologies and AI. *Nature.* 2017. Available at: <https://www.nature.com/articles/551159a> . Accessed on: June 18, 2024.

The global BCI market, currently valued at approximately US\$1.2 billion, is showing impressive growth, with a projected compound annual growth rate of 13-15% through 2030.<sup>19</sup> However, the rapid expansion of this sector raises significant concerns regarding the privacy and security of neural data, since, on the one hand, it cannot be ruled out that our personal data is already processed on a large scale and that the agents mentioned above by the authors already draw up an individual profile of each person. On the other hand, the motivation to generate wealth enables the occurrence of various harmful effects on the social and mental aspects of the population, influencing them without them even being able to realize that they are being manipulated.

Given this scenario, the need arises to address what ethicists have called Neurorights, that is, the fundamental normative rules for the protection and preservation of the human brain and mind.<sup>20</sup>, taking into account that the absence of clear regulations can lead to abuses, exacerbating social inequalities and compromising the mental integrity of individuals.

It is therefore imperative that ways of regulating such rights are developed to ensure that the benefits of BCIs are enjoyed in an ethical and fair manner.<sup>21</sup>

## 2. Paths and proposals for the implementation of Neuro-rights

Having presented these aspects, since most existing privacy laws do not explicitly deal with neural data, nor with Neurorights, we then resort to a comparative analysis of legislation and other frameworks on the subject, in order to establish legal safeguards for the brain and for the processing of such data.

In this way, the following subchapter will serve to carry out a *overview* legislative efforts around the world, especially in the European Union, America,

19. GRAND VIEW RESEARCH. *Brain Computer Interface Market Size, Share & Trends Analysis Report By Application (Healthcare, Communication & Control), By Product (Invasive, Non-invasive), By End Use (Medical, Military), And Segment Forecasts, 2023 – 2030*. Report ID: 978-1-68038-459-8 Available at: <https://www.grandviewresearch.com/industry-analysis/brain-computer-interfaces-market> . Accessed on June 19, 2024.

20. IENCA, M. ANDORNO, R. *A new category of human rights: neurorights*. BMC, 2017. Available at: <https://blogs.biomed-central.com/bmcblog/2017/04/26/new-category-human-rights-neurorights/> . Accessed on: 20 Jun. 2024.

21. RODRÍGUEZ, J. Artificial intelligence and neuroderechos. Straights and perspectives. *Constitutional Questions*, Revista Mexicana de Derecho Constitucional, Núm. 46, Enero-Junio 2022 ISSN (electronic version): 2448-4881. Available at: <https://www.scielo.org.mx/pdf/cconst/n46/1405-9193-cconst-46-93.pdf> . Accessed on: July 26, 2024.

rich Latin America and the United States, in order to recognize common tendencies regarding the challenges of protecting mental privacy in the age of neurotechnology.

## 2.1 Analysis of laws and regulations around the world

Most of the time, when discussing innovation, data protection and new technologies, the European Union (EU) is seen as a precursor in global standardization, standing out in a scenario lacking regulation and full of potential and irreparable losses, due to the speed of technological development.

This stance by the EU is nothing new. By positioning itself as a global reference, this economic group aims to encourage other nations to broaden the debate, accelerate their legislative proposals and guidelines related to BCI and artificial AI systems, and plan technological development in an ethical manner, in order to gain space in debates around the world.

For illustrative purposes, we can recall the precursor regulations on personal data, firstly, with Directive 95/46 and, subsequently, with *General Data Protection Regulation* (GDPR), which even served as the basis for the creation of the General Data Protection Law (LGPD) in Brazil and, more recently, the *AI Act*, the new European legislation for AI regulation.

In the discussion on BCIs, Neurorights and neural data, in turn, the EU appears only as an academic precursor, since the debates are still under the purview of the European Neuroethics Network, which brings together a wide range of actors, including renowned researchers such as Rafael Yuste, Adrian Owen, and Emmanuelle Charpentier.

A significant milestone in this context was the *Human Brain Project* (HBP), an ambitious project launched in 2013 with the aim of deepening the understanding of the human brain and boosting the development of neurotechnologies. Active for 10 years, the project has generated more than 3,000 academic publications, developed more than 160 digital tools, medical and technological applications, and created the open research infrastructure *EBRAINS*. It has also driven significant advances in brain research and the development of medical technologies, such as personalized brain medicine and new brain-inspired technologies, including AI tools and neuromorphic computing.<sup>22</sup>

22. HBP - HUMAN BRAIN PROJECT. *The Human Brain Project ends: What has been achieved*. Human Brain Project, Press release, 2023. Available at: <https://www.humanbrainproject.eu/en/follow-hbp/news/2023/09/28/human-brain-project-ends-what-has-been-achieved/>. Accessed on: 22 Jul. 2024.

Another highlight in Europe is the Council of Europe's "Strategic Action Plan", which focuses on human rights and new biomedical technologies, including recent changes in neurotechnology.

Contrary to the rule, in terms of incorporating these concepts into legal regulations, the highlight is Latin America, in particular, due to the fact that Chile has become a reference on the subject, being the first country in the world to incorporate them into its Constitution, by approving a constitutional amendment, through Law 21,383.<sup>23</sup>, which modified Article 19 to protect brain activity and associated information, and emphasizing the need to balance physical and mental integrity with advances in neurotechnology.

Another crucial arc in the Latin American scenario<sup>24</sup> was the approval of the Inter-American Declaration of Principles on Neuroscience, Neurotechnology and Human Rights<sup>25</sup>, by the Organization of American States (OAS), in mid-2023, demonstrating a regional commitment to the protection of individual rights, in the face of advances in brain science.

Following these examples, other countries such as Costa Rica, Colombia, Argentina, Uruguay, Peru, Mexico and Brazil are also moving towards regulating neurotechnologies and providing safeguards for brain integrity and neural data, with the latter being at a more advanced regulatory stage, considering that, up to the date on which these considerations are made, two bills related to "neuroprivacy" were under consideration in Mexico, and several proposals in Brazil. See the table below:

23. STRICKLAND, E. *Worldwide campaign for neurorights notches its first win*. IEE Spectrum, 2021. Available at: <https://spectrum.ieee.org/neurotech-neurorights> . Accessed on: 22 Jul 2024

24. DO, B. SPIVACK, J. BADILO, M. *Privacy and the rise of "neurorights" in Latin America*. Future of Privacy Forum, 2024. Available at: <https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/> . Accessed on: July 23, 2024.

25 OAS - ORGANIZATION OF AMERICAN STATES. *Inter-American Declaration of Principles on Neuroscience, Neurotechnology and Human Rights*. Available at: [https://www.oas.org/es/sla/cji/temas\\_culminados\\_reciente\\_Neurociencias\\_Neurotecnologias\\_y\\_Derechos\\_Humanos.asp](https://www.oas.org/es/sla/cji/temas_culminados_reciente_Neurociencias_Neurotecnologias_y_Derechos_Humanos.asp) . Accessed on: July 23, 2024.

**Table 01 – Regulation of Neurorights in Latin America**

Country	Proposal/ regulation	Main points	Current status	Sources
<b>Chile</b>	Law 21383	It amends the Constitution to establish guidelines for scientific and technological development, at the service of people, defending the physical and psychological integrity of individuals, in addition to requiring consent for the use of these tools.	In Force	<a href="#">Library of the Congress National from Chile</a>
<b>Mexico</b>	Proposal by Deputy Maria Eugenia Hernandez Perez	It has the same wording as the Chilean constitutional amendment.	Under discussion	<a href="#">System of Information-Legislative Assembly</a>
	Proposal by Senator Alejandra Lagunes Soto Ruiz	Amend Article 73 of the Constitution to regulate, in a unified manner, artificial intelligence, cybersecurity and Neurorights	Under Discussion	<a href="#">Senate of the Republic-here</a>
<b>Uruguay</b>	Initiatives legislative based on dialogue with experts and parliamentarians Chileans	Regular Neurorights	In phase preliminary of discussion	<a href="#">UNESCO</a>
<b>Argentina</b>	Bill 2446/23	Create a specific committee to develop new regulations on Neurorights	Under discussion	<a href="#">Senate of the nation Argentina</a>
<b>Costa Rica</b>	Proposal of amendment to the law of protection of data	Categorize neural data as biometric data	Under discussion	<a href="#">UNESCO</a>
<b>Colombia</b>	Proposal of amendment to the law of protection of data	Create a specific section, with the aim of establishing the guiding principles for the processing of this data, through AI and neurotechnologies	Under discussion.	<a href="#">UNESCO</a>

(continues)

Table 01 – Regulation of Neurorights in Latin America

(continuation)

Country	Proposal/ regulation	Main points	Current status	Sources
Peru	Project of Law No. 5968/2023-CR (Carlos Javier Zeballos Madariaga)	It aims to protect people's fundamental rights by regulating the use of neuroscientific evidence in legal proceedings.	Under analysis in the Commission of Justice and Rights Humans of the Congress of the Peru since September 2023	<u>Congress Peruvian</u>
Brazil	PEC 298 of 2023 (Rio Grande do South)	Amend the State Constitution, with the aim of including Neurorights, elevating mental integrity to the status of a constitutional principle.	In force at Rio Grande do South.	<u>Assembly Legislative-go to Rio Big of the South</u>
	PEC No. 29/2023 (Senator Randolph Rodrigues)	Inclusion of regulations aimed at protecting mental integrity and algorithmic transparency, under the pretext that mental integrity is closely linked to human dignity in this new social context.	Stop at Senate, waiting rapporteur.	<u>Senate Federal</u>
	Bill 2174/2023 (Rubens Pereira-Junior)	It establishes the rules and principles for the protection of fundamental rights related to the brain and the human nervous system, aiming to guarantee the protection and promotion of individuals' neurorights.	Waiting Designation of Rapporteur in the Commission of Constitution and Justice and of Citizenship (CCJC)	<u>Chamber of the Deputies-states</u>
	Bill 1229/2021 (Carlos Henri that Gaguim)	Modifies Law No. 13,709 of August 14, 2018 (General Law on the Protection of Personal Data), in order to conceptualize neural data and regulate its protection.	Removed by Author	<u>Chamber of the Deputies-states</u>

(continues)

## Table 01 – Regulation of Neurorights in Latin America

(continuation)

Country	Proposal/ regulation	Main points	Current status	Sources
Brazil	Bill 522/2022 (Carlos Henri- that Gaguim)	Amendment to the Brazilian General Data Protection Law (LGPD) to recognize neural data as a type of sensitive personal data.	Approved in CHEALTH, in October 2023 and had the Dep. Adriana Ventura (NEW-SP) designated as rapporteur on April 10th of 2024	<u>Chamber of the Deputies- states</u>
	Preliminary draft of update of Civil Code (2024)	Insertion of Neurorights in the Civil Code.	Presented to the Senate, under analysis.	<u>Senate Federal</u>

**Source:** prepared by the author, based on various sources from official government channels, 2024.

Finally, in the United States, efforts to address Neurorights are led by academic organizations, professionals, and government advisory bodies. The contributions of scholars such as Martha J. Farah and Hank Greely stand out, whose work has been fundamental in the discussion of this topic.

In April, the state of Colorado passed promising legislation designed to protect consumers from devices that collect brain activity data, promoting the defense of mental integrity and the protection of neural data. On the topic, state representative Cathy Kipp, a Colorado Democrat, stressed that while the technology has potential benefits, “there should be safeguards for those who do not wish to have their thoughts read and their biological data used.”<sup>26</sup>

Also, recently, California amended its Consumer Privacy Act (CCPA) to include neural data as sensitive information, seeking to protect data generated by brain activity from potential

26. MOENS, J. *Your Brain Waves Are Up for Sale. A New Law Wants to Change That.* New York Times, 2024. Available at: <https://www.nytimes.com/2024/04/17/science/colorado-brain-data-privacy.html>. Accessed on: June 24, 2024.

misuse, allowing users to control, delete or limit this data<sup>27</sup>.

Given the above, it is clear that, in general, several countries are seeking ways to address Neurorights and the management of neural data, not with the aim of prohibiting new technologies, but rather regulating them in a way that protects the rights of individuals. Therefore, what these measures aim to ensure is precisely to promote an environment in which advances in Neuroscience and neurotechnology respect people's cognitive autonomy, privacy and dignity.

## 2.2 The Chilean case: Girardi vs Emotiv Inc.

As seen, to date, Chile is the only country in the world to include Neurorights in its legal system, even granting them the status of a fundamental right, in a clear recognition of the importance of providing a framework to face the ethical and legal challenges emerging from neurotechnology, with the aim of shaping an environment in which innovation can thrive without compromising the rights to cognitive freedom, mental privacy, mental integrity and psychological continuity of individuals.

Thus, it was expected that the first legal dispute on this issue would also take place in the country. And that is precisely what happened, in August 2023. At the time, the Third Chamber of the Supreme Court of Chile was faced with an emblematic case, the details of which and the reasons for the decision would represent a milestone, far beyond its borders.<sup>28</sup>

In the case in question, Mr. Guido Girardi Lavín filed a constitutional protection action against Emotiv Inc., a bioinformatics company based in San Francisco, United States, which develops and manufactures portable electroencephalography products, along with neuro-headphones, software development kits, software, mobile applications and data products.

In the initial, the author claimed to have acquired a device called '*Insight*'- which works like a headband with sensors that capture information about the brain's electrical activity, obtaining data about the user's gestures, movements, preferences, reaction times and cognitive activity – and that as a result, he would have accepted the software's terms of service, which require

27. CANTER, L. BRIM, E. *California Enacts Health AI Bill and Protections for Neural Data*. Covington, 2024. Available at: <https://www.insideprivacy.com/uncategorized/california-enacts-health-ai-bill-and-protections-for-neural-data/> . Accessed on: October 16, 2024.

28. CORNEJO-PLAZA, MI CIPPITANI, R. PASQUINO, V. *Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata*. *Frontiers in Psychology*, 2024. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10929545/> . Accessed on: July 25, 2024.

saw the company storing their neural data, in an anonymized form, for scientific research purposes.

However, to the author's surprise, Emotiv began to use his data for different purposes and, due to this improper treatment, he claims to have been exposed to different risks, pointing out violations of the provisions of article 11 of Law No. 19,628, regarding due diligence in the care of personal data to which those responsible for personal records or databases are obliged, and the provisions of article 13 of the same law, regarding the right of individuals to cancel or block their personal data, since, even with the user account closed, the company retained his brain information for scientific and historical research purposes.

In its defense, Emotiv claimed that its product consists of a non-invasive neurotechnology device, without therapeutic purposes, of the mobile electroencephalogram type, designed for self-quantification and field research, and is not sold as a medical device; in addition, it pointed out that the product and its installation contain a detailed explanation of the terms and conditions, in which express consent is requested for the processing of personal and brain data, which would have been granted by the author.

In the judgment, the Court upheld the sentence that ruled in favor of the author, adding to it only to order the Public Health Institute and the customs authority to ensure that the marketing and use of data from the Insight device are in compliance with current regulations, as well as confirming the request for deletion of any stored data related to the use of the device by the author.

In its reasoning, the Court emphasized the need for informed consent for the use of information in research, as required by Law No. 20,120, and referred in particular to Article 19 of the Constitution of the Republic, which constitutes a direct mandate for the protection of Neurorights, in addition to citing international agreements such as the International Covenant on Economic, Social and Cultural Rights (Article 15) and UNESCO declarations, emphasizing the search for a balance between scientific progress and its application to human rights. In summary, the Court consolidated the understanding that:

**In view of the development of new technologies that increasingly involve aspects of the human person – aspects that, a few years ago, would have been unthinkable to know –, special attention and care must be given to their review by the State, with the aim of preventing and anticipating possible effects, in addition to directly protecting human integrity in its entirety, including its**

**privacy and confidentiality, as well as the rights inherent to psychic integrity and the subject of scientific experimentation [...]** That way (...) **It is absolutely necessary that, before allowing its commercialization and use in the country, this technology and its devices are analyzed by the competent authority, considering that it presents problems that have not been studied until now. [...]**the conduct reported in the records, in the circumstances noted, **violates the constitutional guarantees contained in items 1 and 4 of article 19 of the Political Constitution of the Republic, which refer to physical and mental integrity and the right to privacy**[...] For these reasons, and given that the device does not have a Customs Destination Certificate, this action will be accepted as indicated in the operative part of this judgment, so that the health and customs authority can fully study the Insight device in light of the regulations mentioned in this judgment. (gn)<sup>29</sup>

In addition to being paradigmatic, this case established fundamental parameters that should guide future analyses on the subject. Among the highlighted aspects, the following can be mentioned: **(i)** the recognition that neural data also constitutes personal data and is therefore protected by data protection legislation. This consideration, although it may seem basic, is crucial, as it demonstrates that data protection emerges as the main legal basis in the analysis of neurotechnologies; **(ii)** the clear connection between data protection legislation and the fundamental rights to mental integrity and privacy, showing that the lack of consent for the specific processing of brain information simultaneously constitutes a legal and constitutional violation; and **(iii)** the debate on the need for express consent, highlighting the importance of framing the treatment on an adequate legal basis, under penalty of incurring illegality.

In this sense, it is understood that the Chilean judges decided correctly, since they weighed up the benefits associated with the development of neurotechnologies and sought a balanced, non-radical solution, which could culminate in the prohibition of Emotiv Inc.'s activities in the country and, consequently, discourage other companies operating in this market.

29. CHILE. Jurisprudential Basis of the Judicial Power. *GIRARDI/EMOTIV INC: 09-08-2023 (CIVIL) APELACIÓN PROTECCIÓN*, Roll No. 105065-2023. In the Supreme Court Jurisprudence Search Engine. Available at: [https://juris.pjud.cl/busqueda/pagina\\_detalle\\_sentencia?k=L2FadjlzYUdmbGx1UWNKWmV6ZjZ3dz09](https://juris.pjud.cl/busqueda/pagina_detalle_sentencia?k=L2FadjlzYUdmbGx1UWNKWmV6ZjZ3dz09). Accessed on: July 30, 2024.

In short, this approach not only highlights the importance and effectiveness of Neurorights, given the challenges arising from these new technologies, but also reveals the possibility of defining a communicative path, in which innovation can be improved, in an ethical and responsible manner.

## Final considerations

This article focuses, in summary, on the analysis of how neurotechnologies and Artificial Intelligence are shaping the creation of new rights, exploring the paths currently proposed to promote an ethical and responsible development of these innovations, with the aim of protecting the so-called Neurorights, in view of the risks associated with the processing of neural data.

The initial chapters present a brief historical retrospective of brain-computer interfaces (BCIs), highlighting their benefits and the evolution driven by integration with AI tools. Some practical applications of BCIs are examined, highlighting their transformative potential and positive impact, especially for people with disabilities. In addition, the challenges and concerns that these advances may bring to society in the short term are discussed, considering the sensitivity and harmful potential of processing neural data, and highlighting the importance of studying Neurorights.

The subsequent chapter was divided into two parts. The first analyzes the proposals and regulations that exist around the world, seeking to identify points of convergence and highlighting how the diversity of proposals and the lack of a uniform consensus demonstrate the growing interest and need for a regulatory framework to guarantee the protection of Neurorights. The second offers a detailed analysis of the *Girardi vs. Emotiv Inc.* case, bringing important considerations about the potential for the application of these rights in practical scenarios, their effectiveness and the approach to Neurorights in the judicial sphere.

Finally, although the debate on the topic is far from being concluded, the objective of this article is to stimulate a deeper and more incisive reflection on the issues presented therein, aiming to promote greater effectiveness in the protection of Neurorights.

Given the complexity of the technologies involved and the speed with which they develop, building a robust and adaptable legal framework that balances innovation with the protection of data subjects is a challenge that requires a collaborative approach between legislators, scientists and civil society.

In conclusion, the study of Neurorights must therefore be continuous and dynamic, seeking to ensure that innovations, however disruptive they may be, respect the dignity and autonomy of individuals, so that we can advance safely in the increasingly uncertain terrain of BCIs and AI, in order to take advantage of their benefits and avoid abuse, protecting individuals against the risks inherent in the processing of neural data.

## Bibliographic References

ARMSTRONG, W. MICHAEL, K. The Implications of Neuralink and Brain Machine *Interface Technologies*. *IEEE International Symposium on Technology and Society (ISTAS)*, Tempe, AZ, USA, 2020, pp. 201-203. Available at: <https://ieeexplore.ieee.org/abstract/document/9462223> . Accessed on: April 20, 2024.

AR-SNAP AR. Welcome Nextmind. Available at: <https://ar.snap.com/welcome-nextmind> . Accessed on: June 11, 2024.

BOSELLI, G. *Neurorights: the urgency of legal protection for neurotechnologies*. Legal Consultant, 2024. Available at: <https://www.conjur.com.br/2024-fev-06/neurodireitos-a-urgencia-de-legal-protection-of-neurotechnologies/> . Accessed on: June 10, 2024.

BRAZIL. *Law no. 13,709, of August 14, 2018*. General Law on the Protection of Personal Data (LGPD). Brasília: Presidency of the Republic, 2018. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm) . Accessed on: June 7, 2024.

BRAZIL, Ministry of Human Rights and Citizenship. *Brazil has 18.6 million people with disabilities, according to research released by IBGE and MDHC*. Gov.br, 2023. Available at: <https://www.gov.br/mdh/pt-br/assuntos/noticias/2023/julho/brasil-tem-18-6-milhoes-de-pessoas-com-deficiencia-indicates-research-released-by-ibge-and-mdhc> . Accessed on July 31, 2024.

CANTARINI, P. *The new frontier of behavioral manipulation and the role of compliance in mitigating risks in AI*. *USP Journal*, 2024. Available at: <https://jornal.usp.br/artigos/a-nova-frontier-of-behavioral-manipulation-and-the-role-of-compliance-in-risk-mitigation-in-ia/> . Accessed on: July 30, 2024.

CANTER, L. BRIM, E. California Enacts Health AI Bill and Protections for Neural Data. Covington, 2024. Available at: <https://www.insideprivacy.com/uncategorized/california-enacts-health-ai-bill-and-protections-for-neural-data/> . Accessed on: October 16, 2024.

CHILE. Jurisprudential Basis of the Judicial Power. GIRARDI/EMOTIV INC: 09-08-2023 (CIVIL APELACIÓN PROTECCIÓN), Roll No. 105065-2023. In Jurisprudential Searcher of the Supreme Court. Available at: [https://juris.pjud.cl/busqueda/pagina\\_detalle\\_sentencia?k=L2FadjlzYUdmb-Gx1UWNKWmV6ZjZ3dz09](https://juris.pjud.cl/busqueda/pagina_detalle_sentencia?k=L2FadjlzYUdmb-Gx1UWNKWmV6ZjZ3dz09) . Accessed on: July 30, 2024.

CORNEJO-PLAZA, MI CIPPITANI, R. PASQUINO, V. Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata. *Frontiers in Psychology*, 2024. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10929545/> . Accessed on: July 25, 2024.

DREW, L. Elon Musk's Neuralink brain chip: what scientists think of first human trials. *Nature*, 2024. Available at:<https://www.nature.com/articles/d41586-024-00304-4> . Accessed on: June 11, 2024.

DO, B. SPIVACK, J. BADILO, M. Privacy and the rise of “neurorights” in Latin America. *Future of Privacy Forum*, 2024. Available at:<https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/> . Accessed on: July 23, 2024.

FIANI, Brian. Reardon, Taylor *et al.* *An Examination of Prospective Uses and Future Directions of Neuralink: The Brain-Machine Interface*. Cureus, 2021. Available at:<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8083990/#> . Accessed on: June 14, 2024.

FLORES FILHO, E. FIRMO, M. Human dignity and neurorights in the digital age. *Journal of the Institute of Constitutional Law and Citizenship-IDCC*, Londrina, v. 7, n. 2, e063,, 2022. Available at: <file:///C:/Users/hsmol/Downloads/157-Texto%20do%20Artigo-386-2-10-20230523.pdf> . Accessed on: July 15, 2024.

GAGUIM, C. *Bill No. 522, of 2022*. Chamber of Deputies, 2022. Available at:<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317524> . Accessed on: July 29, 2024.

GENSER, J. DAMIANOS, S. YUSTE, R. Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies. *Neurorights Foundation*, 2024. Available at:[https://www.perseus-strategies.com/wp-content/uploads/2024/04/FINAL\\_Consumer\\_Neurotechnology\\_Report\\_Neurorights\\_Foundation\\_April-1.pdf](https://www.perseus-strategies.com/wp-content/uploads/2024/04/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf) . Accessed on: 12. Jul. 2024.

GRAND VIEW RESEARCH. *Brain Computer Interface Market Size, Share & Trends Analysis Report By Application (Healthcare, Communication & Control), By Product (Invasive, Non-invasive), By End Use (Medical, Military), And Segment Forecasts, 2023 – 2030*. Report ID: 978-1-68038-459-8 Available at:<https://www.grandviewresearch.com/industry-analysis/brain-computer-interfaces-market> ; Accessed on June 19, 2024.

HALLINAN, D. *et al* *Neurodata and Neuroprivacy: Data Protection Outdated?* *Surveillance & Society*, 2014. Available at:<https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/neurodata> . Accessed on: July 12, 2024.

HIGGINS, N. *Neuralink implants chip in human brain: what can go wrong*. *Galileo*, 2024. Available at:<https://revistagalileu.globo.com/tecnologia/noticia/2024/02/neuralink-implanta-chip-in-human-brain-what-can-go-wrong.ghtml> . Accessed on: 02. Jun. 2024.

HBP–HUMAN BRAIN PROJECT. *The Human Brain Project ends: What has been achieved*. *Human Brain Project*, Press release, 2023. Available at:<https://www.humanbrainproject.eu/en/follow-hbp/news/2023/09/28/human-brain-project-ends-what-has-been-achieved/> . Accessed on: 22 Jul. 2024.

IENCA, M.. ANDORNO, R.. *A new category of human rights: neurorights*. *BMC*, 2017. Available at: <https://blogs.biomedcentral.com/bmcblog/2017/04/26/new-category-human-rights-neurorights/> . Accessed on July 15, 2024.

ANDORNO, R. *Towards new human rights in the age of neuroscience and neurotechnology*. *Life Sciences, Society and Policy*, 2017. Available at:<https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1> . Accessed on: July 1, 2024.

KAWALASTE-STERNIUK, A. BROWASKA, N. Summary of over Fifty Years with Brain-Computer Interfaces-A Review. *Brain Sciences* 2021 Jan 3;11(1):43. doi: 10.3390/brainsci11010043. PMID: 33401571; PMCID: PMC7824107. Available at:<https://doi.org/10.3390/brainsci11010043> . Accessed: June 11, 2024.

KUMAR, B. Integration of AI and Neuroscience for Advancing Brain-Machine Interfaces: A Study. *International Journal of New Media Studies (IJNMS)*, Volume 9 Issue 1, January-June, 2022. Available at:[https://www.researchgate.net/profile/BharathKumarNagaraj/publication/380785142\\_Integration\\_of\\_AI\\_and\\_Neuroscience\\_for\\_Advancing\\_Brain-Machine\\_Interfaces\\_A\\_Study/links/664e2edfbc86444c72f79492/Integration-of-AI-and-Neuroscience-for-Advancing-Brain-Machine-Interfaces-A-Study.pdf](https://www.researchgate.net/profile/BharathKumarNagaraj/publication/380785142_Integration_of_AI_and_Neuroscience_for_Advancing_Brain-Machine_Interfaces_A_Study/links/664e2edfbc86444c72f79492/Integration-of-AI-and-Neuroscience-for-Advancing-Brain-Machine-Interfaces-A-Study.pdf) . Accessed on: June 11, 2024.

LOTTE, F. NAM, CS Introduction: Evolution of Brain-Computer Interfaces. *Hal Open Science: Brain-Computer Interfaces Handbook: Technological and Theoretical Advance*, Taylor & Francis (CRC Press), pp.1-11, 2018, 9781498773430. fhal-01656743f. Available at:<https://inria.hal.science/hal-01656743/document> . Accessed on: June 10, 2024.

MARDEN, C. MARTINS, G. *Law and neuroscience: beyond first impressions*. Curitiba: Juruá, 2020.

MARR, B. AI's next frontier: are brain-computer interfaces the future of communication? *Forbes Innovation*, 2023. Available at:<https://www.forbes.com/sites/bernardmarr/2023/08/11/ai-next-frontier-are-brain-computer-interfaces-the-future-of-communication/> . Accessed on: June 10, 2024.

MAYNARD, A. SCRAGG, M. *The Ethical and Responsible Development and Application of Advanced Brain Machine Interfaces*. *J Med Internet Res*, 2019. Available at:<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7351257/> Accessed on: July 10, 2024.

MCAFEE, A. BRYNJOLFSSON, E. *The Second Machine Age*. Rio de Janeiro: Alta Books, 2014.

METHA, D. *How Elon Musk's Neuralink brain implant 'expands the boundaries of the mind'*. *BBC News Brazil*, 2024. Available at:<https://www.bbc.com/portuguese/articles/cp0qyj3lv01o> . Accessed on: July 23, 2024.

MUSK, E. Neuralink. An Integrated Brain-Machine Interface Platform With Thousands of Channels. *J Med Internet Res* 2019;21(10):e16194. Available at:<https://www.jmir.org/2019/10/e16194> . Accessed on: July 20, 2024.

MOENS, J. Your Brain Waves Are Up for Sale. A New Law Wants to Change That. *New York Times*, 2024. Available at:<https://www.nytimes.com/2024/04/17/science/colorado-brain-data-privacy.html> . Accessed on: June 24, 2024.

NICOLELIS, M. Are we at risk of becoming biological digital machines? *Nature Human Behavior*. *Nat Hum Behav*, 2017. Available at:<https://doi.org/10.1038/s41562-016-0008> . Accessed on: 02. Jul. 2024.

NICOLELIS, M. *Far beyond our selves: the new neuroscience that unites brain and machines—and how it can change our lives*. 1st ed. São Paulo: Planeta, 2017. 25-28 p.

NIETO-CHAUPIS, H. "The Internet of Brain Things: Theoretical Basis for the Usage of Neuralink Chip." *IEEE 13th International Conference on Consumer Electronics–Berlin (ICCE-Berlin)*, Berlin, Germany, 2023, pp. 1-6. Available at:<https://ieeexplore.ieee.org/abstract/document/10375671> . Accessed on: 02. Aug. 2024.

OCHANG, P. EKE, D. STAHL, B. *Towards an understanding of global brain data governance: ethical positions that underpin global brain data governance discourse*. Front Big Data. 2023. Available at: <https://pubmed.ncbi.nlm.nih.gov/38025947/> . Accessed on: July 8, 2024. 03 p.

OAS – ORGANIZATION OF AMERICAN STATES. Inter-American Declaration of Principles on Neuroscience, Neurotechnology and Human Rights. Available at: [https://www.oas.org/es/sla/cji/temas\\_culminados\\_reciente\\_Neurociencias\\_Neurotecnologias\\_y\\_Derechos\\_Humans.asp](https://www.oas.org/es/sla/cji/temas_culminados_reciente_Neurociencias_Neurotecnologias_y_Derechos_Humans.asp) . Accessed on: July 23, 2024.

PIVA, S. *Neurorights: the necessary protection of the human mind in times of advances in neurotechnology and AI*. Fenalaw, 2023. Available at: <https://www.fenalaw.com.br/fenalawlab/neurodireitos-a-necessaria-protecao-da-mente-humana-em-tempos-de-avanco-de-neurotecnologias-and-da-ia/> . Accessed on: August 2, 2024.

RODRÍGUEZ, J. Artificial intelligence and neuroderechos. Straights and perspectives. Constitucional Cuestiones, Revista Mexicana de Derecho Constitucional, Núm. 46, Enero-Junio 2022 ISSN (electronic version): 2448-4881. Available at: <https://www.scielo.org.mx/pdf/cconst/n46/1405-9193-cconst-46-93.pdf> . Accessed on: July 26, 2024.

SOLOMON, L. et al. *Final Report – Committee of Jurists Responsible for the Review and Update of the Civil Code*. Brasilia. Federal Senate, 04/05/2024. Available at: <https://legis.senado.leg.br/comissoes/comissao?codcol=2630> . Accessed on: July 28, 2024.

SCHWAB, K.. *The fourth industrial revolution*–New York: Routledge, 2016. 115 p.

SILVA, GA A New Frontier: The Convergence of Nanotechnology, Brain Machine Interfaces, and Artificial Intelligence. *Front. Neurosci.* 12:843. Available at: <https://www.frontiersin.org/journals/neuroscience/articles/10.3389/fnins.2018.00843/full> . Accessed on: July 20, 2024.

STRICKLAND, E. Worldwide campaign for neurorights notches its first win. IEE Spectrum, 2021. Available at: <https://spectrum.ieee.org/neurotech-neurorights> . Accessed on: 22 Jul 2024

THE NEURORIGHTS FOUNDATION. *The Five Neurorights*. Available at: <https://neurorightsfoundation.org/mission> . Accessed on: June 1, 2024.

WHO – World Health Organization. Global report on health equity for persons with disabilities. Geneva: WHO, 2022. Available at: <https://www.who.int/publications/i/item/9789240063600> . Accessed on July 31, 2024.

WILD, K. 'Our notion of privacy will be useless': what happens if technology learns to read our minds? The Guardian, 2021. Available at: <https://www.theguardian.com/technology/2021/nov/07/our-notion-of-privacy-will-be-useless-what-happens-if-technology-learns-to-read-our-minds> . Accessed on: June 17, 2024.

YUSTE, R. GOERING, S. et al. Four ethical priorities for neurotechnologies and AI. Nature. 2017. Available at: <https://www.nature.com/articles/551159a> . Accessed on: June 18, 2024.

ZHANG, X. MA, Z. ZHENG, H. et al. The combination of brain-computer interfaces and artificial intelligence: applications and challenges. *Ann Transl Med.* 2020 Jun;8(11):712. doi: 10.21037/atm.2019.11.109. PMID: 32617332; PMCID: PMC7327323. Available at: <https://doi.org/10.21037/atm.2019.11.109> . Accessed on: June 18, 2024.

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

Axis II

# Cities smart and new technologies

## AUTHORS

Carolina Freitas

Daniel Santiago Diniz

Victor Call Alvim

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

11

# Smart Cities and Necropolitics: Protection Data and Fundamental Rights in the Digital Age

Claudio Mendes da Silva

*Cowards are those who have everything good and provide evil for the favela to die.* Creole.

Summary: Introduction. **1.** Smart Cities and Social Inequalities: A Non-Par Debate **2.** “Dadification” of life and fundamental rights in the digital age **3.** From Colonialism to the Digital Age: The Persistence of Surveillance and Social Control in Brazil. Final Considerations. References.

## Introduction

The first decades of the 21st century have been marked by the massive increase in the use of data, especially personal data, to support the new market style, based on this type of input for the supply of products or services. In this scenario, not only the handling of data through data mining techniques is considered, *big data* by business agents, but also by governments, due to the computerization of cities and public policies based on the use of information and automation technologies, with a view to building new models of *Smart Cities* also called “Smart Cities”. It is important to emphasize that, in this study, the conceptual dilemmas and controversies on this topic will not be addressed, but rather the aim will be to make its understanding more accessible, to a greater or lesser extent, highlighting its practical application and social implications.

Despite the undeniable possibility of citizens benefiting from products, policies and facilities generated through the use of data, it is also necessary to evaluate the impacts on citizens themselves with regard to their constitutional rights to privacy, autonomy and data protection. The latter was more recently included in the list of fundamental rights, in the form of Art. 5, LXXIX, Constitution of the Federative Republic of Brazil (CRFB/88), through Constitutional Amendment No. 115, of 2022.

In this regard, the General Data Protection Law, which was approved in 2018, in the form of Law No. 13,709, of 14 December, is also highly relevant.

1. Graduated in Law from the State University of Rio de Janeiro - UERJ; Postgraduate in Digital Law from the Institute of Technology and Society (ITS Rio), in partnership with UERJ; Lawyer; Legal Advisor at the Decodifica Institute.

2. According to the report produced by the Rio de Janeiro Institute of Technology and Society (ITS-Rio), “it is, literally, the set of data whose existence is only possible as a result of the massive collection of data that has become possible in recent years, thanks to the omnipresence of devices and sensors in everyday life and the growing number of people connected to such technologies through digital networks and also sensors”. *Big data in the Global South. Case study report*. Rio Institute of Technology & Society. Rio de Janeiro, 2016. Available at: [https://itsrio.org/wp-content/uploads/2017/02/ITS\\_Big-Data\\_PT-BR\\_v4.pdf](https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf). Accessed: Jul. 2024.

August 2018, and came into force on September 18, 2020. The regulation comes in a scenario in which the aim is to define guidelines for the consolidation of the regulation of an ecosystem for the protection of the rights to privacy and personal data. This, considering that the LGPD becomes the first general regulation on this subject in Brazil.

Innovation, in the broadest sense of the word, should not emerge at any cost. The so-called 4th Industrial Revolution that the world is experiencing has been causing a profound change in the structures of cities, requiring a comprehensive and contextualized reflection on its social and ethical impacts. This event has redefined the way we interact with urban spaces, bringing new dynamics of power and control that have directly affected the quality of life and individual rights of citizens.

This article, in turn, aims to bring more local insights, initially focused on Brazil, and examine the impacts and highly harmful potential of these technologies, such as those used for monitoring purposes, especially in the area of public safety, given the accentuated use of data, in historically vulnerable populations, especially black and peripheral populations. This examination will be carried out in light of the guarantees of civil-constitutional laws that aim to protect the right to privacy and data protection, even despite the non-direct incidence of the LGPD, according to its art. 4, item III, item "a".

Furthermore, we seek to reflect on what is understood about the theme of *Smart Cities*, the role of the State as a sovereign entity in the formulation and implementation of public policies, surveillance technologies and data control in smart cities and how such role can influence and potentially reinforce necropolitical practices in the lives and rights of historically vulnerable groups, as already mentioned, but considering the perspective of Achille Mbembe<sup>3</sup>.

The urgency of the topic is due to the current market model, in which personal data are important assets for the different actors in the economy, taking into account that the State occupies a position as an active agent in this sense. This is without mentioning the issue of its political power in the formulation of public policies, and it is crucial to emphasize how the lack of citizen participation in the formulation of these can further exacerbate the inequalities already experienced. Furthermore, it is worth noting that the guiding question of this work is embodied in the following question: how or in what

3. MBEMBE, Achille. *Necropolitics. Biopower, sovereignty, state of exception, politics of death (ebook)*. Sao Paulo: N-1 editions, 2018.

To what extent can Smart Cities be an environment of non-discrimination in the current technological context?

The search for possible solutions or mitigation for this problem, which is already on the rise in our scenario, will involve a brief, but not so simplistic, analysis and historical-social-political contextualization of Brazil, based on the assumption that what we understand as discrimination, in general, is not something new, considering the age of information and technological inputs, but that it reproduces what is already something intrinsic to society, in itself, both of those who provide these tools, in the case of the Global North, and of those who consume them, in the case of Brazil, as one of the representatives of the Global South.

## 1. Smart Cities and Social Inequalities: A Debate non-parity

Right off the bat, it is worth noting that all societies are technological to some extent. What measures the degree of innovation – if this type of measurement is “fair” for comparison purposes – is the context in which a certain group or society finds itself. For example, the stone knife was a major innovation in the society that lived 3,000 years before Christ (BC), because it was a sharp object that could be used for hunting and defense.<sup>4</sup> Likewise, in a more current time frame, it is also a highly functional technology that serves us for food – considering, of course, the Western lifestyle. Therefore, the use of technological devices such as *tablets* and *smartphones*, with or without Artificial Intelligence (AI), does not necessarily define what is modern and/or innovative.

Smart Cities, in turn, are commonly characterized by the massive use of technology with the use of data that, at least in theory, has the power to improve the quality of life of its citizens, as well as enhance the important element of efficiency with regard to the management of resources – financed and belonging to its population – and the sustainability of the urban space itself.<sup>5,6</sup>

4. BOLLA, Carla. *How France popularized the use of cutlery*. *Forbes*. Sep 15, 2022. Available at: <https://forbes.com.br/forbeslife/2022/09/carla-bolla-como-a-franca-popularizado-o-uso-de-talheres/>. Accessed: Jul. 2024.

5. OB.BR. NATIONAL DATA PROTECTION AUTHORITY (ANPD). Smart Cities. Available at [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao\\_radar\\_tecnologico\\_jan\\_2024.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf). Accessed: Jul. 2024.

6. Furthermore: The ABNT standard, based on ISO 37122 (ABNT, 2021), defines a smart city as a city that increases the pace at which it delivers social, economic and environmental sustainability results and that responds to challenges such as climate change, rapid population growth and political and economic instability, fundamentally improving the way it engages society, applies collaborative leadership methods, works through municipal disciplines and systems, and uses data information and modern technologies, to provide better services and quality of life for those who live there (residents, businesses, visitors), now and in the foreseeable future, without unfair disadvantages or degradation of the natural environment. *Ibidem*.

Bill (PL) No. 976 presented on 03/19/2021, with a view to establishing the National Smart Cities Policy (PNCI)<sup>7</sup>, conceptualizes the term as follows, *verbatim*:

Art. 2 For the purposes of this Law, the following definitions apply:

I – smart city: urban space oriented towards investment in human and social capital, sustainable economic development and the use of available technologies to improve and interconnect city services and infrastructure, in an inclusive, participatory, transparent and innovative way, with a focus on improving the quality of life and well-being of citizens.

This current lifestyle that we are increasingly experiencing in our daily lives, especially in the use of technology in the area of public safety, is directly associated with the importation of a model produced in the Global North, where the most powerful companies in the sector are concentrated, from an economic point of view. This dynamic has been driven by the private market, within the capitalist system of production, in which large technology companies are the main agents. These, in turn, regulate contemporary social life, a perspective in which our personal data is collected and/or sold by or to other companies, which will use it for their own benefit.<sup>8</sup>, given that obtaining profit is a condition *sine qua non* for companies to be established in this way.

In this regard, it is necessary to reflect on the impacts of this internalization in a context that, in itself, is one of extreme inequality. Despite this, it is also worth considering that:

Cities are living (non-static) organisms and, therefore, when managed by technological systems, these must have sufficient flexibility to contemplate not only changes in direction dictated by the needs of the inhabitants, but also challenges imposed by new urban problems. Are current systems capable of this flexibility? Furthermore, are these systems inclusive or targeted at a small portion of the population capable of having access to these resources?<sup>9</sup>

7. Available at: [https://www.camara.leg.br/proposicoesWeb/prop\\_mostrarintegra?codteor=1977843&filename=PL%20976/2021](https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1977843&filename=PL%20976/2021). Accessed: Jul. 2024.

8. RIBEIRO, Laura Talho. *Smart surveillance technologies: insights into security in urban centers*. Available at: [https://itsrio.org/wp-content/uploads/2018/03/laura\\_talho\\_smartsurveillance.pdf](https://itsrio.org/wp-content/uploads/2018/03/laura_talho_smartsurveillance.pdf). Accessed: July 2024.

9. MENDES, Teresa Cristina M. *Smart Cities: Solution for cities or deepening social inequalities?* Rio de Janeiro, 2020. p.4. Available at: [https://www.observatoriodasmetroles.net.br/wp-content/uploads/2020/01/TD-011-2020\\_Teresa-Mendes\\_Final.pdf](https://www.observatoriodasmetroles.net.br/wp-content/uploads/2020/01/TD-011-2020_Teresa-Mendes_Final.pdf). Accessed: July 2024.

Teresa Cristina Mendes highlights that the flexibility of technological systems is crucial to meet the needs of residents<sup>10</sup>. This raises the question of how Smart Cities can be adapted so as not to perpetuate existing inequalities, considering the social dynamics experienced in cities, and also understanding the historical context of the country as a whole, since this aspect also reflects social inequalities. In this regard, the position of the black population in the current situation cannot be analyzed in isolation, as it would be a mistake to ignore the almost four hundred years of slavery suffered, its structural limitations and, even more so, the issue related to the total alienation of its dignity – here in reference to the already consolidated principle of the dignity of the human person –, a scenario that was marked by the emptying of the humanity of this public.

A well-known fact that we must also keep in mind in order to try to understand how this new dynamic brought by Smart Cities, imported from another reality, can be equally harmful and exclusionary, indirectly and directly affecting the black community, is that the Portuguese colonizer, in his process of alienating an entire culture, also developed a mechanism to neutralize ethnic consciousness through his imperialist ideology of an “agent of evolution and civilization”. This process is expressed by Clóvis Moura in words such as: “*democratic verbalization*”<sup>11</sup>. This caused a significant portion of the black population, having assimilated such ideological imposition, to try to pass themselves off as white, or at least promote themselves as such.

- if in this chromatic scale that the colonizer had established, having as a superior model to be achieved, the white. This phenotypic policy sought and still seeks to make the components of this specific group flee from their origins, seeking to assimilate the scale of white values and standards.

Although we are making a leap forward in time, it is crucial to emphasize that this ideology remains deeply rooted in our society, given that we are still in the historical process of recovering the identity, dignity, autonomy and well-being of the black population. For example, it is worth noting that Law No. 12,711, of August 29, 2012, the Quota Law, is an extremely recent policy of reparation for slavery in our timeline, one of the only ones that explicitly exists, not to mention the Lei Áurea, a law that marked the abolition of slavery in Brazil. It is possible to infer, through these facts, how delicate and urgent the existing social abyss is.

10. Ibid.

11. MOURA, Clóvis. *Slavery, colonialism, imperialism and racism*. Afro-Asia, Salvador, n. 14, 1983. p.3. Available at: <https://periodicos.ufba.br/index.php/afroasia/article/view/20824/13425>. Accessed: Jul. 2024.

In short, it is also worth inferring that “the racialized distribution of Brazilian cities is the result of both the convergent accumulation of countless decisions and incidences of inequality and racism and the adoption of racist ideologies in planned cities.”<sup>12</sup>

Still in the case of Brazil, a country that faces major problems of digital inclusion and profound social and economic inequalities, among the people who do not access the internet, 24 million are in urban areas, 17 million declared themselves black or brown and 17 million belong to classes DE, which points to a digital exclusion in the urban peripheries of the country.<sup>13</sup> Thus, the concept of *Smart Cities* It is being incorporated in a limited way, although some segments, such as public safety, receive robust investments already thinking about this model of reality<sup>14</sup>. It is still far from being a full reality to think about the complete implementation of technological resources in urban development, being yet another megalomaniac policy without empirical knowledge of its consequences.

This issue is also addressed by Teresa Cristina, who corroborates:

Despite inclusive discourses, it is clear that the issue of inequality is still present in most initiatives (notably in less developed countries), as the inhabitants, despite having the potential to play an active role, are defined as mere consumers of technological solutions.<sup>15</sup>

The lack of adequate infrastructure, high implementation costs and the absence of effective public policies aggravate this situation. Not to mention the difficulty of replicating a model – even if it has been efficient in another context, especially if it takes into account the global north. In addition, regional inequalities and the concentration of investments in richer urban areas intensify the exclusion of peripheral and rural populations. For Brazil to move closer to a truly smart city, it is essential to implement policies that promote inclusion.

12. SILVA, Tarcizio. *Algorithmic racism: artificial intelligence and discrimination in digital networks*. New York: New York University Press, 2019. p.

13. CAMARGO, Bianca. *About 84% of Brazilian homes have access to the internet, says survey*. CNN, São Paulo, November 16, 2023. Available at: <https://www.cnnbrasil.com.br/nacional/cerca-de-84-dos-lares-brasileiros-tem-acesso-a-internet-diz-pesquisa/>. Accessed: Aug. 2024.

14. The Governor of Rio de Janeiro, Cláudio Castro, invested R\$236.5 million reais in the purchase of facial recognition equipment. SANTO, Thaís Espírito. RJ announces cameras with facial recognition and license plate recognition in police vehicles. *G1*, Rio de Janeiro, April 3, 2021. Available at: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/04/03/rj-announces-cameras-with-facial-recognition-and-license-plate-reading-in-pm-vehicles.ghtml> Accessed: Jul. 2024.

15. MENDES, Teresa Cristina M. *Smart Cities: Solution for cities or deepening of social inequalities?*. Rio de Janeiro, 2020. p.6. Available at: [https://www.observatoriodasmetroles.net.br/wp-content/uploads/2020/01/TD-011-2020\\_Teresa-Mendes\\_Final.pdf](https://www.observatoriodasmetroles.net.br/wp-content/uploads/2020/01/TD-011-2020_Teresa-Mendes_Final.pdf) Accessed: July 2024.

are digital, ensure equitable access to new technologies and promote citizen participation in decisions on urban development.

It is essential to note that the aforementioned citizen participation brings with it the idea that peripheral territories have empirical knowledge about the reality they experience, especially when it comes to the process of formulating, monitoring the execution and evaluating a public policy, but that it requires multisectoral efforts to, for example, participate in popular forums, seminars, workshops and other co-construction mechanisms, in which informed knowledge and autonomy to deliberate on the topic in question are guaranteed.<sup>16</sup> Without these efforts, technologies may end up deepening existing divisions and perpetuating the marginalization of the most vulnerable communities.<sup>17</sup>

## 2. “Gifting” of life and fundamental rights in digital age

Stefano Rodotà<sup>18</sup>, in a lecture-class entitled “Body Transformations”, held on November 6, 2015, at the State University of Rio de Janeiro (UERJ), accompanied *on site* by the author of the work, discussed the profound transformations that the human body was undergoing, a fact that is still extremely current, especially in the age of information and technology. Rodotà observed that the body, previously seen as an inviolable physical entity, is now transformed into data and information that can be manipulated and used by third parties. The digital age introduced the concept of the “electronic body”, where biometric elements such as fingerprints, irises, retinas and even facial expressions are also “datafied”, being used to identify and control individuals.

This control extends to technologies such as subcutaneous microchips and even cell phones. *smartphones*, which allow constant localization

16 For example, the Popular Public Security Forum, which was launched in 2022 in Rio de Janeiro, according to the Observatório de Favelas. This event is recent from a historical point of view, but it already opens the way to think about a national initiative and the construction of a space in which governments and decision-makers can also make better informed decisions on such a sensitive issue. VELLASCO, Ramon. Popular Public Security Forum is launched in Rio de Janeiro. *Slum Observatory*. Rio de Janeiro. June 29, 2023. Available at: <https://observatoriodefavelas.org.br/public-security-forum-is-launched-in-rio-de-janeiro/>. Accessed: Aug. 2024.

17. In this sense, Clarissa Nassar Tambelli also concludes: “In this sense, it is important that the opportunities of a smart city do not overshadow other notable issues such as social inequality, technological illiterates, generational and even gender differences in access. On the contrary, such aspects need to be raised when thinking about a solution that involves technology, and other solutions that do not only consider its use should also be explored and applied.” TAMBELLI, Clarice Nassar. *Smart Cities: a brief critical investigation into the limits of a contemporary narrative on cities and technology*. Available at: [https://itsrio.org/wp-content/uploads/2018/03/clarice\\_tambelli\\_smartcity.pdf](https://itsrio.org/wp-content/uploads/2018/03/clarice_tambelli_smartcity.pdf). Accessed: Jul. 2024.

18. RODOTÁ, Stefano. *Electronic Body and Privacy. Lecture-Class presented at the University of Rio de Janeiro*, Rio de Janeiro, November 6, 2015.

of a person, generating a new form of surveillance that threatens privacy and human dignity. Mass surveillance, exemplified by security cameras that can film a person hundreds of times a day in large cities, raises questions about the expectation of privacy and the impact of these practices on individuals' personal and professional lives.

In view of this, Danilo Doneda also observed:

Personal information – which includes all information relating to a person – therefore assumes importance for various reasons. We can establish, from the outset, two factors that are almost always among the justifications for the use of personal information: efficiency and control. A series of interests are articulated around these two factors, involving the State as private entities [...] <sup>19</sup>

Data protection therefore emerges as a fundamental element in relation to the topic under debate, particularly considering the aforementioned information age. As the degree of exposure of individuals and their subjection to technological structures belonging to States and large companies increases, it becomes increasingly important to develop not only instruments that place the rights to data protection and privacy in a position of preeminence, in the face of strictly patrimonial situations.<sup>20</sup>, but also to offer tools in terms of knowledge and information to citizens – especially those belonging to historically more vulnerable groups. This is also independent of equipping them with political awareness, in order to possibly question certain types of public policies employed based solely on the supremacy of the public interest, such as the use of facial recognition technologies in public security.

It is also important to note that the right to privacy, despite the fact that it arose, in theory, as a desire for isolation (outside the Brazilian context and the global south, it must be said), became not just a desire, but a right enforceable against third parties, from the end of the 19th century, with the consecration of the Bourgeois Revolutions, starting from the article *The Right to Privacy*, on December 15, 1980, developed respectively by Samuel Warren and

19. DONEDA, Danilo. *From privacy to personal data protection: Fundamentals of the General Data Protection Law [e-book]*. 2nd ed. São Paulo: Thomson Reuters Brazil, 2019. p. 33.

20. TEFFÉ, Chiara Spadaccini de. *Sensitive personal data: qualification, processing and good practices*. 1st ed. Indaiatuba, SP: Foco, 2022. E-book.

Louis Brandeis<sup>21</sup>. This was the first legal construction on this right in the world. Privacy was born as an individualistic right, but currently, when it migrates to an ecosystem based on personal data, it connects people to society, still requiring a secure regime for this to happen without harm.

In short, privacy and data protection have different orders, but they are interconnected. Data protection does not replace privacy, but complements it. For these reasons, they are crystallized in our Constitution.<sup>22</sup>, which protects privacy and private life as fundamental rights in accordance with art. 5, X, in addition to the right to data protection, including in digital media, as provided for in art. 5, item LXXIX, also of the CRFB/88, this last regulation being inserted in a more recent context, through Constitutional Amendment No. 115, of 2022.

In addition, the General Data Protection Law emerged, the first regulation and also the most specific that deals with the protection of personal data, which was approved in 2018, in the form of Law No. 13,709, of August 14, 2018 and came into force on September 18, 2020.<sup>23</sup>. The regulation emerges in a scenario in which the aim is to define guidelines for the consolidation of the regulation of an ecosystem for the protection of the rights to privacy and personal data. The aforementioned law also aims, among other objectives, to (i) guarantee material equality and freedom of natural persons; (ii) ensure the free development of the human personality; (iii) prevent unlawful and/or abusive discrimination; (iv) prevent certain groups from suffering undue restrictions on assets and scenarios of prejudice and stigmatization.

Such contextualization is essential so that the model of *Smart Cities* as a phenomenon isolated from others, as an apparent symbol of progress, especially when analyzed from the perspective of public safety in a territory as rugged as Brazil, especially

21. Samuel Warren and Louis Brandeis, *"The right to privacy"*, in: 4 Harvard Law Review 193 (1890).

22. In this regard, with regard to the prevalence of the civil-constitutional law system, with regard to the protective bias towards human beings in disputes not only between individuals, but also between them and the State itself, according to the teachings of the collective work organized by masters Anderson Schreiber and Carlos Nelson Konder: "In other words, it is the constitutional norms that must guide the hermeneutic process, so that it is not up to the parties to choose the prevailing source. This prevalence will be the result of the interpretation of the Federal Constitution and ordinary legislation in its light." SOARES, Felipe Ramos Ribas; MATIELI, Louise Vago; DUARTE, Luciana da Mota Gomes de Souza. *Unity of ordering in the plurality of sources: a critique of microsystems theory*. In: SCHREIBER, Anderson; KONDER, Carlos Nelson (Coords.). *constitutional civil law*. e-book. New York: Oxford University Press, 2016. p.79.

23. However, as Chiara de Teffé teaches, the protection of rights concerning data protection was claimed based on certain provisions established, in addition to the Federal Constitution, in some sectoral standards, which directly or indirectly deal with issues related to both privacy and personal data, such as the Consumer Protection Code (Law No. 8,078/90), the Internet Civil Rights Framework (Law No. 12,965/14), in addition to the Access to Information Law (Law No. 12,527/11) and the Positive Registry Law (Law No. 12,414/11). However, this regulatory framework showed - if not very precise and did not offer adequate guarantees to people (...). TEFFÉ, Chiara Spadaccini de. *Sensitive personal data: qualification, processing and good practices*. 1st ed. Indaiatuba, SP: Foco, 2022. E-book.

all because the inestimable value of the right to privacy and data protection must be considered as fundamental and inherent to citizens. The idea of progress brought about by that dynamic begins to be seen as relative in the face of this.

In a study that resulted from the research project of the Center for Technology and Society of the Getúlio Vargas Foundation, linked to the Law course in the State of Rio de Janeiro (CTS-FGV)<sup>24</sup>, conducted between 2017 and 2019 in three Brazilian cities: Salvador, Rio de Janeiro and Campinas, three researchers examined both the scope and scale of state surveillance practices associated with public security in Brazil, based on the observation of three video surveillance tools – facial recognition, automatic license plate recognition and cameras. In the end, they found that: the enthusiasm for incorporating new technologies into the portfolio of state authorities does not necessarily translate into advances in public security; secondly, that material and human resource limitations can lead to discrimination against people and groups already traditionally persecuted by police authorities, particularly black and poor people, who circulate in spaces where these technologies are in full operation; and that in this way, instead of being expanded, the security of citizens is potentially threatened by the increase in the repression of fundamental rights.<sup>25</sup>

The reflections of Stefano Rodotà and, later, those of Danilo Doneda raise crucial questions about the transformation of the concept of body and privacy in the digital age. The notion of “electronic body” reveals how individuality is increasingly subject to data manipulation, representing a threat to privacy, data protection and human dignity itself. The aforementioned authors warn of the need for a legal framework that protects the integrity of personal data, but in addition to this, it is crucial to offer tools that also seek to empower citizens with knowledge and instruments to defend their rights in a scenario of increasing surveillance against both private individuals and the State itself. At this point, it is worth highlighting the incessant contribution of Civil Society Organizations to uphold the most basic rights of Brazilian citizens.

24. See more at:<https://diretorio.fgv.br/pesquisa/centro-de-tecnologia-e-sociedade> .

25. REIA, Jess; BELLI, Luca. *Smart Cities in Brazil: regulation, technology and rights*. Belo Horizonte, MG: House of Law, 2021. p.112. Available at:<https://repositorio.fgv.br/server/api/core/bitstreams/390c1729-357b-4c4f-ba30-e236419debf1/content> . Accessed: Jul. 2024.

The LGPD emerges as an essential response to regulate the use of personal information, guaranteeing the freedom and material equality of individuals in the face of the unprecedented contribution to the models of *Smart Cities*. In order to ensure effective data protection, it is worth considering a more practical perspective that considers citizen participation, from a perspective in which we can co-construct, that is, not only construct in relation to others, we must place ourselves as part of the problem in order to generate an effective solution, within the reality of direct connection with the most latent social policy aspirations in respect of basic-fundamental rights. In fact, this element of participation is what has the potential to confer citizenship in a more concrete way, guaranteeing protagonism to an underrepresented group within the democratic model in which we are inserted.

This approach is essential to ensure that technological innovations do not increase inequalities, but promote inclusive urban development that respects human dignity.

### 3. From Colonialism to the Digital Age: The Persistence of Surveillance and Social Control in Brazil

An analysis of Brazilian history, since the arrival of the Portuguese in 1500<sup>26</sup>, until the “end” of slavery, with the signing of the Lei Áurea, shows us that even today we still find policies that reflect aspects of that time. Despite significant legal and social advances, the control, surveillance and genocide of the lives and bodies of black and peripheral people is still a keynote of the most recent state organization<sup>27</sup>.

It is no coincidence that it is the State itself that defines which legal assets receive a greater or lesser degree of protection, something that directly reflects on the definition of public policies. In this sense, it tends to privilege individuals who are members of the dominant classes and have greater possibilities and opportunities for capital accumulation, “giving maximum emphasis to the protection of private assets

26. Cf. <https://brasil500anos.ibge.gov.br/>.

27. An example of this was the reaffirmation of the institutionalization of the policy propagated and implemented by the former Governor, also impeached in Rio de Janeiro, Wilson Witzel, under the guidelines of “aiming for the little head”. This, while since his election in 2018, the number of police operations in the favelas of RJ has also increased indiscriminately under the government of his successor Cláudio Castro, who also invested massively in facial recognition technologies, without any assessment of the impact of this measure, and without taking into account structural aspects of the territory, given that what can be observed most are bullets and more “stray” bullets at people belonging to the communities of Rio, such as the massacre that occurred in the Jacarezinho favela on May 6, 2021, which resulted in a total of 28 people dead, including a police officer. By not protecting lives, in fact, the State is already failing profoundly, it must be said, given that there have been no significant improvements in the public safety rates of the state of Rio de Janeiro. MENA, Fernanda. 'Aiming for the little head' is missing the target. *Sao Paulo Newspaper*. Nov 7, 2018. Available at: <https://www1.folha.uol.com.br/columnas/fernanda-mena/2018/11/aim-at-the-little-head-and-miss-the-target.shtml>. Accessed: Aug. 2024.

to target the forms of deviation typical of the socially weakest and most marginalized groups”<sup>28 29</sup>. However, in this aspect, such an actor does not take into account such social processes that are inherent to his history.

Achille Mbembe has made a significant contribution to this literature in terms of the construction of the concept of necropolitics, which is embodied in the idea that sovereignty is the ability to exercise control over mortality and define life as the implementation and manifestation of power.<sup>30</sup>, initially thinking about the State's performance. Taking into account that data is also in a spectrum of power relations, the models of *Smart Cities*, when thought of without citizen participation, are basically expressing an act of power, solely serving as a tool for automating systematic oppression, and are also harmful to those who historically no longer fully enjoy their fundamental rights and who have also traditionally been subjugated and controlled.

The social and political power of the State to dictate how some people can live and how others should die, one of the aspects of Mbembe's concept of necropolitics, leads us to consider not only the death of bodies, in itself, from a biological point of view, a fact that in itself is of extreme relevance. There are also acts that dehumanize, silence and curtail fundamental rights.<sup>31</sup>, such as privacy and data protection, in acts explained by structural racism, being propagated by models of *Smart Cities*, leading black people to have their “deaths in life”, in analogy to what Mbembe also understands as “invisible killings”<sup>32</sup>.

28. BARATTA, Alessandro. *Critical criminology and criticism of criminal law: introduction to the sociology of law*. Translated by Juarez Cirino dos Santos. Rio de Janeiro: Carioca Institute of Criminology/Revan, 3rd ed., 2002. p. 176.

29. State institutions use data such as the use of social media posts as a trigger for investigations that culminate in police operations, such as the Jacarezinho Massacre that occurred on May 6, 2021 in the city of Rio de Janeiro. This event is considered the deadliest in the history of Rio de Janeiro, caused by a police operation that resulted in the death of 28 people, including 1 police officer. This action raised several suspicions of illegalities and human rights violations and, despite the seriousness and the consequent need for transparency in the case, the operation report was kept confidential for five years. See BARREIRA, Gabriel; BRASIL, Filipe. Available at: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/05/06/operacao-no-jacarezinho-rio-tem-numero-recorde-de-mortes.ghtml> . Accessed in July 2024. Cf. NUNES, Pablo; SILVA, Mariah Rafaela; OLIVEIRA, Samuel R. de. *A Rio of cameras with selective eyes: use of facial recognition by the Rio de Janeiro police*. Rio de Janeiro: CeSec, 2022, p. 14. Available at: [https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT\\_riodecameras\\_mar22\\_0404b.pdf](https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf) . Accessed in August 2024.

30. MBEMBE, Achille. *Necropolitics. Biopower, sovereignty, state of exception, politics of death (ebook)*. São Paulo: N-1 editions, 2018. p.7.

31. In this sense, it is worth recording the testimony of João Antônio, a young black fan who suffered great embarrassment, which should never be naturalized, when he was detained in a football stadium in Sergipe, after a “failure” in the police recognition system used by the police: “In the Sergipe Championship final, I went through a situation that I never imagined possible and I am ashamed and indignant to share it so that something happens and this does not happen again. I was extremely embarrassed, trying to hide my face, I didn't know what to do because the entire Confiança fan base was looking at me, acquaintances and strangers alike.” After the incident, the government of Sergipe suspended the use of the system and announced that it will review the approaches to avoid embarrassments like those of João Antônio. Fan is detained by mistake in Sergipe after failure of facial recognition tool. *The Day*, Rio de Janeiro, April 28, 2024. Available at: <https://odia.ig.com.br/sport/2024/04/6828699-fan-is-held-for-mistake-in-sergipe-after-failure-of-the-facial-recognition-tool.html> . Accessed: Aug. 2024.

32. MBEMBE, Achille. *Necropolitics. Biopower, sovereignty, state of exception, politics of death (ebook)*. São Paulo: N-1 editions, 2018. p. 38.

In fact, this is a considerable concern of the National Data Protection Authority (ANPD) – the body responsible for monitoring and regulating the LGPD, and which is also an ally in the fight for the effectiveness of achieving the full enjoyment of the rights to privacy and data protection of Brazilian citizens:

Data collected by governments and companies at various levels in cities can generate detailed information, categorizations and reports on the personal lives of residents, worsening the asymmetry of information and power.<sup>33</sup>

Given the above scenario, it is clear how important it is to invest in education, a right that is a fundamental aspect of social development. According to the patron saint of Brazilian education, Paulo Freire, failure to comply with this requirement contributes to the maintenance of oppressive structures, based on an unjust order and also responsible for violence against those historically vulnerable individuals who, not surprisingly, live in the communities and outskirts of the city. This fact further exacerbates social inequalities.<sup>34</sup>

However, it is urgent to ensure citizen participation in decision-making processes, whether through public consultations or impact assessments, in which, as a rule, Civil Society Organizations (such as some mentioned here) have contributed significantly based on their methodological research to assess the impacts of introducing an extreme surveillance model. On the other hand, it is also worth thinking about the lack of diversity in the composition of decision-makers, ranging from governments to institutions in society and companies.<sup>35</sup>. This issue is essential to build a culture that promotes greater dialogue between different social groups and their multiple facets, especially to have a truly humanized view of the most vulnerable populations, who are also data subjects.

Final Considerations

33. GOB.BR NATIONAL DATA PROTECTION AUTHORITY (ANPD). Smart Cities. Available at [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao\\_radar\\_tecnologico\\_jan\\_2024.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf). Accessed in July 2024.

34. FREIRE, Paulo. *Pedagogy of the Oppressed*. 78th ed. Rio de Janeiro: Peace and Land, 2021.

35. Despite this, the research Social inequalities by color or race in Brazil, carried out by IBGE, is cited, which identified that 69% of management positions in the country are occupied by white people, while only 29.5% are occupied by black or brown people. See IBGE – Brazilian Institute of Geography and Statistics, 2022 (Second Edition). Social inequalities by color or race in Brazil. Available at: [https://static.poder360.com.br/2022/11/IBGE-DESIGUALDADES-11.NV\\_.pdf](https://static.poder360.com.br/2022/11/IBGE-DESIGUALDADES-11.NV_.pdf). Accessed in August 2024.

The growing urbanization and digitalization of cities, under the label of the model *Smart Cities*, promises significant improvements in quality of life through the application of advanced technologies. However, the reality faced by several Brazilian cities reveals a complex web of social and economic inequalities that cannot be ignored in the import and implementation of these technologies, under penalty of automating (even more) historical oppressions.

In this work, we discuss how the advancement of Smart Cities can both reinforce and mitigate existing social inequalities, depending on the contextualization of the historical-social scenario of the territory and the sector of the economy in which the technological inputs will be used, especially public security. The importance of citizen participation is substantial: without the active inclusion of all voices, especially those of marginalized communities and groups, technological innovations run the risk of perpetuating practices of historical exclusion and discrimination. As evidenced by the analysis of Achille Mbembe's concept of necropolitics, technology can be used as a tool for extreme surveillance, social control, biological death and "in life", aggravating the vulnerability of populations that already face systemic oppression.

The protection of the rights to privacy and personal data emerges as a central pillar in the discussion on fundamental rights in the information age. In Brazil, the LGPD represents a significant advance in the regulation of the processing of personal data, seeking to guarantee the privacy and autonomy of individuals. However, the effective implementation of these protections also depends on widespread awareness and the strengthening of a culture of data protection, which must be widely accessible to all citizens, regardless of their socioeconomic background.

The model of *Smart Cities*, if implemented without an inclusive governance structure, can amplify pre-existing inequalities, becoming yet another layer of social control. For smart cities to truly contribute to a more just and equitable future, it is essential to integrate policies that promote digital equity, social and racial justice, ensuring that all communities have equal access to the benefits offered by technology, as long as it is human-centered.

Finally, it is crucial that the development of smart cities is guided by principles of transparency, inclusion and respect for fundamental rights. Citizen participation should not be just an additional component,

but rather the foundation on which urbanization and digitalization policies must be built. Only through a truly participatory approach will we be able to move towards cities that not only use technology to innovate, but also to promote the dignity and well-being of all their inhabitants.

## References

BARATTA, Alessandro. *Critical criminology and criticism of criminal law: introduction to the sociology of law*. Translated by Juarez Cirino dos Santos. Rio de Janeiro: Carioca Institute of Criminology/ Revan, 3rd ed., 2002. p. 176.

BARREIRA, Gabriel; BRAZIL, Filipe. Available at: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/05/06/operacao-no-jacarezinho-rio-tem-numero-recorde-de-mortes.ghtml> . Accessed: Jul. 2024.

BOLLA, Carla. How France popularized the use of cutlery. *Forbes*. Sep 15, 2022. Available at: <https://forbes.com.br/forbeslife/2022/09/carla-bolla-como-a-franca-popularizando-o-uso-de-talheres/> Accessed: Jul. 2024.

BRAZIL: 500 years of settlement. Brazilian Institute of Geography and Statistics (IBGE). Available at: <https://brasil500anos.ibge.gov.br/> .

CAMARGO, Bianca. About 84% of Brazilian homes have access to the internet, says research. *CNN*, São Paulo, November 16, 2023. Available at: <https://www.cnnbrasil.com.br/nacional/cerca-de-84-dos-brazilian-homes-have-access-to-internet-says-research/> . Accessed: Aug. 2024.

CENTER FOR TECHNOLOGY AND SOCIETY. Available at: <https://diretorio.fgv.br/pesquisa/centro-de-tecnologia-e-sociedade> .

DONEDA, Danilo. *From privacy to personal data protection: Fundamentals of the General Data Protection Law [e-book]*. 2nd ed. São Paulo: Thomson Reuters Brazil, 2019. p 33.

FREIRE, Paul. *Pedagogy of the Oppressed*. 78th ed. Rio de Janeiro: Peace and Land, 2021.

GOB.BR. NATIONAL DATA PROTECTION AUTHORITY (ANPD). Smart Cities. Available at [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao\\_radar\\_tecnologico\\_jan\\_2024.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf). Accessed: Jul. 2024.

Rio de Janeiro Institute of Technology and Society of Rio. *Big data in the Global South. Case study report*. Rio Institute of Technology & Society. Rio de Janeiro, 2016. Available at: [https://itsrio.org/wp-content/uploads/2017/02/ITS\\_Big-Data\\_PT-BR\\_v4.pdf](https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf) . Accessed: Jul. 2024.

Brazilian Institute of Geography and Statistics, 2022 (Second Edition). Social inequalities by color or race in Brazil. Available at: [https://static.poder360.com.br/2022/11/IBGE-DESIGUALDA-DES-11.NV\\_.pdf](https://static.poder360.com.br/2022/11/IBGE-DESIGUALDA-DES-11.NV_.pdf) . Accessed: Aug. 2024.

MBEMBE, Achille. *Necropolitics. Biopower, sovereignty, state of exception, politics of death (ebook)*. São Paulo: N-1 editions, 2018. p.7.

MENA, Fernanda. 'Aiming for the little head' is missing the target. *Sao Paulo Newspaper*. Nov 7, 2018. Available at: <https://www1.folha.uol.com.br/colunas/fernanda-mena/2018/11/mirar-na-cabecinha-e-errar-the-target.shtml> Accessed: Aug. 2024.

MENDES, Teresa Cristina M. *Smart Cities: Solution for cities or deepening social inequalities?*. Rio de Janeiro, 2020. Available at: [https://www.observatoriodasmetrolopoles.net.br/wp-content/uploads/2020/01/TD-011-2020\\_Teresa-Mendes\\_Final.pdf](https://www.observatoriodasmetrolopoles.net.br/wp-content/uploads/2020/01/TD-011-2020_Teresa-Mendes_Final.pdf) Accessed: Jul. 2024.

MOURA, Clovis. *Slavery, colonialism, imperialism and racism*. Afro-Asia, Salvador, n. 14, 1983. Available at: <https://periodicos.ufba.br/index.php/afroasia/article/view/20824/13425> . Accessed: Jul. 2024.

NUNES, Pablo; SILVA, Mariah Rafaela; OLIVEIRA, Samuel R. de. *A Rio of cameras with selective eyes: use of facial recognition by the Rio de Janeiro police*. Rio de Janeiro: CeSec, 2022, p. 14. Available at: [https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT\\_riodecameras\\_mar22\\_0404b.pdf](https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf) . Accessed: Aug. 2024.

*The Day*, Rio de Janeiro, April 28, 2024. Available at: <https://odia.ig.com.br/esporte/2024/04/6828699-torcedor-e-detido-por-engano-em-sergipe-apos-falha-da-ferramenta-de-reconhecimento-facial.html> . Accessed: Aug. 2024.

BILL N° 976/2021. Available at: [https://www.camara.leg.br/proposicoesWeb/prop\\_MostrarIntegra?codteor=1977843&filename=PL%20976/2021](https://www.camara.leg.br/proposicoesWeb/prop_MostrarIntegra?codteor=1977843&filename=PL%20976/2021) . Accessed: Jul. 2024.

REIA, Jess; BELLI, Luca. *Smart Cities in Brazil: regulation, technology and rights*. Belo Horizonte, MG: House of Law, 2021. p.112. Available at: <https://repositorio.fgv.br/server/api/core/bitstreams/390c1729-357b-4c4f-ba30-e236419debf1/content> . Accessed: Jul. 2024.

RIBEIRO, Laura. *Smart surveillance technologies: insights into security in urban centers*. Available at: [https://itsrio.org/wp-content/uploads/2018/03/laura\\_talho\\_smartsurveillance.pdf](https://itsrio.org/wp-content/uploads/2018/03/laura_talho_smartsurveillance.pdf) . Accessed: Jul. 2024.

RODOTÁ, Stefano. *Electronic Body and Privacy. Lecture-Class presented at the University of Rio de Janeiro*, Rio de Janeiro, November 6, 2015.

SANTO, Thaís Espírito. RJ announces cameras with facial recognition and license plate reading in PM vehicles. *G1*, Rio de Janeiro, April 3, 2021. Available at: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/04/03/rj-anuncia-cameras-com-reconhecimento-facial-e-leitura-de-placas-in-pm-veiculos.ghtml> Accessed: Jul. 2024.

Samuel Warren and Louis Brandeis, "The right to privacy", in: 4 Harvard Law Review 193 (1890).

SOARES, Felipe Ramos Ribas; MATIELI, Louise Vago; DUARTE, Luciana da Mota Gomes de Souza. Unity of ordering in the plurality of sources: a critique of the theory of microsystems. In: SCHREIBER, Anderson; KONDER, Carlos Nelson (Coords.). *constitutional civil law*. e-book. New York: University of Chicago Press, 2016.

SILVA, Tarcizio. *Algorithmic racism: artificial intelligence and discrimination in digital networks*. New York: New York Times, 2021.

TAMBELLI, Clarice Nassar. *Smart Cities: a brief critical investigation into the limits of a contemporary narrative on cities and technology*. Available at: [https://itsrio.org/wp-content/uploads/2018/03/clarice\\_tambelli\\_smartcity.pdf](https://itsrio.org/wp-content/uploads/2018/03/clarice_tambelli_smartcity.pdf) . Accessed: Jul. 2024.

TEFFÉ, Chiara Spadaccini de. *Sensitive personal data: qualification, processing and good practices*. 1st ed. Indaiatuba, SP: Foco, 2022. E-book.

VELLASCO, Ramon. Popular Public Security Forum is launched in Rio de Janeiro. *Slum Observatory*. Rio de Janeiro. June 29, 2023. Available at: <https://observatoriodefavelas.org.br/public-security-forum-is-launched-in-rio-de-janeiro/> . Accessed: Aug. 2024.

**Implementation of cities  
smart and sandbox  
regulatory: Challenges and  
opportunities in Juiz de Fora's  
innovation law**

Daniel Santiago Diniz

Summary: Introduction. 1. History, Technology and Governance in Smart Cities. 2. Legislative Bases for Innovation in Brazil. 3. The Innovation Law of Juiz de Fora: Structure, Mechanisms and Impacts. 4. Implementation and Regulation of the sandbox in Juiz de Fora. Final considerations. References.

## Introduction

The concept of smart cities has been widely discussed in recent years, standing out as a promising solution to contemporary urban challenges. The use of information and communication technologies (ICTs) to optimize the efficiency of urban services, improve the quality of life of citizens and promote sustainable development are central objectives of these initiatives. However, the practical implementation of these concepts varies significantly, leading to debates about the true effectiveness and inclusiveness of these strategies.

In Brazil, a set of legislative frameworks and regulations establish the basis for technological advancement in the urban environment, with emphasis on the Legal Framework for Innovation and the Legal Framework for Startups. These legislative instruments promote the creation of innovation and experimentation ecosystems in different government spheres, encouraging cooperation between the public and private sectors. In this context, the Innovation Law of Juiz de Fora (Law No. 14,746/2023) represents an example of how a Brazilian city can adapt these national guidelines to foster local innovation, introducing mechanisms such as the regulatory sandbox, a controlled environment where it is possible to test innovations in compliance with specific municipal regulations.<sup>2</sup>

This article seeks to answer the question: “How does the Juiz de Fora Innovation Law, through its regulatory framework and sandbox, implement the principles of smart cities, and what are the challenges and opportunities of this approach?”. To this end, the structure of the work goes from the theoretical and historical bases of smart cities, including the critical view

1. Lawyer and Public Manager, graduated in Law from the Federal University of Juiz de Fora (UFJF), postgraduate in Digital Law from the State University of Rio de Janeiro (UERJ) and the Rio Institute of Technology and Society (ITS Rio)

2. JUIZ DE FORA. Law No. 14,746, of December 4, 2023. Institutes the Innovation System of Juiz de Fora; defines the development hubs of the Municipality; establishes the attributions of the Municipal Council for Development, Technology and Innovation (Comdeti) and contains other provisions. Official Gazette of the Municipality of Juiz de Fora, Juiz de Fora, MG, December 5, 2023.

by authors such as Robert G. Hollands<sup>3</sup>, Evgeny Morozov and Francesca Bria<sup>4</sup>, up to the analysis of the Brazilian legislative bases that facilitate this urban transformation.

The study delves into the Juiz de Fora Innovation Law, examining its structure, mechanisms and expected impacts, with attention to Decree No. 16,734/2024<sup>5</sup>, which details how the regulatory sandbox works. The analysis explores how regulation seeks to balance innovation with social responsibility, promoting urban governance aligned with community interests. Finally, the final considerations present the main findings and suggestions for improving the application of smart city concepts, emphasizing the importance of governance that supports fair, sustainable and innovative urban development.

## 1. History, Technology and Governance in Smart Cities

Smart cities as discussed by Robert G. Hollands<sup>6</sup>, are characterized by the use of information and communication technologies (ICTs) to improve the efficiency of urban services and the quality of life of citizens. However, Hollands argues that the concept of smart cities is multifaceted and subject to diverse interpretations, which can lead to a superficial or distorted understanding of what actually constitutes a smart city. He highlights that the term “smart” is often associated with positive urban technological innovations, but warns that this label can hide underlying problems and create unquestioned assumptions about urban development.

One of Hollands’ central criticisms is that the term “smart cities” can be used rhetorically, without a precise definition, leading to self-congratulation and a lack of critical inquiry. Many cities that call themselves smart do so as an urban marketing strategy, without necessarily implementing structural or sustainable changes. Hollands questions the assumption that technology alone can solve

3. HOLLANDS, Robert G. *Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? City*, v. 12, no. 3, p. 303-320, 2008. DOI: 10.1080/13604810802479126.

4. MOROZOV, Evgeny; BRIA, Francesca. *The smart city: urban technologies and democracy*. Translated by Humberto do Amaral. 192 p. ISBN: 978-85-7126-046-7.

5. JUIZ DE FORA. Decree No. 16,734, of August 20, 2024. Regulates the operation of the regulatory sandbox in Juiz de Fora and specifies the conditions for its implementation and supervision. Official Gazette of the Municipality of Juiz de Fora, Juiz de Fora, MG, August 21, 2024.

6. HOLLANDS, Robert G. *Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? City*, v. 12, no. 3, p. 303-320, 2008. DOI: 10.1080/13604810802479126.

complex urban problems and suggests that a deeper and more critical understanding of the social and political implications of ICTs in cities is needed, emphasizing the importance of considering social justice and inclusion in discussions on smart cities.

According to the Organization for Economic Cooperation and Development (OECD)<sup>7</sup>, smart cities involve the effective use of digitalization to improve the quality of life of residents, providing more efficient, sustainable and inclusive urban services and environments.

Morozov and Bria discuss the social and democratic implications of urban technologies<sup>8</sup>. Although ICTs promise to make cities more efficient and safer, there is a significant risk that these technologies will be used to primarily benefit private interests rather than serve the common good. The authors point out that the “smart city” often becomes a brand associated with services offered by large technology companies, such as Google, IBM and Cisco, which prioritize optimization and control over citizen participation and social justice.

The technological shift promoted by large corporations has transformed data into an essential element of the neoliberal economy. Smart cities, full of sensors and algorithmic systems, become spaces for the permanent extraction of data, control and modulation of behavior. To prevent smart cities from becoming machines for making workers precarious and benefiting only private interests, Morozov and Bria propose a cooperative management of urban technologies, which must be democratic and inclusive, emphasizing the need to regain control over technologies, data and infrastructures to ensure governance that promotes citizen participation and social equity.

The implementation of urban technologies, according to Morozov and Bria, must be accompanied by policies that guarantee democratic participation and social inclusion. They suggest creating a shared infrastructure and promoting technological sovereignty, where data governance and collaborative practices are essential. This means that cities must adopt approaches that allow citizens to deliberate on the use of their data and actively participate in the development of the technologies that shape their urban environment.

7. OECD. *Smart Cities and Inclusive Growth*. 2020. Available at: [https://www.oecd.org/cfe/cities/OECD\\_Policy\\_Paper\\_Smart\\_Cities\\_and\\_Inclusive\\_Growth.pdf](https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf).

8. MOROZOV, Evgeny; BRIA, Francesca. *The smart city: urban technologies and democracy*. Translated by Humberto do Amaral. 192 p. ISBN: 978-85-7126-046-7.

When discussing the social and democratic implications of smart cities, it is crucial to acknowledge the challenges and opportunities that arise from the digital transformation of cities. On the one hand, there is the potential to significantly improve the quality of urban life through efficiency and innovation. On the other hand, there is the risk of exacerbating social inequalities and creating new forms of exclusion if the implementation of these technologies is not carefully regulated and oriented towards the common good. Therefore, innovative legislation plays a key role in ensuring that smart cities not only utilize advanced technologies, but also promote fair and inclusive urban development.

The development of e-government is a crucial part of the evolution of smart cities. According to Jon Agar<sup>9</sup>, the history of e-government can be traced back to the earliest efforts to mechanize and computerize government processes. The integration of information technologies into administrative processes has had a profound impact on the efficiency and responsiveness of government institutions. The e-government revolution began with the introduction of basic office technologies such as typewriters and filing systems and evolved into the implementation of computers and digital networks.

In the context of smart cities, e-government represents the application of digital technologies to improve urban management and the delivery of public services. Agar argues that the computerization of government was a crucial step towards the implementation of smart technologies in cities, enabling the automation of administrative tasks and improving communication between different government departments. The introduction of computer systems in public administrations has transformed the way data is collected, stored and used, facilitating decision-making and the delivery of more efficient and transparent services.

The interaction between technology and governance is another important aspect in the evolution of smart cities. Eden Medina<sup>10</sup> discusses how the implementation of cyber systems in Allende's Chile is an early example of how technology can be integrated into urban governance to create smarter cities. During Salvador Allende's government, cyber systems were implemented to manage the national economy, an attempt to

9. HAGAR, Jon. *The Government Machine: a Revolutionary History of the Computer*. Cambridge, MA: MIT Press, 2003.

10. MEDINA, Eden. *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*. Cambridge: The MIT Press, 2011. ISBN: 978-0-262-01649-0.

pioneering initiative to use advanced technologies to improve the efficiency and transparency of public administration.

Medina emphasizes that the integration of technologies into urban governance can bring significant benefits, such as improved administrative efficiency, transparency in government operations, and citizen participation. However, he also warns of the associated challenges and risks, such as the centralization of power and the potential exclusion of marginalized groups. The Chilean experience demonstrates the need for a balanced approach, where technology is used to empower citizens and promote more inclusive and participatory governance.

The evolution of e-government and the interplay between technology and governance illustrate how cities can become smarter and more efficient through technological integration. The history of e-government, as described by Agar, and the Chilean example of cyber-enabled systems discussed by Medina, show that the successful implementation of technologies in cities depends on an approach that considers both the benefits and the challenges of these innovations.

In this context, the inclusion of regulatory sandboxes represents a significant advance in the experimentalist approach of public administration to promote innovation. According to Quirino, Hocayen and Cunha<sup>11</sup>, the regulatory sandbox is a controlled environment where standards applicable to innovative products or services are temporarily suspended to test their impact on the market. This tool allows local public administrations to experiment and adjust their regulations based on evidence, promoting economic development that is more aligned with local needs.

The regulatory sandbox is a strategic tool that allows the Public Administration to create experimental environments in which regulatory standards are temporarily relaxed, facilitating the development and testing of innovative products or services without the restrictions imposed by traditional regulations. According to Quirino, Hocayen and Cunha, this experimentalist approach is particularly advantageous for local administrations, as it offers a safe testing ground where the Public Administration can observe the impacts of innovations under controlled conditions and with continuous supervision, promoting more dynamic economic development adapted to the specific needs of each location.

11. QUIRINO, Carina de Castro; HOCAYEN, Helena Gouvêa de Paula; CUNHA, Marcella Brandão Flores da. *Regulatory sandbox: experimental instrument available to local public administration to support economic development*. Public Law Review of the Economy – RDPE, Belo Horizonte, v. 21, n. 84, p. 9-33, Oct./Dec. 2023.

The potential of a regulatory sandbox lies in the flexibility it offers local governments in implementing emerging urban technologies and testing innovative solutions that can transform public administration and city life. However, this flexibility comes with considerable challenges. For a regulatory sandbox to fulfill its role effectively, it is essential that there is strong inter-agency collaboration and that the experimental regulatory environment has comprehensive and inclusive governance. This means that the participation of multiple sectors, such as transportation, public safety and digital infrastructure, is essential to integrate innovations smoothly into urban policies and ensure that the results meet collective goals.

A critical challenge to the effective implementation of regulatory sandboxes lies in defining rigorous criteria and limits for companies' participation. Without detailed regulations that establish limits on action, there is a risk that the sandbox will function more as a regulatory loophole than as a space for responsible experimentation. Hollands and Morozov and Bria<sup>12</sup> warn about this risk, discussing how the concept of smart cities is often used rhetorically, promoting urban technology without a thorough analysis of social impacts and the need for inclusion. They highlight that, without clear guidelines, urban innovations can end up favoring large corporations, promoting data extraction and behavioral control, to the detriment of collective well-being and social justice.

Furthermore, transparency in the process of selecting and monitoring participating companies is essential. Regulatory sandboxes must have supervision and monitoring guidelines, ensuring that companies comply with their established responsibilities and that emerging risks are promptly identified and mitigated. According to Quirino et al., the regulatory sandbox must function as a testing ground where there is a constant feedback cycle between the Public Administration and participating companies, adjusting regulations based on real data and social demands. Continuous supervision is crucial to prevent abuses and ensure that the sandbox contributes to the promotion of urban technologies in an ethical and inclusive manner.

Another critical point for the success of regulatory sandboxes is the adaptation to rapid changes in the urban and technological context. The experimental approach offered by the sandbox allows the Public Administration to adjust

12. HOLLANDS, Robert G. *Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? City*, v. 12, n. 3, p. 303-320, 2008; MOROZOV, Evgeny; BRIA, Francesca. *The smart city: urban technologies and democracy*. Translated by Humberto do Amaral. New York: Routledge, 2019.

The standards are set as the technologies being tested develop, but this requires a commitment to adaptive governance and responsible innovation. Morozov and Bria argue that the implementation of urban technologies must be accompanied by mechanisms of technological sovereignty, which guarantee citizens control over their data and an active participation in the construction of the smart urban environment. This is especially important in smart cities, where the application of new technologies can directly impact urban life and create new ethical, social and political challenges.

In summary, the regulatory sandbox is a tool with the potential to promote sustainable and inclusive urban innovation by providing a controlled space for new technologies to be tested and evaluated before their large-scale application. The challenges of governance, definition of criteria and transparency in supervision highlight the need for a cautious approach and robust regulation. In this way, the regulatory sandbox not only allows for the experimentation of innovative solutions, but also contributes to a more responsive public administration committed to promoting an ethical and responsible digital transformation.

## 2. Legislative Bases for Innovation in Brazil

Brazil, in response to the growing demands for technological development and sustainability, has consolidated an innovative legislative framework that serves as a basis for the advancement of science, technology and innovation at various levels. This set of rules, which we call the “legislative bases for innovation in Brazil,” includes significant legal frameworks and their specific regulations, such as the Legal Framework for Innovation (Law No. 13,243/2016)<sup>13</sup>, the Legal Framework for Startups (Complementary Law No. 182/2021)<sup>14</sup> and strategic guidelines such as the Brazilian Charter for Smart Cities<sup>15</sup>. These laws and guidelines are essential to create environments conducive to the development of innovative ecosystems, from the federal to the municipal level.

The Innovation Legal Framework, sanctioned in 2016, improves the 2004 Innovation Law (Law No. 10,973/2004)<sup>16</sup> by establishing mechanisms to simplify

13. BRAZIL. *Law No. 13,243*, of January 11, 2016. Provides for incentives for scientific development, research, scientific and technological training and innovation, and amends several laws. *Official Gazette of the Union*: section 1, Brasília, DF, p. 1, Jan. 12, 2016.

14. BRAZIL. *Complementary Law No. 182*, of June 1, 2021. Establishes the legal framework for startups and innovative entrepreneurship and amends Complementary Law No. 123, of December 14, 2006. *Official Gazette of the Union*: section 1, Brasília, DF, p. 2, June 2, 2021.

15. Ministry of Regional Development. *Brazilian Charter for Smart Cities*. Brasília, 2021.

16. BRAZIL. *Law No. 10,973*, of December 2, 2004. Provides incentives for innovation and scientific and technological research in the production environment and contains other provisions. *Official Gazette of the Union*: section 1, Brasília, DF, p. 2, December 3, 2004.

promote collaboration between the private sector and public research institutions, aiming to decentralize the promotion of innovation to states and municipalities. This legal framework reformulates nine federal laws and introduces independent measures that facilitate the development of science and technology in the country. Decree No. 9,283/2018<sup>17</sup> complements the regulation of the Legal Framework for Innovation, establishing incentives such as economic subsidies and technological orders, which strengthen the transfer of technologies from Scientific, Technological and Innovation Institutions (STIs) to the market. This decree allows direct and indirect public administration, including STIs, to participate as minorities in the share capital of innovative companies, encouraging the creation of innovative products and processes.

The regulation also encourages cooperation between public and private entities for the execution of Research, Development and Innovation (RD&I) projects, ensuring greater legal certainty in partnerships and facilitating the implementation of innovation policies. This cooperation is exemplified by public-private partnership programs that finance renewable energy and green technology projects.

In the theme of the Internet of Things (IoT), the publication of Decree No. 9.854/2019<sup>18</sup>, which established the “National Internet of Things Plan,” has moved the country forward in its goal of implementing and developing IoT, promoting free competition and the free circulation of data, while respecting information security and personal data protection guidelines. This plan was developed through a partnership between the Ministry of Science, Technology and Innovation and the National Bank for Economic and Social Development (BNDES), encouraging the creation of smart cities that use IoT sensors and networks to improve public services such as transportation and security.

Complementary Law No. 182/2021, known as the Legal Framework for Startups, complements innovation initiatives by establishing a favorable regulatory environment for startups and entrepreneurs. This law defines specific guidelines to foster the startup ecosystem in Brazil, including the creation of experimental regulatory environments, known as regulatory sandboxes, that allow the testing of innovations with regulatory flexibility.

17. BRAZIL. *Decree No. 9,283*, of February 7, 2018. Regulates Law No. 10,973, of December 2, 2004, and Law No. 13,243, of January 11, 2016, on incentives for innovation and scientific and technological research in the productive environment. *Official Gazette of the Union*: section 1, Brasília, DF, p. 1, Feb 8, 2018.

18. BRAZIL. *Decree No. 9,854*, of June 25, 2019. Institutes the National Internet of Things Plan and provides for the Management and Monitoring Chamber for the Development of Machine-to-Machine Communication Systems and the Internet of Things. *Official Gazette of the Union*: section 1, Brasília, DF, p. 5, June 26, 2019.

Among the main points of Complementary Law No. 182/2021 are the clear definition of what constitutes a startup, facilitating access to incentive and financing programs, the establishment of public procurement mechanisms that favor the participation of startups, such as the contracting modality through technological challenges, tax incentives and facilitated access to investments for startups in early stages. The creation of regulatory sandboxes allows the experimentation of new technologies and business models in a controlled environment, mitigating regulatory risks and promoting innovation. A practical example is the regulatory sandbox of the Central Bank of Brazil, which allowed financial startups to develop and test new digital payment solutions.<sup>19</sup>

In 2020, the Federal Government launched an essential guide for sustainable and innovative urban development in Brazil, the Brazilian Charter for Smart Cities <sup>20</sup>. Developed collaboratively, the Charter seeks to integrate digital transformation with sustainable urban development, addressing issues such as reducing inequalities, digital inclusion, innovative urban governance and local economic development.

The Charter establishes fundamental guidelines that guide the development of smart cities. Among these guidelines, it is important to have specific legislation aimed at implementing smart technologies in Brazilian cities. The legislation must be robust and capable of integrating ICTs in a way that promotes sustainability, social inclusion and urban efficiency.

Legislation plays a crucial role in creating an environment conducive to the adoption and development of smart technologies. It provides the necessary legal basis for cities to integrate ICTs into their urban processes, facilitating resource management, the provision of public services and the promotion of digital inclusion.

To address urban and social challenges, the Charter highlights that it is essential that digital transformation be accompanied by public policies that guarantee equity and sustainability. This includes promoting internet accessibility, personal data protection, citizen participation and transparent governance. The Charter integrates the urban development and digital transformation agendas to define a Brazilian concept for

19. AMATO, Lucas Fucci; MISSAGIA, Caio Rezende. Experimental regulatory environments: the sandbox in the Brazilian financial system. *RBSD – Brazilian Journal of Sociology of Law*, v. 10, n. 3, p. 143-171, Sep./Dec. 2023.

20. Ministry of Regional Development. *Brazilian Charter for Smart Cities*. Brasilia, 2021.

smart cities, present an articulated public agenda and support municipalities in their local actions.

Since 2021, Bill (PL) No. 976 has been in progress, which aims to establish a National Smart Cities Policy (PNCI). This bill aims to improve the quality of life in municipalities and establishes the principles and guidelines that guide this policy, in addition to defining its objectives, actions to be carried out and allocable resources. The bill was sent to the Constitution, Justice and Citizenship Committee of the Chamber of Deputies on July 11, 2022, where it remains awaiting the rapporteur's opinion.

According to the ABNT standard based on ISO 37122 (ABNT, 2021)<sup>21</sup>, a smart city is defined as a city that accelerates the achievement of sustainable results in the social, economic and environmental spheres. In addition, it significantly improves social engagement, applies collaborative leadership, integrates municipal disciplines and systems, and uses data and modern technologies to offer better services and quality of life to its inhabitants (residents, businesses and visitors), both now and in the future, avoiding injustices and environmental degradation.

São José dos Campos (SP) was the first city to receive this certification, on March 16, 2022. To obtain the certification, the city went through a rigorous process that evaluated up to 252 indicators, including sustainability, mobility, health, education and public safety.

The importance of innovative legislation lies in its ability to establish a regulatory framework that not only supports but also promotes the digital transformation of cities in a sustainable and inclusive manner. Global population growth, especially in urban areas, brings significant challenges in the economic, social, organizational and structural spheres. In this scenario, smart cities will be essential to solve the various challenges and meet the demands of large urban areas.

By following the guidelines set out in the Brazilian Charter for Smart Cities and the aforementioned legislation, Brazilian cities can develop in a more balanced way, facing the challenges of the 21st century with technological solutions that improve the quality of life of all citizens. In this context, the role of municipal regulations stands out, such as Law No. 14,746/2023 and Decree No. 16,734/2024, which act in a

21. ABNT NBR ISO 37122:2021. Sustainable cities and communities – Indicators for smart cities. Brazilian Association of Technical Standards, 2021.

complementary to federal frameworks, fostering a robust local innovation ecosystem and applying national guidelines at the municipal level.

### 3. The Juiz de Fora Innovation Law: Structure, Mechanisms and Impacts

Law No. 14,746/2023, which institutes the Juiz de Fora Innovation System, establishes a series of objectives and guidelines to promote technological innovation, sustainable development and economic competitiveness in the city. This legislation aims to create an environment conducive to the growth of startups, technology companies and technology-based cooperatives, providing the financial, structural and regulatory support necessary for the development of new technologies and business models.

Among the main objectives of the law, the need to stimulate, organize and support innovation ecosystems and mechanisms in Juiz de Fora and the region stands out. Law No. 14,746/2023 was regulated by three main decrees: Decree No. 16,372/2024<sup>22</sup>, which provides for the composition and attributions of the Municipal Council for Development, Technology and Innovation (COM-DETI); Decree No. 16,448/2024<sup>23</sup>, which defines the guidelines for the creation and operation of the Municipal Innovation System (Simi-JF); and Decree No. 16,734/2024<sup>24</sup>, which addresses additional aspects not provided for in previous decrees, including details on co-investment funds, minority participation in special purpose companies, seed capital and the experimental regulatory environment of the sandbox.

The mission of the law, as specified in Art. 1, is to promote startups, sustainable companies, low socio-environmental impact businesses, local production networks and technology-based cooperatives, with the aim of enhancing the competitiveness, cooperation and growth of these organizations, focusing on the generation of innovative products, processes and services and on the transfer and dissemination of technologies.

To achieve these objectives, the law establishes the Municipal Innovation System of Juiz de Fora (Simi-JF) and the Municipal Fund for the Development of

22. JUIZ DE FORA. Decree No. 16,372, of January 30, 2024. Regulates arts. 39, 40 and 41 of Municipal Law No. 14,746, of December 4, 2023, which provide for the composition and attributions of the Municipal Council for Development, Technology and Innovation (COMDETI) and provides other measures. *Official Gazette of the Municipality of Juiz de Fora*, Juiz de Fora, MG, January 31, 2024.

23. JUIZ DE FORA. Decree No. 16,448, of March 11, 2024. Regulates arts. 1, 2 (item I) and 6 of Municipal Law No. 14,746, of December 4, 2023, which provides for the creation, composition and purposes of the Municipal Innovation System in Juiz de Fora. *Official Gazette of the Municipality of Juiz de Fora*, Juiz de Fora, MG, March 12, 2024.

24. JUIZ DE FORA. Decree No. 16,734, of September 11, 2024. Provides for the municipality's innovation system and other measures. *Official Gazette of the Municipality of Juiz de Fora*, Juiz de Fora, MG, September 12, 2024.

Innovation (FMDI) as the main support instruments, as detailed in Art. 2. These mechanisms are essential to provide financial and structural support to innovation initiatives, ensuring that projects have the necessary resources for their development and implementation. Capacity building and social inclusion are also priorities of the law, with Art. 3 emphasizing the importance of equipping the municipal production system with additional human resources and specific technologies. In addition, the law aims to support programs and projects that promote innovation, social inclusion, renewable energy, environmental preservation and the mitigation of socio-environmental impacts, fostering models of sustainable cities.

The FMDI, as provided for in Article 2, II, is a fundamental financial instrument to support innovation projects in the municipality. This fund is intended to support projects that promote science, technology and innovation, providing resources for the development of new innovative products, processes and services. FMDI resources are used to subsidize technological bonuses, research grants in innovation, technological orders, acquisition of innovative management systems, scientific-technological training projects, and organization and participation in events related to science, technology and innovation, as per Article 21.

The law introduces the possibility of participation by the City of Juiz de Fora and its agencies, foundations and controlled companies in co-investment funds and special purpose companies. These funds are registered with the Brazilian Securities and Exchange Commission (CVM) and aim to support innovative companies, especially those headquartered in Juiz de Fora and focused on technology. The legislation allows minority participation in the share capital of special purpose companies and technology-based cooperatives, expanding support for the development of scientific and technological projects in the city, as specified in Article 4 of the law. This mechanism allows alignment with the city's strategic innovation priorities, favoring a stronger connection between the public and private sectors.

In addition to co-investment funds, the Law regulates the possibility of seed capital contributions for innovative companies carried out in partnership with Science, Technology and Innovation Institutions (ICTs), following financial and technological impact guidelines. This capital is directed to companies formally included in strategic innovation areas, which present a robust business plan aligned with the economic and social priorities of the municipality. The management and monitoring of these funds and the participation of

The municipality's activities are coordinated by the Municipal Secretariat for Sustainable and Inclusive Development, Innovation and Competitiveness (SEDIC) and the Finance Secretariat.

Another aspect regulated by the Law refers to innovation-promoting environments (APIs), defined by law as financial or virtual spaces designed to foster innovation and entrepreneurship in Juiz de Fora. Among the main innovation-promoting environments, accelerators, incubators, technology parks, innovation ecosystems and Living Labs stand out. Business accelerators, as described in Art. 5, are environments that participate, monitor and invest material and financial resources in startups, receiving compensation such as share capital, royalties and other revenues. Incubators, in turn, are environments that house and monitor startups, offering guidance and support for their graduation, in addition to the infrastructure necessary for their development.

Technology parks and public innovation ecosystems are described by law as areas that enable the integration of scientific and technological research, business and government organizations, providing support for the interrelationships between these groups for the development of innovative products and processes. These innovation environments are also regulated by the decree so that they meet safety, economic and environmental impact criteria.

The regulation of Decree No. 16,734/2024 also presents provisions for the regulatory sandbox, originally introduced in Law No. 14,746/2023. The regulatory sandbox allows companies to develop and test technological innovations in a controlled environment, with temporary authorization, facilitating experimentation while managing the risks associated with new technologies. The Decree establishes clear criteria for the creation and operation of the sandbox, requiring companies to submit substantiated proposals with specific innovation planning, objectives, testing methodologies, timeline and risk assessment. This regulation is essential to ensure that the regulatory sandbox functions as a safe experimental space that encourages innovation.

In terms of governance, Decree No. 16,734/2024 stipulates that COM-DETI and SEDIC will be responsible for supervising projects in the regulatory sandbox, including audits and continuous monitoring, ensuring compliance with performance targets and risk mitigation measures. Authorization to participate in the sandbox is valid for up to 12 months,

and may be extended upon technical justification. The public administration also promotes transparency through the publication of notices, public calls and results of evaluations of innovative projects.

The governance of the innovation system in Juiz de Fora is structured to ensure transparency, effectiveness and oversight of projects funded and incentivized by law. COMDETI plays a central role in the governance of the system. The Management Board of the Municipal Fund for Innovation Development (FMDI) is responsible for planning and applying the fund's resources, as specified in articles 22 to 24. This board is composed of representatives from various municipal departments and civil society, ensuring broad and diverse representation.

Its responsibilities include approving the budgetary and financial programming of FMDI resources, evaluating and approving projects in the areas of Economic Development, Technology and Innovation that will be financed with FMDI resources, preparing the Annual Resource Application Plan, creating and publishing the annual activity report, and monitoring the application of resources, ensuring legality and transparency in the application of resources granted by the fund, in addition to evaluating the indicators and goals achieved.

The tax incentives provided for in the law, detailed in Articles 25 to 36, include exemptions from ITBI, ISSQN and IPTU for companies located in areas designated as Development and Innovation Hubs. These incentives are intended to encourage the attraction and expansion of technological ventures in the municipality, creating an environment favorable to innovation and economic growth. Decree No. 16,734/2024 complements these incentives, establishing specific conditions and procedures for granting tax benefits, with a process of analyzing the economic and social impact of the benefited companies.

Law No. 14,746/2023, together with the three regulatory decrees, in particular Decree No. 16,734/2024, establishes a robust framework of development mechanisms and innovation-promoting environments that are essential to foster technological development and economic competitiveness in the municipality. With financial investments, strategic partnerships, and a comprehensive support infrastructure, the legislation in Juiz de Fora creates a favorable environment for the growth of startups, technology companies, and technology-based cooperatives. These efforts are aligned with national and international guidelines, such as the Brazilian Charter for Smart Cities, promoting sustainable and innovative urban development.

## 4. Implementation and Regulation of the Sandbox in Juiz

from outside

With the publication of Decree No. 16,734/2024, the regulation of the Juiz de Fora Innovation Law significantly advances in the implementation of the regulatory sandbox, detailing the necessary conditions for the creation, operation and monitoring of this experimental regulatory environment. Decree No. 16,734/2024 stands out for offering specific and defined guidelines so that companies and innovation institutions can develop and test new technologies in a safe and controlled environment, with the supervision of the public administration.

Chapter VI of Decree No. 16,734/2024 defines the regulatory sandbox as a set of simplified and temporary special conditions that allow companies and institutions to develop, test and implement technological innovations with specific authorization from regulatory agencies. This decree establishes the process for submitting proposals for the sandbox, including both cases of direct request from companies and those made through a public call. Proposals must be presented with specifications of the technology, justification for the creation of the sandbox, expected objectives, test plans, schedule, methodology and risk assessment, ensuring that the public administration can carefully evaluate each project before authorization.

The sandbox selection process is based on criteria established by decree, such as the degree of innovation and originality, the potential economic, social and environmental impact, the technical and economic feasibility of the project, the experience of the proposing team and the alignment with the strategic priorities of the municipality. The evaluation of the proposals is carried out by a technical committee appointed by COMDETI, composed of representatives of the public administration and experts in the relevant areas. This selection system aims to ensure that only projects with high potential for impact are accepted, minimizing the risks associated with experimenting with emerging technologies in an urban environment.

During the participation period, which is initially valid for up to 12 months and may be extended for the same period upon technical justification, companies must submit periodic progress reports, including partial results, challenges faced and recommendations for possible adjustments. Continuous supervision is carried out by the Municipal Secretariat for Sustainable and Inclusive Development, Innovation and Competitiveness (SE-

DIC), together with the Treasury Department and the Department of Digital and Administrative Transformation (STDA). This constant monitoring, including the possibility of audits and technical visits, aims to ensure that projects comply with security and risk mitigation requirements, promoting innovation in a manner aligned with public interests.

The regulation also establishes the responsibilities for maintenance and support of the technologies during the testing period, which are the responsibility of the participating companies. The infrastructure necessary for the implementation of the solutions will be made available by the municipality, as agreed in the terms of collaboration, and the terms of confidentiality and intellectual property will be defined to guarantee the security of the data and information generated. At the end of the testing period, the participating companies must submit a detailed final report, documenting the results, the assessment of the impacts and possible recommendations for the adoption or expansion of the solution.

This detailed regulation represents a significant step forward for the innovation ecosystem in Juiz de Fora. Unlike previous criticism, which pointed to the lack of guidelines for the regulatory sandbox, Decree No. 16,734/2024 offers a robust and transparent framework for conducting regulatory experiments. The regulation responds to concerns raised by authors such as Hollands, Morozov and Bria, Agar and Medina, who warn of the risks of unregulated technological initiatives and their possible instrumentalization by private interests. Through the process of supervision, monitoring and quality control, the decree seeks to ensure that initiatives in the regulatory sandbox are carried out in an inclusive manner, with citizen participation and social responsibility, minimizing the risk that the space for experimentation exclusively benefits private companies or results in the centralization of power.

However, the practical implementation of the sandbox regulation is not without its challenges. The need for ongoing oversight, in addition to rigorous selection criteria and the definition of performance indicators, raises questions about the capacity of human and technical resources to closely monitor all approved projects. The reliance on municipal oversight structures, even with the involvement of multiple departments, may limit the scope and reach of the sandbox, especially as the volume of projects increases. This limitation may affect the efficiency and safety of innovation testing in urban environments if oversight is not structured to accommodate the growth of initiatives.

Another point that deserves attention is the temporality of the authorization. Although the possibility of extension allows flexibility for projects that need more time to conduct tests, it can also generate risks if quality control and compliance with regulations are not maintained throughout the experimentation period. The decree aims to mitigate these risks by requiring periodic reports and audits, but the effectiveness of these measures depends on the administrative capacity to act responsively to the particularities of each project.

The regulation also allows the municipality to evaluate, at the end of the testing period, the adoption or expansion of the innovations tested in the sandbox, considering the results obtained and the recommendations presented. This flexibility is an important feature for urban development, as it allows Juiz de Fora to adopt technological solutions that have been proven to be effective and safe. However, it is essential that adoption decisions be based not only on technical results, but also on social and environmental impacts, ensuring that the renewed technology contributes to collective well-being and not just to private benefits.

The regulatory sandbox regulation in Juiz de Fora, according to Decree No. 16,734/2024, provides the necessary framework for the controlled experimentation of technological innovations in the urban environment. The regulation meets several demands for safety and inclusion, providing a space for innovation that promotes social responsibility and sustainability. However, for this experimental regulatory environment to fully realize its potential, it is essential that the public administration is prepared to implement strict controls, guarantee transparency and ensure that technological development serves the interests of the population, avoiding exclusions or marginalizations.

## Final considerations

Throughout this study, the concept and evolution of smart cities were reviewed, considering their multiple interpretations and the challenges of implementing inclusive and effective urban technologies. Global innovation models and Brazilian legal frameworks were contextualized to identify the essential role of legislation in promoting sustainable and technologically advanced urban environments. The analysis of the Juiz de Fora Innovation Law positions this legislative framework as a catalyst for the development of

local economic and technological development, integrating the city into the principles of smart governance.

An analysis of the Juiz de Fora Innovation Law, together with its specific regulations, reveals a coordinated effort to implement the principles of smart cities, centered on efficiency, sustainability and social inclusion. Through the Municipal Innovation System (Simi-JF) and the Municipal Innovation Development Fund (FMDI), the law provides a robust regulatory framework that aims to create an environment conducive to technological and economic development. This ecosystem seeks to transform the city into a hub of innovation, promoting the creation of products and services that respond to contemporary urban needs.

The introduction of the regulatory sandbox, structured by Decree No. 16.734/2024, represents a significant innovation in this context. By allowing companies and institutions to test new technologies in a controlled and supervised environment, the sandbox materializes the experimentalist principle fundamental to smart cities. This experimentalist approach allows Juiz de Fora to explore technological innovations in a safe manner and in line with public interests, providing a basis for evaluating the impacts of new solutions before their large-scale implementation. In this way, the sandbox contributes to the city's progress towards efficient urban management, promoting the responsible and ethical use of digital technologies.

However, the challenges of this approach are substantial. The need for rigorous selection criteria and inclusive governance highlights the complexity of managing the sandbox in a way that promotes collective benefits and avoids the concentration of power. Ongoing oversight of experimental projects and the definition of specific performance metrics are essential to ensure that the technologies tested in the sandbox truly contribute to urban well-being and social justice. Without robust governance, there is a risk that these innovations will favor private interests at the expense of the inclusive and sustainable goals that guide the concept of smart cities.

In terms of opportunities, the regulatory sandbox positions Juiz de Fora as a pioneering city in Brazil, creating a model for other locations seeking to integrate technology and urban governance in a responsible way. By adopting experimental practices and promoting transparency and citizen participation, the city can ensure that its innovation policies meet

to the demands of the population and reflect the principles of a truly smart city. The experimental regulatory environment also encourages the creation of a constant feedback loop between the public and private sectors, allowing regulatory adjustments based on evidence and promoting economic development that is more aligned with local needs.

Finally, for Juiz de Fora to fully realize the potential of its regulatory framework and sandbox, it will be essential to maintain a commitment to regulatory adaptability and to monitoring the social and environmental impacts of the innovations tested. Juiz de Fora's Innovation Law and its regulations provide the foundation for a city that reconciles technological advances with social justice, but the success of this journey will depend on the ability to continually improve these mechanisms and ensure that innovation is at the service of inclusive and sustainable urban development.

## References

ABNT NBR ISO 37122:2021. *Sustainable Cities and Communities – Indicators for Smart Cities*. Brazilian Association of Technical Standards, 2021.

HAGAR, Jon. *The Government Machine: a Revolutionary History of the Computer*. Cambridge, MA: MIT Press, 2003. viii + 554 p. ISBN: 0-262-01202-2.

AMATO, Lucas Fucci; MISSAGIA, Caio Rezende. Experimental regulatory environments: The sandbox in the Brazilian financial system. *RBSD–Brazilian Journal of Sociology of Law*, v. 10, n. 3, p. 143-171, Sep./Dec. 2023.

ANTONIELLI, Dennys Marcelo; KIRA, Beatriz. Urban Planning of the Future, Data of the Present: Protecting Privacy in the Context of Smart Cities. *Brazilian Journal of Urban and Regional Studies (RBEUR)*, v. 22, e202003, 2020. DOI:<https://doi.org/10.22296/2317-1529.rbeur.202003> .

DUARTE, Fabio; *Unplugging the City: The Urban Phenomenon and its Sociotechnical Controversies* . 1st Edition. New York: Routledge, 2017. eBook. DOI:<https://doi.org/10.4324/9781315523255> . eISBN: 9781315523255.

HOLLANDS, Robert G. Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? *City*, v. 12, no. 3, p. 303-320, 2008. DOI: 10.1080/13604810802479126.

JUIZ DE FORA. Law No. 14,746, of December 4, 2023. Institutes the Juiz de Fora Innovation System; defines the development hubs of the Municipality; provides for the attributions of the Municipal Council for Development, Technology and Innovation (Comdeti) and provides other measures. *Official Gazette of the Municipality of Juiz de Fora*, Juiz de Fora, MG, December 5, 2023.

JUIZ DE FORA. Decree No. 16,372, of January 30, 2024. Regulates articles 39, 40 and 41 of Municipal Law No. 14,746, of December 4, 2023, which provide for the composition and attribution

tions of the Municipal Council for Development, Technology and Innovation (COMDETI) and provides other measures. *Official Gazette of the Municipality of Juiz de Fora*, Juiz de Fora, MG, January 31, 2024.

JUIZ DE FORA. Decree No. 16,448, of March 11, 2024. Regulates arts. 1, 2 (item I) and 6 of Municipal Law No. 14,746, of December 4, 2023, which provide for the creation, composition and purposes of the Municipal Innovation System in Juiz de Fora. *Official Gazette of the Municipality of Juiz de Fora*, Juiz de Fora, MG, March 12, 2024.

JUIZ DE FORA. Decree No. 16,734, of September 11, 2024. Provides for the municipality's innovation system and other measures. *Official Gazette of the Municipality of Juiz de Fora*, Juiz de Fora, MG, September 12, 2024.

MINISTRY OF REGIONAL DEVELOPMENT. *Brazilian Charter for Smart Cities*. Brasilia, 2021.

MEDINA, Eden. *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*. Cambridge: The MIT Press, 2011. ISBN: 978-0-262-01649-0.

MOROZOV, Evgeny; BRIA, Francesca. *The smart city: urban technologies and democracy*. Translated by Humberto do Amaral. 192 p. ISBN: 978-85-7126-046-7.

OECD. *Smart Cities and Inclusive Growth*. 2020. Available at: [https://www.oecd.org/cfe/cities/OECD\\_Policy\\_Paper\\_Smart\\_Cities\\_and\\_Inclusive\\_Growth.pdf](https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf).

QUIRINO, Carina de Castro; HOCAYEN, Helena Gouvêa de Paula; CUNHA, Marcella Brandão Flores da. Regulatory sandbox: experimental instrument available to local Public Administration to support economic development. *Public Directorate of Economics – RDPE*, Belo Horizonte, v. 21, n. 84, p. 9-33, Oct./Dec. 2023.

REIA, Jess; BELLI, Luca (org.). *Smart Cities in Brazil: Regulation, Technology and Rights*. Belo Horizonte, MG: House of Law, 2021. ISBN: 978-85-9530-274-7.

**From Legal Security to  
Technical Security: Decoding  
Themes for Progress  
Technological in the Registry  
Real Estate Electronics**

Louis Henry de Menezes Acioly

Summary: Introduction. 1. Development of the Electronic Real Estate Registry in the Brazilian Legal Scenario. 2. First decoder: The electronic signature and digital acts involving real estate in the public registry. 2.1. Electronic signature: concept and relationship with the Brazilian legal system. 2.2. Acceptability of electronic signatures before the Real Estate Registry. 3. Second decoder: the security of digital document storage and the possibility of using Technology *Blockchain*. 3.1. *Blockchain*: conceptual elements and applications. 3.2. Applicability of Blockchain to the Trusted Repository of Electronic Documents. Final considerations.

## Introduction

Regarding the regulatory environment of new technologies, it is possible to observe the direction of regulatory measures towards new tools and the renewal of social dynamics, as occurs with *Internet of Things (IoT)*, the platformization of services and generative artificial intelligence. However, we cannot ignore the fact that technological evolution has implications for exhaustively systematized sectors, raising questions about how to align old standards with the current scenario.

This concern is very well expressed by Professor Lyria Bennett Moses<sup>2</sup>, for whom the standardization incident on technology is also a matter that affects the problem of regulatory disconnection, when new techniques are presented in a regulated space in a way that changes the very nature of the activity, promoting the need for regulatory adaptation. This is the case of the real estate market and property registration.

Extrajudicial offices and the royal folio system are of vital importance for the legal security and publicity of real rights, contributing to social pacification, and as such, they have also been inserted into the digital age. Thus, the challenge arises of the appropriate way to enable legal security, the object of real estate registration, in compatibility with technical security in the use of new technologies.

To this end, two themes are decoders of technological advances in real estate registration: the acceptability of different types of electronic signatures

1. Postgraduate student in Digital Law (Specialization) at the Institute of Technology and Society (ITS) and the Center for Studies and Research in Legal Education (CEPED) at UERJ. Graduated in Law from the Ruy Barbosa University Center - UniRuy. Research Coordinator of the Study Group on Technology, Information and Society - GETIS/CNPq. Lawyer. Contact at: acioly10@gmail.com .

2. MOSES, Lyria Bennett. How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target. *Law, Innovation and Technology*, v. 5, n. 1, p. 1-20, 2013.

electronics to guarantee the authenticity of native-digital documents; and the security parameters of documents archived electronically, especially in the Reliable Electronic Document Repository (RCDE), being the *blockchain* a possible relevant auxiliary technology. The research problem is the technical-legal delimitation of the authenticity requirements and elements of confluence of the electronic registration of real estate with the *Blockchain*.

This study seeks to outline the current legal panorama of the insertion of real estate registration in the digital environment, with emphasis on the Electronic Real Estate Registration System (SREI) and from the perspective of decoding themes. To this end, it is essential to understand the evolutionary framework of the SREI, the horizon of electronic signatures for acts involving real estate in public registries and the technical framework in which the *Blockchain* is founded. This research consolidates two constructive arguments: the first decoder will be analyzed with a focus on the existing normative structure; and the second decoder will be evaluated based on its confluence with technological possibilities, that is, the *Blockchain*.

To this end, we proceeded methodologically from a critical review of the reference literature on the subject, to materialization in a descriptive bibliographic and documentary research, qualitative in nature and exploratory in nature, in which dialogue between authors from different areas of social sciences was advocated. A literary review was undertaken here, materialized through a bibliographic research, whose data collection took place through books, dissertations and articles, deposited in electronic databases – *Scientific Electronic Library Online* (SciELO), *Index Law Journals* and *Google Scholar* –, having as descriptors: “electronic signature”; “electronic registration”; “electronic real estate registration system”; “*blockchain*”; “*smart contracts*”.

## 1. Development of the Electronic Real Estate Registry in Brazilian Legal Scenario

Unlike other activities, in which regulation comes as a follow-up, Brazilian real estate registration, for the most part, has had its development as a result of regulatory advances, in light of the constant improvement of legal and archival techniques. This was the case with Federal Law No. 6,015 of 1973, which instituted the real folio system, in which registration was given precedence as the core of the registration activity.<sup>3</sup>

3. RIBEIRO, Moacyr Petrocelli de Ávila. Registration: Paradigms for the Electronic Real Estate Registration System. *Real Estate Law Journal*, a. 42, vol. 86, p. 215-262, Jan./Jun. 2019.

This technical and legal improvement occurred as a reaction to the transcription system which, as Fioranelli asserts,<sup>4</sup> made it mandatory to repeat the characterization of the registered property each time its ownership was transferred or in any other way it was encumbered. With the registration system, properties began to have a concentrated record, making the entire chain of ownership of the property appear<sup>5</sup>, as well as its reality, observing the appropriate objective qualification and structural modifications<sup>6</sup>.

The efficiency and effectiveness of this system provided the basis for the expansion of real estate registration, giving the registrar the leading role in protecting property rights based on the quality of information linked to the real estate registration.<sup>7</sup> However, in contemporary society *hyperinformation*<sup>8</sup>, the *Internet* has assumed the role of protagonist in social relations, promoting changes in cultural, economic, legal and governmental terms<sup>9</sup>.

However, it is important to highlight the depth of the theme “Government as a Platform”<sup>10</sup>, the remodeling of the provision of public services through *Internet*. It also reached the real estate registry, notably from Federal Law No. 11,977, of 2009. This diploma gave light to the possibility of receiving and issuing electronic documents, as long as the requirements of the Brazilian Public Key Infrastructure – ICP Brasil and the e-PING architecture are observed.

Federal Law No. 11,977 of 2009 also established the duty of public registry services to establish an “electronic registry system”, according to its own regulations. Following this line, the National Council of Justice issued its Recommendation No. 14 of 2014 to guide the General Inspectorates of Justice of the respective Federation Units,

4. FIORANELLI, Ademar. Registration in the real estate registry: practical issues. *In*: YOSHIDA, Consuelo Yatsuda Moromizato Yoshida; FIGUEIREDO, Marcelo. AMADEI, Vicente de Abreu (coords). *Advanced notarial and registration law*. São Paulo: Courts Magazine, 2014.

5. CASTRO, Manuella Santos. *Real Estate Registration in the Digital Age*: Impacts of new technologies on the Brazilian registry system. 2021, 306 p. Thesis (Doctorate) - Faculty of Law, USP, São Paulo, 2021.

6. RIBEIRO, Moacyr Petrocelli de Ávila. Registration: Paradigms for the Electronic Real Estate Registration System. *Real Estate Law Journal*, a. 42, vol. 86, p. 215-262, Jan./Jun. 2019.

7. RIBEIRO, Moacyr Petrocelli de Ávila. Registration: Paradigms for the Electronic Real Estate Registration System. *Real Estate Law Journal*, a. 42, vol. 86, p. 215-262, Jan./Jun. 2019.

8. MADALENA, Juliano. Regulation of Internet Borders: a first step towards a General Theory of Digital Law. *In*: MARTINS, GM; LONGHI, JVR (coords.). *Digital Law*. Private Law and the Internet. 2nd ed. Indaiatuba: Foco, 2019. p. 183-206.

9. CASTELLS, Manuel. *The network society*. Translated by Roneide Venâncio Majer. 6th ed. New York: Routledge, 2002.

10. As Faleiros Júnior explains, the “Government as a Platform” theory is based on a study developed by O’Reilly and refers to the “state duty to promote the implementation of technological infrastructure aimed at facilitating interaction between different agents, with different purposes” (FALEIROS JÚNIOR, José Luiz de Moura. Innovation, development and the Digital Government Law (Law No. 14,129/2021): perspectives on government structures as a platform. *Innovate Law* - *UEMG Law Journal*, Belo Horizonte, v. 1, no. 1, p. 1-29, Jan./Jun. 2022, p. 6; O’REILLY, Tim. Government as platform. *Innovations: Technology, Governance, Globalization*, Cambridge, vol. 6, no. 1, p. 13-40, 2011).

in the implementation of an “electronic real estate registration system”<sup>11</sup>.

Recommendation No. 14 of 2014 established that the parameters defined by the Association of the Laboratory of Technological Integrable Systems should be observed in the implementation of this system, without providing further definitions.<sup>12</sup>

However, the General Inspectorate of Justice of São Paulo (CGJ-SP) had already published, in 2012, its Provision no. 42, providing guidelines for the implementation of the Electronic Real Estate Registry System (SREI) in that State, giving shape to the Shared Electronic Services Center of Real Estate Registrars as an access point to real estate registry services through the *Internet*<sup>13-14</sup>. In light of this rule, the development, operation and administration of SREI in the state of São Paulo would be the responsibility of ARISP

– Association of Real Estate Registrars of São Paulo<sup>15-16</sup>.

Not long ago, the National Council of Justice issued the Provision No. 47, of 2015, to outline the technical and legal guidelines that should be observed in the implementation of the Electronic Real Estate Registration System (SREI) within each State and the Federal District<sup>17</sup>. Based on this standard, the creation of shared electronic service centers was promoted, managed locally, through a normative act promoted by each General Inspectorate of Justice<sup>18</sup>. Provision No. 47 of 2015, of the CNJ, brought the need for uniformity of electronic centers in each of the States.

11. GRUBER, Rafael Ricardo. Electronic Real Estate Registry, Cadastres and SINTER: Interconnection without Submission. *Real Estate Law Journal*, a. 39, v. 81, p. 253-287, Jul./Dec. 2016; CASTRO, Manuella Santos. *Real Estate Registration in the Digital Age: Impacts of new technologies on the Brazilian registry system*. 2021, 306 p. Thesis (Doctorate) - Faculty of Law, USP, São Paulo, 2021.

12. ASSAD, Frederico Jorge Vaz de Figueiredo. Electronic property registration and land governance. *Real Estate Law Journal*, a. 39, v. 81, p. 215-234, Jul./Dec. 2016; TAVARES, Ramos André. The National Operator of the Electronic Real Estate Registration System: Response to the Constitutional Requirement for an Efficient Registration System. *Electronic Newspaper Migalhas*, v. 136, p. 23-42, 2018.

13. In light of the aforementioned diploma, the modules that should be offered by the Central Registry Office would be: I - Electronic Office; II - Electronic Seizure of Real Estate (Online Seizure); III - Digital Certificate; IV - Online Registration; V - Electronic Search; VI - Electronic Title Protocol (e-Protocol); VII - Reliable Electronic Document Repository (RCDE); VIII - Online Registry Monitoring; IX - Registry Monitor; X - Online Correction (Monitoring, control and inspection); and XI. - Urban Land Regularization Registry. This same structure was maintained in the Shared Electronic Service (SAEC), with the pertinent improvements and inclusions, constituting the skeleton of the “front-end” of the entire Electronic Property Registry.

14. ASSAD, Frederico Jorge Vaz de Figueiredo. Electronic property registration and land governance. *Real Estate Law Journal*, a. 39, v. 81, p. 215-234, Jul./Dec. 2016; CASTRO, Manuella Santos. *Real Estate Registration in the Digital Age: Impacts of new technologies on the Brazilian registry system*. 2021, 306 p. Thesis (Doctorate) - Faculty of Law, USP, São Paulo, 2021.

15. *Verbatim*: “258. The Electronic Real Estate Registration Service (SREI) will be provided to external users through a single platform on *Internet* which will operate on the Electronic Portal of the Shared Electronic Services Center of Real Estate Registrars (Central Real Estate Registrars), developed, operated and administered by the Association of Real Estate Registrars of São Paulo (ARISP) (...)”.

16. ASSAD, Frederico Jorge Vaz de Figueiredo. Electronic property registration and land governance. *Real Estate Law Journal*, a. 39, v. 81, p. 215-234, Jul./Dec. 2016; CASTRO, Manuella Santos. *Real Estate Registration in the Digital Age: Impacts of new technologies on the Brazilian registry system*. 2021, 306 p. Thesis (Doctorate) - Faculty of Law, USP, São Paulo, 2021.

17. GRUBER, Rafael Ricardo. Electronic Real Estate Registry, Cadastres and SINTER: Interconnection without Submission. *Real Estate Law Journal*, a. 39, vol. 81, p. 253-287, Jul./Dec. 2016.

18. *Verbatim*: “Art. 3. The exchange of electronic documents and information between real estate registry offices, the Judiciary, the Public Administration and the general public will be the responsibility of shared electronic service centers that will be created in each of the States and in the Federal District. § 1. The shared electronic service centers will be created by the respective real estate registry officers, through a normative act of the local General Inspectorate of Justice.”

states and the Federal District, also requiring coordination between them, so that the provision of the registry service is standardized<sup>19</sup>.

The pulverization of state electronic exchanges was, however, contrasted by the need to consolidate a universal access point through *Internet*, as well as interoperability inherent to the various technical layers involved in the provision of real estate registration services at a national level. Combined with the need to provide effectiveness to the land regularization policy, this context gave rise to the text of Federal Law No. 14,365 of 2017, the National Operator of the Electronic Real Estate Registration System (ONR) as responsible for implementing and operating the SREI at a national level<sup>20</sup>.

The diploma provided the general structure for the training<sup>21</sup>, financial support<sup>22</sup> and regulation<sup>23</sup> of the ONR, which would be constituted as a private entity with mandatory links to all real estate registration officers<sup>24</sup>. They do not, therefore, form part of the federal public administration, but have a legal nature. *sui generis*<sup>25</sup>. The General Inspectorate of the CNJ was responsible for issuing Provision No. 89, of 2019, with specific guidelines for the statutory purposes of the ONR and for its performance, designating the implementation and operation of the Shared Electronic Service – SAEC<sup>26</sup>.

With Provision No. 89 of the CNJ, the SREI is now composed of: (i) all real estate registration officers in Brazil; (ii) the Shared Electronic Service (SAEC); and (iii) the shared electronic service centers. Little by little, the state centers lost prominence in relation to the SAEC, which horizontally encompassed a range of activities involved in real estate registration, integrating extrajudicial services on a national level from a single access point in the *Internet*<sup>27</sup>.

19. *Verbatim*: “Art. 3 (...). § 2. There shall be a single shared electronic services center in each of the States and in the Federal District. (...) § 5. The shared electronic services centers shall coordinate with each other so that access to electronic traffic is universalized and the same services are provided throughout the country.”

20. TAVARES, Ramos André. The National Operator of the Electronic Real Estate Registration System: Response to the Constitutional Requirement for an Efficient Registration System. *Electronic Newspaper Migalhas*, v. 136, p. 23-42, 2018.

21. *Verbatim*: “Art. 76. (...) 2nd The ONR will be organized as a private law legal entity, non-profit”.

22. *Verbatim*: “Art. 76 (...) § 9º The fund for the implementation and financing of the SREI is hereby created, which will be managed by the ONR and subsidized by the real estate registration service units of the States and the Federal District referred to in § 5º of this article”.

23. *Verbatim*: “Art. 76. (...) § 4 The National Justice Inspectorate of the National Justice Council shall be responsible for exercising the role of regulatory agent of the ONR and ensuring compliance with its statute”.

24. *Verbatim*: “Art. 76. (...) § 5 The real estate registration service units of the States and the Federal District are part of the SREI and are linked to the ONR”.

25. CASTRO, Manuella Santos. *Real Estate Registration in the Digital Age*. Impacts of new technologies on the Brazilian registry system. 2021, 306 p. Thesis (Doctorate) - Faculty of Law, USP, São Paulo, 2021.

26. CASTRO, Manuella Santos. *Real Estate Registration in the Digital Age*. Impacts of new technologies on the Brazilian registry system. 2021, 306 p. Thesis (Doctorate) - Faculty of Law, USP, São Paulo, 2021.

27. VALERIO, Alexandre Scigliano; BONFATTI, Fabio Fernandes Neves. Possibility of Electronic Signature, Registration and Protest of Agribusiness Credit Titles. *Brazilian Journal of Business Law*, v. 7, no. 2, p. 17-38, Jul./Dec. 2021.

The integration of all real estate registration offices into SAEC<sup>28</sup>, and its prevalence in the face of the fragmentation of state centers, gave new contours to the SREI. The promotion of essentially digital acts was boosted, such as the issuance of electronic certificates and the reception of native-digital documents, linking a complex chain of Real Estate Registry officers to the promotion of a new technological level<sup>29</sup>. This convergence of actions to promote electronic extrajudicial services was consolidated with Federal Law No. 14,382 of 2022, which established the Electronic Public Registry System (SERP), with the aim of integrating other public registry offices, in governance models similar to the coordination of the SREI.<sup>30</sup>

SERP – just like SREI in relation to real estate registration – aims to build an electronic system that makes interoperability between the databases of the registry offices effective, their interconnection and the universality of user service, using technological structures based on *Internet*. To this end, the construction of technical parameters, based on a solid regulatory framework, is essential to enable a safe environment for the development of electronic property registration.

## 2. First decoder: Electronic signature and acts digital records involving real estate in the public registry

The validity of the electronic registration act depends on the guarantee of authenticity of the issuers of the will documented therein, which leads to the recognition of the electronic signature as a pillar of the digital era of notary offices. The electronic protocol of documents by the user of the extrajudicial service is subject to compliance with specific technical and legal rules. The construction of this regulatory framework is, in turn, a thermometer for measuring the fluidity of the debureaucratization-security binomial in the real estate market.

28. It is important to highlight that the integration of all real estate registration offices into the SAEC was the subject of standardization promoted by the National Inspectorate of the CNJ which, with its Provision No. 124 of 2021, established the date of February 15, 2022 as the deadline for the completion of this process.

29. MIRANDA, Caleb Matheus Ribeiro de. Comments on the Electronic Public Records System (SERP) – articles 1 to 9. *In*: KÜMPEL, Vitor (Coord). *Brief comments on Law No. 14,382/2022*. 2nd ed. New York: Routledge, 2013, p. 11-48.

30. Federal Law No. 14,382 of 2022 established that a national operator should be established in the form of a private entity managed by registration officers, in accordance with CNJ regulations. With Provision No. 139 of 2024, the CNJ brought into being the National Operator of the Electronic Public Registry System (ONSERP), composed of the National Operator of the Civil Registry of Natural Persons (ON-RCPN), the National Operator of the Registry of Titles and Documents and Civil Registry of Legal Entities (ON-RTDPJ), also created under this regulation, and the ONR. Provision No. 139 had its guidelines inserted in Provision No. 149 of 2023, of the CNJ. At this point, art. 212, § 2, of the latter, consolidated the shared management structure: “The management of ONSERP will be the responsibility of the Executive Management Committee, composed of the presidents of the national public registry operators, which will operate under the guidance and supervision of the National Justice Inspectorate”.

## 2.1 Electronic signature: conceptualization and relationship with the Brazilian legal system

Electronic contracts do not constitute a new type of agreement, but a specific form of their conclusion, in which information technology means are used to construct the document.<sup>31</sup> However, for the technical validity of an electronic document, some formative elements must be observed: (i) authenticity, in the sense of guaranteeing that its originator is who he claims to be; (ii) integrity, that is, the guarantee that the received document is identical to the originally created document; (iii) confidentiality, that is, the guarantee that no unauthorized person can access its content; and (iv) non-repudiation, that is, the impossibility of the issuer denying that he produced the document.<sup>32</sup>

The electronic signature<sup>33</sup> plays, in this context, the role of giving authenticity and integrity to the document, so that non-repudiation arises from a presumption given by the legal system, validating the act according to the level required for the signature<sup>34</sup>. The Brazilian legal system embraced the acceptability of electronic signatures with Provisional Measure No. 2,200-2, of 2001, which incorporated guidelines from the Model Law of *United Nations Commission on International Trade Law-UNCITRAL*<sup>35</sup>.

The UNCITRAL Model Law establishes two parties necessary for the functioning of Public Identification Keys: (i) the signatory ("*signatory*"), the person responsible for creating the electronic signature; and (ii) the trusted party ("*relying party*"), person responsible for checking and accepting or not this

31. MENKE, Fabiano. The form of electronic contracts. *Journal of Contemporary Civil Law*, São Paulo: Courts Review, a. 8, v. 26, p. 85-113, Jan./Mar. 2021.

32. PINHEIRO, Patricia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. *Fundamentals of Digital Business and Contracts*. 2nd ed. São Paulo: Revista dos Tribunais, 2021; SOTTANO, Augusto; LAGO, Ivan Jacopetti. Electronic signatures and real estate registration: current state of the issue. In: GALHARDO, Flaviano; PARO, John P.; NALINI, Jose R.; BRANDELLI, Leonardo (org.). *Registration Law and New Technologies*. Rio de Janeiro: Forensic, 2021.

33. An electronic signature is understood as a mathematical summary computationally calculated using asymmetric key technology. In Asymmetric Key Cryptography, a pair of keys work together, so that one key encrypts and the other decrypts. The private key is kept under the exclusive control, knowledge and use of the signatory and the public key is freely distributed. *hashing*, in turn, transforms data of any size into a fixed-size data block, so that when any information in the document's original data is changed, a new one is obtained. *hash*, completely different from the previous one. The issuer of the signature, in this case, sends the original document and the *hash* of the document encrypted by the private key, while the receiver uses the public key to decrypt the *hash*, calculate the *hash* of the document and validate both *hash* by comparison. There being identity between the two *hash*, a valid electronic signature is obtained, denoting authenticity to the digital document. This procedure is capable of authenticating the signature, granting integrity to the native-digital document. After its completion, it is possible to provide an additional layer of security from a digital certificate, verified by a Certifying Authority, which affixes a Digital Certificate (PINHEIRO, Patricia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. *Fundamentals of Digital Business and Contracts*. 2nd ed. New York: Courts Review, 2021).

34. LEITE, Clarisse Frechiani Lara. Electronic signature. *Process Journal*, São Paulo: Courts Review, a. 48, v. 345, p. 79-121, Nov. 2023.

35. MENKE, Fabiano. The form of electronic contracts. *Journal of Contemporary Civil Law*, São Paulo: Revista dos Tribunais, a. 8, v. 26, p. 85-113, Jan./Mar. 2021; SOTTANO, Augusto; LAGO, Ivan Jacopetti. Electronic signatures and real estate registration: current state of the issue. In: GALHARDO, Flaviano; PARO, John P.; NALINI, Jose R.; BRANDELLI, Leonardo (org.). *Registration Law and New Technologies*. Rio de Janeiro: Forensic, 2021; LEITE, Clarisse Frechiani Lara. Electronic signature. *Process Journal*, New York: Courts Review, v. 48, p. 79-121, Nov. 2023.

signature. The standard also described a third party, of an optional nature, concerning an agent responsible for certifying the holder of this signature, and this third party may or may not be a public agent (“*certification authority*” or “*certification services provider*”)<sup>36</sup>.

Provisional Measure No. 2200-2 of 2001, when incorporating the UNCITRAL Model Law, provided for the coexistence of two models of recognition of the validity of the signature.<sup>37</sup> The first model with three parts<sup>38</sup>, concerns the Brazilian Public Key Infrastructure (ICP-Brasil), whose role as Root Certification Authority is assigned to the National Institute of Information Technology (ITI). The second model<sup>39</sup>, with only two figures, concerns certificates that are not issued within the scope of the Brazilian Public Key Infrastructure<sup>40</sup>.

The range of possibilities provided by this device, however, brought doubts and insecurity to citizens when applying electronic signatures, especially in relationships involving the presentation of electronic documents before the Public Authorities.<sup>41</sup> Pointing out directions to fill this gap, Federal Law No. 14,063, of 2020, consolidated three types of electronic signatures: (i) simple signature<sup>42</sup>; (ii) advanced signature<sup>43</sup>; and (iii) qualified signature<sup>44</sup>.

36. SOTTANO, Augusto; LAGO, Ivan Jacopetti. Electronic signatures and real estate registration: current state of the issue. In: GALHARDO, Flaviano; PARO, John P.; NALINI, Jose R.; BRANDELLI, Leonardo (org.). *Registration Law and New Technologies*. Rio de Janeiro: Forensic, 2021.

37. ALVIM, Arruda; CUNHA, Igor Martins da. Electronic signatures in the Brazilian legal system and the relevance of private autonomy: a brief analysis of the validity of electronic documents in light of MP 2.200-2/2001 and Law 14.063/2020. *Process Journal*, New York: Courts Review, v. 48, p. 83-114, New York: RT, Mar. 2023.

38. *Verbatim*: “Art. 10. Electronic documents covered by this Provisional Measure shall be considered public or private documents for all legal purposes. § 1º The statements contained in documents in electronic form produced using the certification process made available by ICP-Brasil shall be presumed to be true in relation to the signatories, in accordance with art. 131 of Law 3,071 of January 1, 1916 - Civil Code”.

39. *Verbatim*: “Art. 10. (...) § 2º The provisions of this Provisional Measure do not prevent the use of another means of proving the authorship and integrity of documents in electronic form, including those that use certificates not issued by ICP-Brasil, provided that it is admitted by the parties as valid or accepted by the person to whom the document is opposed”.

40. PINHEIRO, Patricia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. *Fundamentals of Digital Business and Contracts*. 2nd ed. New York: Courts Review, 2021.

41. ALVIM, Arruda; CUNHA, Igor Martins da. Electronic signatures in the Brazilian legal system and the relevance of private autonomy: a brief analysis of the validity of electronic documents in light of MP 2.200-2/2001 and Law 14.063/2020. *Process Journal*, São Paulo: Courts Review, a. 48, v. 337, p. 83-114, São Paulo: RT, Mar. 2023; LEITE, Clarisse Frechiani Lara. Electronic signature. *Process Journal*, New York: Courts Review, v. 48, p. 79-121, Nov. 2023.

42. *Verbatim*: “Art. 4 For the purposes of this Law, electronic signatures are classified as: I - simple electronic signature: a) the one that allows the signatory to be identified; b) the one that attaches or associates data to other data in electronic format of the signatory”.

43. *Verbatim*: “Art. 4 (...) II - advanced electronic signature: one that uses certificates not issued by ICP-Brasil or another means of proving the authorship and integrity of documents in electronic form, provided that it is admitted by the parties as valid or accepted by the person to whom the document is opposed, with the following characteristics: a) it is associated with the signatory in a unique manner; b) it uses data to create an electronic signature that the signatory can, with a high level of confidence, operate under his/her exclusive control; c) it is related to the data associated with it in such a way that any subsequent modification is detectable”.

44. *Verbatim*: “Art. 4 (...) III - qualified electronic signature: one that uses a digital certificate, in accordance with § 1 of art. 10 of Provisional Measure No. 2,200-2, of August 24, 2001”.

## 2.2 Acceptability of electronic signatures before the Real Estate Registry

When regulating the cases of acceptability of signatures based on certificates not based on ICP-Brasil before the Public Authorities, Federal Law No. 14,063 of 2020 also brought the cases in which this infrastructure would be required.<sup>45</sup> It therefore stated that for acts of transfer and registration of real estate, the qualified form of signature would be required, except for legal exceptions.<sup>46-47</sup> This was revised by Federal Law No. 14,382 of 2022, which amended the Public Records Law to allow the adoption of advanced signatures in public registry acts involving real estate, as regulated by the National Inspectorate of the CNJ<sup>48-49</sup>.

The overcoming of the restriction imposed by Federal Law No. 14,063 of 2020 does not occur only due to the incompatibility of its provisions with Federal Law No. 14,382 of 2022, but also and especially due to the application of the criterion for resolving apparent antinomies between standards of the same hierarchical level. In this sense, it follows that the most recent standard, when incompatible with the previous one, operates its tacit revocation, as stated in the Law of Introduction to the Standards of Brazilian Law (Decree-Law No. 4,657 of 1942).<sup>50</sup>

In this vein, the National Inspectorate of the CNJ presented robust regulations for the handling of electronic signatures under the responsibility of the National Operator of the Civil Registry of Natural Persons (ON-RCPN), based on Provision No. 157 of 2023, which amended the National Code of Extrajudicial Forum Rules to accommodate: (i) the Electronic Authentication System with biographical and biometric data for the identification of internal users

45. ALVIM, Arruda; CUNHA, Igor Martins da. Electronic signatures in the Brazilian legal system and the relevance of private autonomy: a brief analysis of the validity of electronic documents in light of MP 2.200-2/2001 and Law 14.063/2020. *Process Journal*, New York: Courts Review, v. 48, p. 83-114, New York: RT, Mar. 2023.

46. The exceptions provided for in the text of Federal Law No. 14,063, of 2020, were for the registration of acts in the commercial boards (art. 5, § 1, II, "c"), and in the case of the acts being carried out by financial institutions that operate with real estate credit authorized to enter into private instruments with the character of a public deed (art. 17-A).

47. SOTTANO, Augusto; LAGO, Ivan Jacopetti. Electronic signatures and real estate registration: current state of the issue. In: GALHARDO, Flaviano; PARO, John P.; NALINI, Jose R.; BRANDELLI, Leonardo (org.). *Registration Law and New Technologies*. Rio de Janeiro: Forensic, 2021.

48. *Verbatim*: "Art. 17. Any person may request a certificate of registration without informing the official or employee of the reason or interest for the request. § 1º Access to or submission of information to public records, when carried out via the internet, must be signed using an advanced or qualified signature as referred to in art. 4º of Law No. 14,063, of September 23, 2020, under the terms established by the National Justice Inspectorate of the National Council of Justice. § 2º An act of the National Justice Inspectorate of the National Council of Justice may establish hypotheses for the use of an advanced signature in acts involving real estate".

49. LEITE, Clarisse Frechiani Lara. Electronic signature. *Process Journal*, São Paulo: Courts Review, a. 48, v. 345, p. 79-121, Nov. 2023.

50. *Verbatim*: "Art. 2º If it is not intended for temporary validity, the law will remain in force until another modifies or revokes it. § 1º A subsequent law revokes a previous one when it expressly states so, when it is incompatible with it or when it entirely regulates the matter dealt with by the previous law".

and external specialists in all Serp specialties<sup>51</sup>; and (ii) a Civil Registry Public Key Infrastructure (ICP-RC), based on advanced electronic signature<sup>52</sup>.

In this sense, a List of Trusted Electronic Services of the Civil Registry of Brazil was consolidated.<sup>53</sup>(LSEC-RCPN), including the ICP-RC, which recognizes the validity of advanced electronic signatures for acts inherent to electronic documents presented to public registry services, for acts involving real estate, and to enter into private instruments with the character of a public deed by financial institutions that operate with real estate credit.

It should be noted, however, that the protocol of documents in the real estate registry, as well as the conduct of specific registration procedures<sup>54</sup>, may be subject to the formality required by law. In cases where a public deed is required<sup>55</sup>, the role of the notary public is essential. In relation to electronic notarial acts, there is a specific guideline that gives validity to documents signed by means of a notarized certificate (a type of advanced signature) or ICP-Brasil certification in relation to other signatories.<sup>56</sup>

The movement to reduce bureaucracy in real estate registration activities through the acceptance of electronic signatures based on digital certificates not issued by ICP-Brasil ultimately results in greater adherence by society to the extrajudicial service.<sup>57</sup> This is due to the lower cost associated with digital certificates not based on ICP-Brasil, as well as the greater di-

51. *Verbatim*: "Art. 228-C. The IdRC will be considered valid for identifying and authenticating users on all Serp platforms and services, including other registration specialties (...)"

52. *Verbatim*: "Art. 228-E. The ICP-RC will be used to manage the life cycle of public keys for advanced electronic signatures, in accordance with the provisions of art. 38 of Law No. 11,977, of July 7, 2009, and art. 4, II, of Law No. 14,063, of September 23, 2020. § 1 The ICP-RC is not part of the hierarchical chain of ICP-Brasil".

53. *Verbatim*: "Art. 228-F. The LSEC-RCPN will contain data that describes the services accepted as reliable by the ON-RCPN. (...) § 3 The ICP-RC is part of the LSEC-RCPN. § 4 The use of electronic signatures whose root is registered with the LSEC-RCPN is valid for the acts described in art. 38 of Law No. 11,977, of July 7, 2009, art. 17 of Law No. 6,015, of December 31, 1973, and in art. 17-A of Law No. 14,063, of July 14, 2023".

54. In addition to the registration of the documents listed in item I of art. 167 of Federal Law No. 6,015 of 1973, there are also the endorsements contained in item II of the same provision, as well as special procedures, such as, *usucaption* (art. 216-A), area rectification (art. 213) and summons for regularization of payment resulting from a purchase and sale agreement (art. 251-A).

55. In light of art. 108 of the Civil Code, acts aimed at establishing, transferring, modifying or waiving real rights over real estate valued at more than thirty times the highest minimum wage in force in the country must be done by means of a public deed. This rule, however, is relativized for transactions carried out by entities linked to the Housing Finance System (SFH), in accordance with art. 61 of Federal Law No. 4,380 of 1964, and the Real Estate Finance System (SFI), cf. art. 38 of Federal Law No. 9,514 of 1997.

56. ALVARES, Luis Ramon. *The Role of Extrajudicial Notary Offices in the Dynamics of Dejudicialization in Brazil*. 2022, 61 p. Dissertation (Master's) - Postgraduate Program in Law Professional Master's Course, University of Araraquara (UNIARA), Araraquara, 2022.

57. FARIA, Bianca Castellar de; LACERDA, Naurican Ludovico. The efficiency of the Brazilian Real Estate Registry and the impacts of Provisional Measure 1,085/2021. *In*: FIUZA, Cesar Augusto de Castro; MARTOS, Frederico Thales; BORGES, Maria Creusa de Araújo. *Contemporary Civil Law*. Florianópolis: CONPEDI, 2022.

variety of authentication factors that provide multiple layers of security and prevent obsolescence<sup>58</sup>.

This is the decoding key for the advancement of electronic property registration, which promotes greater bureaucracy reduction while ensuring legal security based on a regulatory framework that recognizes the inherent reliability of this type of electronic signature, under the regulated terms.

### 3. Second Decoder: Storage Security digital documents and the possibility of using Blockchain Technology

A second pillar for the insertion of notary offices in the digital age is the security of the storage of native-digital documents. This involves not only preventing unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination, as recommended by Federal Law No. 13,709 of 2018, but also the specific construction of a technical framework that promotes the confidentiality, integrity and availability of the information in the registry.<sup>59</sup>

These rules ended up being developed with an emphasis on Provision No. 74 of 2018, of the National Council of Justice, directed to extrajudicial offices divided into three classes, according to revenue amount. In this sense, there is a regulatory gap regarding the security rules for activities developed within the scope of the SREI and the Reliable Repository of Electronic Documents (RCDE).

However, this is an approach associated with the ONR governance system, which is responsible for establishing technical guidelines for the implementation and coordination of the SREI.<sup>60</sup> The present study therefore sets out to investigate the possibility of using technology *Blockchain* as a possible ally to the technical security of archiving native-digital documents in the Electronic Property Registry.

58. PINHEIRO, Patricia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. *Fundamentals of Digital Business and Contracts*. 2nd ed. New York: Courts Review, 2021.

59. HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. *Information Security Fundamentals*. Based on ISO 27001 and ISO 27002. São Paulo: Brasport, 2018.

60. The ONR is responsible for presenting “suggestions to the National Justice Inspectorate for the publication of technical standardization instructions applicable to the SREI to facilitate the secure operation of the system, the interoperability of data and documents and the longevity of electronic files, as well as the electronic adaptation of the legal-formal requirements involved in the services, aiming to guarantee the authenticity and security of operations carried out with computer documents” (art. 31, II, “d”, of Provision no. 89, of 2019, of the CNJ).

### 3.1 Blockchain: conceptual elements and applications

Commonly associated with “cryptocurrencies” and “*Non-Fungible Tokens*”, the technology *Blockchain* represents an undeniable advance in the security and integrity of information, especially when focusing on the socio-technical context in which the high flow of information affects the various dimensions of society<sup>61</sup>. The *Blockchain* is a technological mechanism that is made possible by the decentralization of data recording in a linked network, a procedure also called *decentralized ledger technology*<sup>62</sup>, as opposed to the centralization of information recording that is common to data flows.

Barbosa<sup>63</sup> brings to light a concept of *Blockchain* as a continually growing list of blocks that are securely linked together through cryptography in a network *peer-to-peer*. Faleiros Junior and Roth<sup>64</sup>, in turn, present the concept of Tapscott and Tapscott<sup>65</sup>, reverberating that the *Blockchain* is based on a set of rules, in the form of distributed calculations, that ensure the integrity of the data in flow, maintaining a shared record in agreement with numerous validators. Each unit of this network stores information, according to its configuration, such as credits, debits or properties, which are verified through consensus with other points<sup>66</sup>.

Decentralization of record is given by a ledger, or “*ledger*”, which receives the information and multiplies it along a complex network of key points<sup>67</sup>, without a centralized or unified registry<sup>68</sup>. There is no hierarchy between the units in the chain, nor is management carried out from a central node, but through a spatial distribution of linear convergence.<sup>69</sup> Each node in this network constitutes a participant, which increases trust through sharing

61. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, v. 21, p. 177-194, 2017.

62. ZETSZCHE, Dirk; BUCKLETY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN -European Banking Institute Working Paper Series 14*, 2017.

63. BARBOSA, Mafalda Miranda. Blockchain and civil liability. In: BARBOSA, MM; BRAGA NETTO, F.; SILVA, MC; FALEIROS JUNIOR, JLM (coords.). *Digital Law and Artificial Intelligence: Dialogues between Brazil and Europe*. Indaiatuba: Foco, 2021, p. 797-824.

64. FALEIROS JUNIOR, José Luiz de Moura; ROTH, Gabriela. How can the use of Blockchain affect Traditional Legal Institutes?. *Legal Journal of the Public Prosecutor's Office of Santa Catarina, Florianópolis*, v. 14, no. 30, p. 39-59, jun./nov. 2019.

65. TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. São Paulo: SENAI-SP, 2016.

66. RASKIN, Max. The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, v. 1, no. 2, p. 305-341, 2017.

67. The idea of a complex network, formed by specific units, is what shapes the conceptualization of *Blockchain*, so that the present study uses the terms “block”, “points”, or “key points” interchangeably, considering that in the context presented here, both can serve the same understanding.

68. BARBOSA, Mafalda Miranda. Blockchain and civil liability. In: BARBOSA, MM; BRAGA NETTO, F.; SILVA, MC; FALEIROS JUNIOR, JLM (coords.). *Digital Law and Artificial Intelligence: Dialogues between Brazil and Europe*. Indaiatuba: Foco, 2021, p. 797-824.

69. ZETSZCHE, Dirk; BUCKLETY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN -European Banking Institute Working Paper Series 14*, 2017.

sharing of the same data. In this circumstance, the addition of participants also gives rise to the addition of validators of the information recorded in the *ledger*<sup>70</sup>. In this vein, the *Blockchain* enshrines the decentralization of information in line with the need for consensus.

The doctrine enshrines five attributes for technology *Blockchain*: (i) distributivity, since each member of the network can infer the totality of the data in flow and its history; (ii) irreversibility, since the records cannot be changed, remaining immutably linked to each recorded transaction that has occurred previously; (iii) *peer-to-peer*, given the direct viability between the *key points* of the network, eliminating the need for an intermediary; (iv) logical programming, due to processing via computer coding; and (v) transparency, as each block is available to any member of the network, even if the data is anonymized<sup>71</sup>. It is the irreversibility that makes the authenticity of the content written in the ledger possible, taking into account the technical burden of its modification.<sup>72</sup>

In the relational context, the use of *Blockchain* is associated with carrying out transactions, by placing a *hasht* to the information pointed out, so that each key point keeps a record of the data flow, in reference to the previous point<sup>73</sup>. The synchronization between the information recorded at the previous and next point maintains the integrity of the data in flow, enabling the transaction.<sup>74</sup> Specifically in the context of cryptoassets, blockchains maintain, in addition to the associated ownership, the date and time record of each transaction carried out, consolidating a chain of ownership.<sup>75</sup>

Here, the validation of the information contained in the ledger is the result of the convergence and consensus of all key points in the chain, as opposed to the centralization of the *ledger* in a trusted intermediary, as occurs in banking transactions<sup>76</sup>. This implies considering that, for a modification not to

70. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, v. 21, p. 177-194, 2017.

71. CHITTENDEN, Tara. *Blockchain: The Legal Implications of Distributed Systems*. The Law Society: London, 2017; BARBOSA, Mafalda Miranda. Blockchain and civil liability. In: BARBOSA, MM; BRAGA NETTO, F.; SILVA, MC; FALEIROS JUNIOR, JLM (coords.). *Digital Law and Artificial Intelligence: Dialogues between Brazil and Europe*. Indaiatuba: Foco, 2021, p. 797-824.

72. NALIN, Paulo; NAGAROLI, Rafaella. Artificial intelligence, blockchain and smart contracts: brief reflections on the new legal design of the contract in the information society. In: BARBOSA, MM; BRAGA NETTO, F.; SILVA, MC; FALEIROS JUNIOR, JLM (coords.). *Digital Law and Artificial Intelligence: Dialogues between Brazil and Europe*. Indaiatuba: Foco, 2021, p. 753-773.

73. DIVINO, Sthéfano Bruno Santos. Smart Contracts: Concepts, Limitations, Applicability and Challenges. *Luso-Brazilian Legal Journal*, a. 4, n. 6, p. 2771-2808, Nov./Dec. 2018.

74. WRIGHT, Aaron; DE FILIPPI, Spring. Decentralized Blockchain Technology and the Rise of Lex Cryptography, *SSRN*, March 10, 2015; CANTALI, Rodrigo Ustároz. Smart Contracts and Contract Law: First Impressions on their Advantages and Limitations. *Luso-Brazilian Legal Journal*, a. 8, n. 3, p. 1529-1599, May/June 2022.

75. RASKIN, Max. The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, v. 1, no. 2, p. 305-341, 2017.

76. ZETSCHE, Dirk; BUCKLEY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN - European Banking Institute Working Paper Series 14*, 2017.

For the authorized action to occur, it is necessary that the action be coordinated with all blocks in the chain, simultaneously, which makes the procedure more difficult.<sup>77</sup>

This panorama expands when we focus on the differentiation between *Blockchain* public and private. In the public blockchain, there is freedom of aggregation by any user, regardless of permission, becoming part of the validation network and contributing to convergence<sup>78</sup>. This model, also known as *Blockchain* non-permissioned, enables the anonymity of its users, while at the same time not defining the number of key points in this chain<sup>79</sup>. In turn, the private blockchain maintains a predetermined parameter of who can join it, the number of users and which ones can effectively contribute to the consensus.<sup>80</sup> In this system – called by Zetsche *et al.*<sup>81</sup> as *allowed*, – there is no anonymity, so that each user's permissions and authenticity can be defined by affixing a digital certificate<sup>82</sup>.

The application of technology *Blockchain* to the "*Smart Contracts*", has resulted in its frank expansion, as it serves as a technical subsidy for robust security in the self-execution of its programming<sup>83</sup>. You *Smart Contracts* is not a specific figure of contract law, but a form of automatic execution of the provisions of an agreement through computer engineering, or a *software*<sup>84-85</sup>. It is a computer program, written

77. GUIMARÃES, Luíza Resende; CASTRO, Maria Clara Versiani de. After all, are smart contracts contracts? Legal nature from a sociological reading. In: CHAVES, NC; COLOMBI, H. (Orgs). *Law and Technology: new models and trends*. Porto Alegre: Fi, 2021, p. 36-64.

78. ZETSCHE, Dirk; BUCKLETY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN -European Banking Institute Working Paper Series 14*, 2017; ALEXANDRE, Marcos Gaspar. *Sharing Economy and Blockchain: Problems and Possible Solutions*, 2018, 105f. Master's Dissertation in Management - Faculty of Economics, University of Coimbra, Coimbra, 2018.

79. VUKOLIC, Marko. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. Proof-of-Work BFT Replication. *Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, v. 9591, p. 112-126, 2016; ALEXANDRE, Marcos Gaspar. *Sharing Economy and Blockchain: Problems and Possible Solutions*, 2018, 105f. Master's Dissertation in Management - Faculty of Economics, University of Coimbra, Coimbra, 2018.

80. PILKINGTON, Marc. Blockchain Technology: Principles and Applications. In: OLLEROS, FX; ZHEGU, M. (eds). *Research Handbook on Digital Transformations*, Cheltenham: Edward Edgar Publishing, 2016.

81. ZETSCHE, Dirk; BUCKLETY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN -European Banking Institute Working Paper Series 14*, 2017

82. ALEXANDER, Marcos Gaspar. *Sharing Economy and Blockchain: Problems and Possible Solutions*, 2018, 105f. Master's Dissertation in Management - Faculty of Economics, University of Coimbra, Coimbra, 2018.

83. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, v. 21, p. 177-194, 2017; CANTALI, Rodrigo Ustároz. Smart Contracts and Contract Law: First Impressions on their Advantages and Limitations. *Luso-Brazilian Legal Journal*, a. 8, no. 3, p. 1529-1599, 2022.

84. It is important to note that, according to Florani, the *Smart Contracts* are a third phase in digital contracting. The first phase concerns electronic contracts, in which there is a mere transposition of the support in which the agreement of wills is recorded. The second stage concerns data-driven contracts, which are positioned as a hybrid between traditional agreements and the automatic filling of information through digital means (FLORANI, Lara Bonemer Rocha. *Smart contracts in business contracts: a study on the possibility and economic viability of its use*. 2020. 163 p. Thesis (doctorate) – Pontifical Catholic University of Paraná, 2020).

85. CANTALI, Rodrigo Ustároz. Smart Contracts and Contract Law: First Impressions on their Advantages and Limitations. *Luso-Brazilian Legal Journal*, a. 8, n. 3, p. 1529-1599, May/June 2022.

in code language, which is structured in algorithms<sup>86</sup> to produce a predetermined result. This concept was devised by Nick Szabó<sup>87</sup>, when seeking to give self-execution to contractual duties upon the occurrence of a triggering event<sup>88</sup>. This product provides a quick response to the conditions in which the software was programmed, making negotiations more rational.

THE *Blockchain* is not essential to the design of a *Smart Contract*, but it is from this that sufficient security is provided so that the execution of contractual duties follows the previously planned form.<sup>89</sup> Recording transactions in the decentralized ledger promotes cohesive validation of data in flow, preventing modification of pre-determined obligations.<sup>90</sup> This schedule of contractual obligations transforms a *ledger* static into a dynamic system capable of executing the business dialectics of a contract<sup>91</sup>. This logic is what provides support for transactions involving cryptocurrencies, based on the recording of the asset's inflow and outflow in wallets protected by asymmetric key encryption.<sup>92</sup> The security inherent in this operation converges with the main demands on the flow of information in the digital age.

86. It is worth noting that "algorithm", although quickly associated with artificial intelligence systems, constitutes a different concept. Algorithms can be conceptualized as a set of instructions, organized sequentially, which determines a command, an order to be executed (MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithmic discrimination: concept, legal basis and typology. *Public Law Journal*, v. 16, n. 90. p. 39-64, Nov./Dec. 2019). It is the programming of commands to be executed by an organism, whether mechanical or computational (ACIOLY, Luis Henrique de Menezes. Reflections on the Use of Artificial Intelligence and Algorithms in Consumer Relations in Light of the General Data Protection Law. *Brazilian Journal of Commercial, Competition, Business and Consumer Law*. Porto Alegre: Lex Magister. v. 48, p. 165-187, Aug./Sept. 2022). Artificial Intelligence, in turn, can be brought as the field of study focused on the construction of systems capable of exhibiting human behaviors, through learning (BIGONHA, Carolina. Artificial Intelligence in Perspective. *Internet Sector Overview*, a. 10, n. 2, p. 1-9, Jul./Oct. 2018). In the context of AI, it is the algorithm that structures the logic for constructing machine learning (ACIOLY, Luis Henrique de Menezes. Reflections on the Use of Artificial Intelligence and Algorithms in Consumer Relations in Light of the General Data Protection Law. *Brazilian Journal of Commercial, Competition, Business and Consumer Law*. Porto Alegre: Lex Magister. v. 48, p. 165-187, Aug./Sept. 2022).

87. SZABO, Nick. Formalizing and Securing Relationships on Public Networks. *First Monday*, v. 2, n. 9, 1997.

88. An example given by Szabó (SZABO, Nick. Formalizing and Securing Relationships on Public Networks. *First Monday*, v. 2, n. 9, 1997), presented by the doctrine is the vending machine, which receives the amount from the user and delivers the chosen product, in a simple way (RASKIN, Max. The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, v. 1, no. 2, p. 305-341, 2017; FLORANI, Lara Bonemer Rocha. *Smart contracts in business contracts: a study on the possibility and economic viability of its use*. 2020. 163 p. Thesis (doctorate) – Pontifical Catholic University of Paraná, 2020; CANTALI, Rodrigo Ustároz. Smart Contracts and Contract Law: First Impressions on their Advantages and Limitations. *Luso-Brazilian Legal Journal*, a. 8, n. 3, p. 1529-1599, May/June 2022).

89. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, v. 21, p. 177-194, 2017; ACIOLY, Luis Henrique de Menezes; OLIVEIRA, Micael Araújo de Souza. Application Spectrum of *Smart Contracts* in Light of Brazilian Contract Law: Brief considerations in the context of objective good faith. *Civilistic Conversations Magazine*, Salvador, v. 2, n. 2, p. 98-121, 2022.

90. ACIOLY, Luis Henrique de Menezes; OLIVEIRA, Micael Araújo de Souza. Application Spectrum of *Smart Contracts* in Light of Brazilian Contract Law: Brief considerations in the context of objective good faith. *Civilistic Conversations Magazine*, Salvador, v. 2, n. 2, p. 98-121, 2022.

91. FLORANI, Lara Bonemer Rocha. *Smart contracts in business contracts: a study on the possibility and economic viability of its use*. 2020. 163 p. Thesis (doctorate) – Pontifical Catholic University of Paraná, 2020.

92. NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009. Available at: <https://bitcoin.org/bitcoin.pdf>. Accessed on: July 1, 2024; FOLLADOR, Guilherme Broto. Cryptocurrencies and tax jurisdiction. *Brazilian Journal of Public Policies*, Brasilia, v. 7, n. 3, p. 79-104, 2017.

## 3.2 Trusted Repository of Electronic Documents and digital storage

Promoting a small leap in reasoning, the insertion of *Blockchain* in the structure of the Brazilian Public Power gained prominence with the *Notarchain*, within the scope of the e-Notary platform, for dissemination via *Internet* of notarial services, associated with Provision No. 100, of 2020, of the National Council of Justice. The *Notarchain* was developed in partnership with IBM, through a technology called "*Hyperledger Fabric*" (Santos, 2022), and constitutes a kind of *Blockchain* private. The *Notarchain* enables different levels of access, according to the permission inherent to the type of user through a digital certificate that guarantees authenticity<sup>93</sup>. In turn, access is restricted to previously authorized users, limiting the number of key points to notaries.

These are cohesive technical parameters that provide sustainability to the delegate's actions in the digital environment, promoting security shared by all blocks in a restricted chain of agents. In another twist, the Reliable Repository of Electronic Documents (RCDE), a specific module of the SAEC, has a similar function, consisting of enabling the storage of electronic documents, *digital* or dematerialized files of powers of attorney, certificates, contracts, mortgage cancellations, public deeds, to support registration acts<sup>94</sup>. These files would then be accessible to any Real Estate Registry Officer, avoiding new requests for documents when the user indicates their submission to the platform.

The RCDE emerged within the scope of the Shared Electronic Service as an initiative associated with compliance with the provisions of art. 10 of Ordinance No. 1,248, of 2023, of the Ministry of Cities, which deals with the declaration of settlement of contracts entered into with resources from the Residential Leasing Fund (FAR) and the Social Development Fund (FDS), within the scope of the National Urban Housing Program (PNHU), administered by Caixa Econômica Federal.<sup>95</sup> The RCDE can be used to store the Settlement and Power of Attorney Terms for these contracts, enabling easy access for registration officers.

93. SANTOS, Gabriel Gonçalves. *Smart Contracts: Concepts, limitations and potential*. 2022, 138f. il. Dissertation (Master's) - Federal University of Minas Gerais, Faculty of Law, Belo Horizonte, 2022.

94. NATIONAL OPERATOR OF THE ELECTRONIC REAL ESTATE REGISTRATION SYSTEM -ONR. *Announcement No. 2, 2024*. Statement of Discharge. Available at: [https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN\\_334%5B1%5D.pdf](https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN_334%5B1%5D.pdf). Accessed on: July 1, 2024.

95. NATIONAL OPERATOR OF THE ELECTRONIC REAL ESTATE REGISTRATION SYSTEM -ONR. *Announcement No. 2, 2024*. Statement of Discharge. Available at: [https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN\\_334%5B1%5D.pdf](https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN_334%5B1%5D.pdf). Accessed on: July 1, 2024.

However, the functionality of consolidating the archiving medium for native-digital documents promotes the reframing of the tool, to give it unique importance in the context of file storage and free access to the Real Estate Registry Officer, serving as a broad support for electronic registration acts. To this end, the *Blockchainprivate* can be used as an archiving technology that combines the security of content unalterability with validation distributed among registration officials, as key points in a complex chain.

## Final Considerations

This article presents issues that are sensitive to the context of technological advancement resulting from the regulatory landscape. It was necessary to investigate the regulatory environment to understand the technical context in which the development of the Electronic Real Estate Registry takes place. To this end, the topics analyzed were key points to understand the dynamics of conducting the digital real estate registry.

When investigating the normative development of the Electronic Real Estate Registry System (SREI), it was possible to understand that its design was not uniform, predictable and systematized since its conception in Federal Law No. 11,977, of 2009, but resulted from a set of norms that successively structured and modeled the activity. It was observed that the SREI, in its current format, presents a solid governance and sustainability structure that enables its operation on a national level, interconnecting real estate registry offices throughout the country and concentrating the digital provision of services in a single access point in the *Internet*, the Shared Electronic Service (SAEC).

The analysis of decoding issues was then carried out. The electronic signature, as a way of providing authenticity and integrity to native-digital documents, developed its acceptability in a similar way to the SREI itself, that is, based on a set of regulations that shaped its use in public registry acts involving real estate. In this context, the prevalence of the qualified signature modality, based on the Brazilian Public Key Infrastructure, has given way to the simultaneous coexistence of this model with the acceptability of the advanced electronic signature. This fosters the debureaucratization and democratization of real estate registration, as advanced signature models allow for diverse authentication factors, ensuring the security of transactions.

In turn, the digital archiving of documents is a subject that is not very well-based on regulatory standards, either because of the inconvenience of technical regulation of the subject, due to the clear risk of legal obsolescence, or because there is already a technical set of information security based on standards and good practices. In this sense, the improvement of the digital archiving model lies in the incorporation of technology *Blockchain*, especially in the context of the Trusted Repository of Electronic Documents with SAEC, shared use by registrars and users.

## Bibliographic References

ACIOLY, Luis Henrique de Menezes. Reflections on the Use of Artificial Intelligence and Algorithms in Consumer Relations in Light of the General Data Protection Law. *Brazilian Journal of Commercial, Competition, Business and Consumer Law*. Porto Alegre: Lex Magister. v. 48, p. 165-187, Aug./Sept. 2022.

ACIOLY, Luis Henrique de Menezes; OLIVEIRA, Micael Araújo de Souza. Application Spectrum of *Smart Contracts* in Light of Brazilian Contract Law: Brief considerations in the context of objective good faith. *Civilistic Conversations Magazine*, Salvador, v. 2, n. 2, p. 98-121, 2022.

ALEXANDER, Marcos Gaspar. *Sharing Economy and Blockchain: Problems and Possible Solutions*, 2018, 105f. Master's Dissertation in Management – Faculty of Economics, University of Coimbra, Coimbra, 2018.

ALVARES, Luis Ramon. *The Role of Extrajudicial Notary Offices in the Dynamics of Dejudicialization in Brazil*. 2022, 61 p. Dissertation (Master's Degree) – Postgraduate Program in Law Professional Master's Degree Course, University of Araraquara (UNIARA), Araraquara, 2022.

ALVIM, Arruda; CUNHA, Igor Martins da. Electronic signatures in the Brazilian legal system and the relevance of private autonomy: a brief analysis of the validity of electronic documents in light of MP 2.200-2/2001 and Law 14.063/2020. *Process Journal*, New York: Courts Review, v. 48, p. 83-114, New York: RT, Mar. 2023.

ASSAD, Frederico Jorge Vaz de Figueiredo. Electronic property registration and land governance. *Real Estate Law Journal*, a. 39, vol. 81, p. 215-234, Jul./Dec. 2016.

BARBOSA, Mafalda Miranda. Blockchain and civil liability. In: BARBOSA, MM; BRAGA NETTO, F.; SILVA, MC; FALEIROS JUNIOR, JLM (coords.). *Digital Law and Artificial Intelligence: Dialogues between Brazil and Europe*. Indaiatuba: Foco, 2021, p. 797-824.

BIGONHA, Carolina. Artificial Intelligence in Perspective. *Internet Sector Overview*, a. 10, no. 2, p. 1-9, Jul./Oct. 2018.

CANTALI, Rodrigo Ustárroz. Smart Contracts and Contract Law: First Impressions on their Advantages and Limitations. *Luso-Brazilian Legal Journal*, a. 8, n. 3, p. 1529-1599, May/June 2022.

CASTELLS, Manuel. *The network society*. Translated by Roneide Venâncio Majer. 6th ed. New York: Routledge, 2002.

CASTRO, Manuella Santos. *Real Estate Registration in the Digital Age: Impacts of new technologies on the Brazilian registry system*. 2021, 306 p. Thesis (Doctorate)–School of Law, University of São Paulo, São Paulo, 2021.

CHITTENDEN, Tara. *Blockchain: The Legal Implications of Distributed Systems*. The Law Society: London, 2017.

DIVINO, Sthéfano Bruno Santos. Smart Contracts: Concepts, Limitations, Applicability and Challenges. *Luso-Brazilian Legal Journal*, a. 4, n. 6, p. 2771-2808, Nov./Dec. 2018.

FALEIROS JÚNIOR, José Luiz de Moura. Innovation, development and the Digital Government Law (Law No. 14,129/2021): perspectives on government structures as a platform. *Inova Jur–Legal Journal of UEMG*, Belo Horizonte, v. 1, no. 1, p. 1-29, Jan./Jun. 2022.

FALEIROS JUNIOR, José Luiz de Moura; ROTH, Gabriela. How can the use of Blockchain affect Traditional Legal Institutes?. *Legal Journal of the Public Prosecutor's Office of Santa Catarina*, Florianópolis, v. 14, no. 30, p. 39-59, jun./nov. 2019.

FARIA, Bianca Castellar de; LACERDA, Naurican Ludovico. The efficiency of the Brazilian Real Estate Registry and the impacts of Provisional Measure 1.085/2021. In: FIUZA, César Augusto de Castro; MARTOS, Frederico Thales de Araújo; BORGES, Maria Creusa de Araújo. *Contemporary Civil Law*. Florianópolis: CONPEDI, 2022.

FIORANELLI, Ademar. Registration in the real estate registry: practical issues. In: YOSHIDA, Consuelo Yatsuda Moromizato Yoshida; FIGUEIREDO, Marcelo. AMADEI, Vicente de Abreu (coords). *Advanced notarial and registration law*. São Paulo: Courts Magazine, 2014.

FLORANI, Lara Bonemer Rocha. *Smart contracts in business contracts: a study on the possibility and economic viability of its use*. 2020. 163 p. Thesis (doctorate) – Pontifical Catholic University of Paraná, 2020.

FOLLADOR, Guilherme Broto. Cryptocurrencies and tax jurisdiction. *Brazilian Journal of Public Policies*, Brasília, v. 7, n. 3, p. 79-104, 2017. Available at: <https://www.publicacoes.uniceub.br/RBPP/article/view/4925/0> . Accessed on: July 1, 2024.

GRUBER, Rafael Ricardo. Electronic Real Estate Registry, Cadastres and SINTER: Interconnection without Submission. *Real Estate Law Journal*, a. 39, vol. 81, p. 253-287, Jul./Dec. 2016.

GUIMARÃES, Luíza Resende; CASTRO, Maria Clara Versiani de. After all, are smart contracts contracts? Legal nature from a sociological reading. In: CHAVES, NC; COLOMBI, H. (Orgs). *Law and Technology: new models and trends*. Porto Alegre: Fi, 2021, p. 36-64.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. *Information Security Fundamentals: Based on ISO 27001 and ISO 27002*. São Paulo: Brasport, 2018.

LEITE, Clarisse Frechiani Lara. Electronic signature. *Process Journal*, New York: Courts Review, v. 48, p. 79-121, Nov. 2023.

MADALENA, Juliano. Regulation of Internet Borders: a first step towards a General Theory of Digital Law. In: MARTINS, GM; LONGHI, JVR (coords.). *Digital Law: Private Law and the Internet*. 2nd ed. Indaiatuba: Foco, 2019. p. 183-206.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithmic discrimination: concept, legal basis and typology. *Public Law Journal*, v. 16, no. 90. p. 39-64, Nov./Dec. 2019.

MENKE, Fabiano. The form of electronic contracts. *Journal of Contemporary Civil Law*, São Paulo: Courts Review, a. 8, v. 26, p. 85-113, Jan./Mar. 2021.

MIRANDA, Caleb Matheus Ribeiro de. Comments on the Electronic Public Records System (SERP) – articles 1 to 9. In: KÜMPEL, Vitor (Coord). *Brief comments on Law No. 14,382/2022*. 2nd ed. New York: Routledge, 2013, p. 11-48.

MOSES, Lyria Bennett. How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target. *Law, Innovation and Technology*, v. 5, n. 1, p. 1-20, 2013. Available at: <http://ssrn.com/abstract=2464750> . Accessed on: June 11, 2023.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009. Available at: <https://bitcoin.org/bitcoin.pdf> . Accessed on: July 1, 2024.

NALIN, Paulo; NAGAROLI, Rafaella. Artificial intelligence, blockchain and smart contracts: brief reflections on the new legal design of the contract in the information society. In: BARBOSA, MM; BRAGA NETTO, F.; SILVA, MC; FALEIROS JUNIOR, JLM (coords.). *Digital Law and Artificial Intelligence: Dialogues between Brazil and Europe*. Indaiatuba: Foco, 2021, p. 753-773.

NATIONAL OPERATOR OF THE ELECTRONIC REAL ESTATE REGISTRATION SYSTEM –ONR. *Announcement No. 2, 2024*. Statement of Discharge. Available at: [https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN\\_334%5B1%5D.pdf](https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN_334%5B1%5D.pdf) . Accessed on: July 1, 2024.

O'REILLY, Tim. Government as platform. *Innovations: Technology, Governance, Globalization*, Cambridge, v. 6, n. 1, p. 13-40, 2011. Available at: <https://direct.mit.edu/itgg/article/6/1/13/9649/Government-as-a-Platform> . Accessed on: June 15, 2024.

O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, v. 21, p. 177-194, 2017.

PILKINGTON, Marc. Blockchain Technology: Principles and Applications. In: OLLEROS, FX; ZHEGU, M. (eds). *Research Handbook on Digital Transformations*, Cheltenham: Edward Edgar Publishing, 2016.

PINHEIRO, Patricia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. *Fundamentals of Digital Business and Contracts*. 2nd ed. New York: Courts Review, 2021.

RASKIN, Max. The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, v. 1, no. 2, p. 305-341, 2017.

RIBEIRO, Moacyr Petrocelli de Ávila. Registration: Paradigms for the Electronic Real Estate Registration System. *Real Estate Law Magazine*, a. 42, v. 86, p. 215-262, Jan./Jun. 2019.

SANTOS, Gabriel Goncalves. *Smart Contracts: Concepts, limitations and potential*. 2022, 138f. il. Dissertation (Master's) – Federal University of Minas Gerais, Faculty of Law, Belo Horizonte, 2022. Available at: <http://hdl.handle.net/1843/57345> . Accessed on: July 1, 2024.

SOTTANO, Augusto; LAGO, Ivan Jacopetti. Electronic signatures and real estate registration: current state of the issue. *In: GALHARDO, Flaviano; PARO, John P.; NALINI, Jose R.; BRANDELLI, Leonardo (org.). Registration Law and New Technologies*. Rio de Janeiro: Forensic, 2021.

SZABO, Nick. Formalizing and Securing Relationships on Public Networks. *First Monday*, v. 2, n. 9, 1997. Available at: <https://doi.org/10.5210/fm.v2i9.548> . Accessed on: July 1, 2024.

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. São Paulo: SENAI-SP, 2016.

TAVARES, Ramos André. The National Operator of the Electronic Real Estate Registration System: Response to the Constitutional Requirement for an Efficient Registration System. *Electronic Newspaper Migalhas*, v. 136, p. 23-42, 2018. Available at: <https://www.migalhas.com.br/arquivos/2018/8/art20180821-03.pdf> . Accessed on: 01. Jul. 2024.

VALERIO, Alexandre Scigliano; BONFATTI, Fabio Fernandes Neves. Possibility of Electronic Signature, Registration and Protest of Agribusiness Credit Titles. *Brazilian Journal of Business Law*, v. 7, no. 2, p. 17-38, Jul./Dec. 2021.

VUKOLIC, Marko. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. Proof-of-Work BFT Replication. *Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, v. 9591, p. 112-126, 2016.

WRIGHT, Aaron; DE FILIPPI, Spring. Decentralized Blockchain Technology and the Rise of Lex Cryptography, *SSRN*, March 10, 2015. Available at: <http://dx.doi.org/10.2139/ssrn.2580664> . Accessed on: July 1, 2024.

ZETSCHE, Dirk; BUCKLEY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN-European Banking Institute Working Paper Series 14*, 2017. Available at: <http://dx.doi.org/10.2139/ssrn.3018214> . Accessed on: July 1, 2024.

## The role of the Central Bank of Brazil in regulating payment fintechs

Victor Call Alvim

Summary: Introduction. 1. The Evolution of Payment Fintechs in Brazil. 2. The Role of the Central Bank of Brazil in Regulating Payment Fintechs. 2.1. Main Regulations and Standards for Payment Fintechs. 3. Challenges and Opportunities in Regulating Payment Fintechs. Final Considerations. References.

## Introduction

Since their emergence, fintechs have played a revolutionary role in the global financial landscape, catalyzing significant transformations through the application of innovative technology. With the ability to disrupt established paradigms, these companies have not only redefined the way financial services are accessed and consumed, but have also provided economic inclusion to previously marginalized segments. This context highlights the importance of understanding not only the exponential growth of fintechs, but also the regulatory challenges and opportunities for innovation that this emerging sector faces.

The rationale for this study lies in the pressing need to explore the impact of fintechs on the Brazilian financial environment. In a country marked by significant banking penetration and rapid adoption of digital technologies, understanding how fintechs are shaping and being shaped by the regulatory and economic context is crucial. This work aims to contribute to a deeper understanding of the dynamics between technological innovation, financial regulation, and financial inclusion, providing relevant insights for policymakers, academics, and professionals in the financial sector.

The central research question of this study is: how are payment fintechs being regulated in Brazil, and how do these regulations influence their ability to promote financial inclusion and technological innovation? This question seeks to investigate not only the challenges faced by fintechs in the Brazilian regulatory context, but also the opportunities that arise with effective and adaptive regulation. By delimiting this problem, the study aims to offer clear and objective answers that contribute to an informed and grounded debate on the future of fintechs in the country.

1. Bachelor of Laws from the Fluminense Federal University -UFF and postgraduate in digital law from ITS Rio in partnership with the State University of Rio de Janeiro -UERJ. Legal Counsel at dLocal Payment Institution.

The objectives of this study include investigating the evolution of payment fintechs in Brazil, addressing the economic, technological and regulatory factors that have driven their growth. The study will examine the different phases of this evolution and how these companies have influenced the national financial landscape. In addition, the study aims to analyze the regulatory challenges faced by fintechs, exploring the rules and regulations that affect their operations in the country. Compliance requirements and the dilemmas faced by fintechs when adapting to a constantly changing regulatory environment will be highlighted, seeking to understand their impact on the development and innovation of the sector.

The methodology adopted in this study will consist of a comprehensive and analytical bibliographic review. Academic sources, reports from financial institutions, regulatory documents and articles from specialized journals will be consulted to map and critically analyze the current state of knowledge on the subject. This approach will allow an integrated synthesis of the available information, providing a solid basis for the analyses and conclusions presented in this scientific article.

## 1. The Evolution of Payment Fintechs in Brazil

Fintech is a term that refers to companies that use innovative technology to offer financial products and services in a more efficient, accessible way, and adapted to the needs of consumers and companies.<sup>2</sup> These companies operate in various segments of the financial market, such as electronic payments, peer-to-peer loans, personal financial management, automated investments, digital insurance, among others. The fintech concept stands out for its ability to disrupt the traditional financial sector, which is generally characterized by more bureaucratic and less agile structures. Fintechs seek to transform users' financial experience through innovative technological solutions, taking advantage of advances such as artificial intelligence, blockchain and big data analysis to offer more efficient, transparent and accessible services.

The emergence and development of payment fintechs represents a significant milestone in the evolution of the global financial sector. Originating from the convergence of technology and finance, fintechs have emerged as disruptive alternatives to traditional financial services models. In the context of

2. WÓJCIK, D. Financial Geography I: Exploring FinTech – Maps and concepts. *Progress in Human Geography*, 45(3), 566-576. 2021.

In Brazil and internationally, there were several driving forces behind this growth, with economic, technological and regulatory factors standing out.<sup>3</sup>

The emergence and evolution of fintechs in Brazil represents a fascinating chapter in the recent history of the financial sector. Fintechs initially gained prominence in the country in the early 2000s, with the growing penetration of the internet and the advancement of mobile technologies. Companies such as PagSeguro and Moip (currently part of the Wirecard group) were pioneers in offering electronic payment solutions and online transaction processing, allowing small merchants and digital entrepreneurs easier access to the financial market.<sup>4</sup>

Since the mid-2010s, the fintech scene in Brazil has expanded significantly. Startups focused on financial services have begun to emerge in a variety of areas, including personal financial management, online credit, automated investments and digital insurance. This growth has been driven by the demand for more accessible and efficient solutions, especially among consumers looking for alternatives to traditional banks.<sup>5</sup>

The regulatory environment also played a crucial role in the evolution of Brazilian fintechs<sup>6</sup>. The Central Bank of Brazil, for example, introduced measures such as Resolution No. 4,282, of 2013, which establishes requirements for the operation of payment institutions, and more recently, in 2020, the creation of the PIX instant payment system, which revolutionized the way financial transactions are carried out in the country, opening up new opportunities for fintechs.

Today, fintechs in Brazil are increasingly integrated into the national financial ecosystem, competing on equal terms with traditional banks in many aspects. They have not only democratized access to financial services, but have also promoted greater efficiency and innovation in the market, contributing to a more dynamic and inclusive financial system for all Brazilians.<sup>7</sup>

3. SILVA, Lucas Leão. LISBON, Erika Farias. FERREIRA, Luciene Braz. VERSIANI, Ângela França. SOUSA, Paulo Renato. CORDEIRO, Marcelo Lisboa. Financial institutions and their relationship with fintechs in Brazil. *Economics & Management Journal*, v. 20, n. 55, 2020.

4. BASTOS, Luiz Felipe Pereira. *Chronology of fintechs in Brazil: a look at the transformation of the financial sector*, 2023. Conclusion work for the Higher Education Course in Business Management Technology. Fatec São Carlos, São Carlos, 2023.

5. MILIAN, Eduardo Z.; SPINOLA, Mauro de M.; CARVALHO, Marly M. Fintechs: A literature review and research agenda. *Electronic Commerce Research and Applications*, vol. 34, p. 100833, 2019

6. LIMA, Talison Layala Praxedes de. Analysis of the regulatory scenario for fintechs in Brazil. Federal Rural University of the Semi-arid Region Center for Applied Social Sciences and Humanities Law course 2020. Available at: <https://repositorio.ufersa.edu.br/server/api/core/bitstreams/754509b9-d274-415f-be7d-c84861ac2bb2/content> Accessed on July 18, 2024.

7. BASTOS, Luiz Felipe Pereira. *Chronology of fintechs in Brazil: a look at the transformation of the financial sector*, 2023. Conclusion work for the Higher Education Course in Business Management Technology. Fatec São Carlos, São Carlos, 2023.

Economically, the emergence of fintechs has been driven by the need for efficiency and accessibility in financial services, especially among segments of the population previously excluded from the traditional banking system. Technologically, advances in digital platforms, cloud computing, big data analytics and artificial intelligence have enabled the creation of agile, personalized and accessible financial solutions. These technologies have not only enabled new business models, but have also transformed the user experience, enabling faster and more secure transactions.<sup>8</sup>

Furthermore, the regulatory environment has played a crucial role in shaping the fintech landscape. In many cases, innovative regulations such as the regulatory sandbox, which provides a controlled environment for testing new products and services, have been instrumental in the development and validation of the solutions proposed by fintechs. On the other hand, traditional regulations often present challenges, requiring significant adaptations from fintechs to comply with security, consumer protection and anti-money laundering requirements.<sup>9</sup>

Throughout the main development phases of fintechs, we observed - a progression from emerging startups to established players in the financial ecosystem. Initially focused on niche areas such as mobile payments and international transfers, fintechs have expanded their operations into areas such as peer-to-peer lending, personal financial management, automated investments and digital insurance. This diversification reflects the adaptive capacity of fintechs to respond to market demands and explore new growth opportunities.

## 2. The Role of the Central Bank of Brazil in Regulating Payment Fintechs

The Central Bank of Brazil was established on December 31, 1964, through the enactment of Law No. 4,595, with the mission of ensuring the stability of the purchasing power of the national currency, maintaining a solid and efficient financial system, and promoting the economic well-being of the population. Over the years, the BCB's mission has evolved to include controlling inflation,

8. LIMA, Talison Layala Praxedes de. Analysis of the regulatory scenario for fintechs in Brazil. Federal Rural University of the Semi-arid Region Center for Applied Social Sciences and Humanities Law course 2020. Available at:<https://repositorio.ufersa.edu.br/server/api/core/bitstreams/754509b9-d274-415f-be7d-c84861ac2bb2/content> Accessed on July 18, 2024

9. DINIZ, Bruno. The Fintech phenomenon: everything about the movement that is transforming the financial market in Brazil and the world. Rio de Janeiro: Alta Books, 2019, p. 31.

regulation of the financial system and the implementation of effective monetary policies<sup>10</sup>.

The structure of the Central Bank of Brazil is composed of several areas and departments, each with specific functions that contribute to the institution's overall mission. The internal organization of the BCB is outlined as follows: the National Monetary Council (CMN), the highest body of the national financial system, responsible for formulating currency and credit policy, is composed of the Minister of Finance, the Minister of Planning, Development and Management and the President of the Central Bank. The Board of Directors, formed by the President of the Central Bank and the Directors, each responsible for a specific area, defines and implements policies to achieve the objectives established by the CMN.<sup>11</sup>

The BCB's departments and functional areas include, among others: the Department of Banking Operations and Payment System (Deban), responsible for managing bank operations and the payment system; the Department of Banking Supervision (Desup), responsible for supervising financial institutions to ensure their soundness and compliance with regulations; the Economic Department (Depec), which conducts economic analyses and monitors macroeconomic indicators; and the Department of Open Market Operations (Demab), responsible for executing open market operations and controlling the liquidity of the financial system.<sup>12</sup>

To achieve its objectives, the Central Bank of Brazil uses several monetary policy instruments. The Selic rate, the basic interest rate of the economy, influences all other interest rates and is used to control inflation and stabilize the currency. Open market operations, which involve the purchase and sale of government bonds, are used to control the amount of money in circulation and maintain the liquidity of the financial system at adequate levels. Compulsory reserves, which correspond to the percentage of deposits that commercial banks are required to maintain at the Central Bank, are used to regulate the supply of credit and the liquidity of the banking system. In addition, interventions in the foreign exchange market aim to

10. CENTRAL BANK OF BRAZIL. Financial stability: fintechs. Brasília, DF: Central Bank of Brazil, 2020a. Available at:<https://www.bcb.gov.br/estabilidadefinanceira/fintechs>. Accessed on July 15, 2024.

11. MENDONÇA, Saulo Bichara; DE PAULA IVO, Felipe. Administrative Council for Economic Defense and Central Bank of Brazil: analysis of the conflict of jurisdiction. *Law Review*, v. 12, n. 1, p. 4, 2020.

12. MISSAGIA, Caio Rezende; AMATO, Lucas Fucci. Experimental regulatory environments: the sandbox in the Brazilian financial system. *Brazilian Journal of Sociology of Law*, v. 10, n. 3, p. 143-171, 2023.

influence the exchange rate and stabilize the currency, protecting the economy from external shocks and exchange rate fluctuations<sup>13</sup>.

The Central Bank of Brazil plays a vital role in the country's economy, being responsible for ensuring economic and financial stability through a well-defined organizational structure and the effective use of various monetary policy instruments. The BCB's mission and functions are essential to fostering a stable economic environment conducive to Brazil's sustainable development.

## 2.1 Main Regulations and Standards for Fintechs Payment

The Central Bank of Brazil has adopted several regulatory initiatives that play a crucial role in supervising payment fintechs. Among the main initiatives, Resolution No. 4,282 of 2013 stands out<sup>14</sup>, which establishes criteria for the authorization and operation of payment institutions. This resolution defines the minimum requirements for capital, corporate governance, internal controls and risk management that must be observed by fintechs to obtain and maintain their operating authorization<sup>15</sup>.

Additionally, the Central Bank instituted Circular No. 3,682, of 2013<sup>16</sup>, which regulates the provision of payment services, establishing specific guidelines for the operation of payment institutions. This standard covers aspects such as the provision of information to users, the protection of customer funds, transparency in fees and the prevention of money laundering and the financing of terrorism. Circular No. 3,682, by promoting

13. SILVA, Christian Feliciano da. Dial 100 – Implementation of regulatory policies: the case of Open Finance from the Central Bank of Brazil. 2023. 42 p., ill. Final Course Work (Bachelor's Degree in Public Policy Management) – University of Brasília, Brasília, 2023.

14. BRAZIL. Ministry of Finance. Central Bank of Brazil. Resolution No. 4,282 of November 4, 2013. Establishes the guidelines that must be observed in the regulation, monitoring and supervision of payment institutions and payment arrangements that are part of the Brazilian Payment System (SPB), as set out in Law No. 12,865 of October 9, 2013. Official Gazette of the Union: section 1, Brasília, DF, year 150, no. 216, p. 16, November 6, 2013c. Available at: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=06/11/2013&jornal=1&pagina=16>. Accessed on: July 18, 2024.

15. OIOLI, Erik Frederico; SILVA, Rafael Toni; ZILIOTI, Matheus. Fintechs and the regulation of the national financial system. In: OIOLI, Erik Frederico (coord.). Law manual for startups. 2nd ed. São Paulo: Thomson Reuters Brasil, 2020, p. 187-210.

16. BRAZIL. Ministry of Finance. Central Bank of Brazil. Circular No. 3,682 of November 4, 2013. Approves the regulation that governs the provision of payment services within the scope of payment arrangements that are part of the Brazilian Payment System (SPB), establishes the criteria according to which payment arrangements will not be part of the SPB, and contains other provisions. Official Gazette of the Union: section 1, Brasília, DF, year 150, no. 216, p. 18-20, November 6, 2013b. Available at: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=06/11/2013&jornal=1&pagina=18>. Accessed on: July 18, 2024.

seeing greater transparency and security in operations reinforces users' trust in the services provided by payment fintechs<sup>17</sup>.

Another important regulatory milestone is the creation of the Brazilian Payments System (SPB), established by Law No. 12,865 of 2013.<sup>18</sup> The SPB establishes the infrastructure necessary for carrying out financial transactions in the country, including electronic payments and fund transfers. By integrating the SPB, payment fintechs begin to operate within a secure and efficient system, which facilitates interoperability between different financial institutions and promotes financial inclusion.

The Central Bank has also implemented the regulatory sandbox concept, as set out in Resolution No. 29 of 2020.<sup>19</sup> The regulatory sandbox allows payment fintechs to test technological innovations in a controlled environment, with supervision and monitoring by the BCB. This initiative aims to foster innovation in the financial sector, while ensuring consumer protection and the stability of the financial system. The regulatory sandbox provides a space for new technologies and business models to be tested and evaluated before their full implementation in the market.

The general term “sandbox” is used in software development strategies and represents an environment isolated from interaction with other systems that allows a new system to operate without interaction with the external environment hindering its development. Brought to the financial environment by fintechs, sandbox

17. Art. 18. Financial institutions may only operate in the country with prior authorization from the Central Bank of the Republic of Brazil or by decree of the Executive Branch, when they are foreign.” (BRAZIL. Law No. 4,595, of December 31, 1964. Provides for Monetary, Banking and Credit Policy and Institutions, Creates the National Monetary Council and provides other measures. Brasília, DF: Presidency of the Republic, [2017], art. 18. Available at: [http://www.planalto.gov.br/ccivil\\_03/leis/L4595compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/L4595compilado.htm). Accessed on: July 18, 2024).

18. “Art. 6 For the purposes of the rules applicable to payment arrangements and institutions that become part of the Brazilian Payment System (SPB), under the terms of this Law, the following are considered: I - payment arrangement - set of rules and procedures that govern the provision of a certain payment service to the public accepted by more than one recipient, through direct access by end users, payers and recipients;” (BRAZIL. Law No. 12,865, of October 9, 2013. Provides for payment arrangements and payment institutions that are part of the Brazilian Payment System (SPB), among others. Brasília, DF: Presidency of the Republic, [2020]. Available at: [http://www.planalto.gov.br/ccivil\\_03/\\_ato20112014/2013/lei/l12865.htm](http://www.planalto.gov.br/ccivil_03/_ato20112014/2013/lei/l12865.htm). Accessed on: July 18, 2024.)

19. In Brazil, the main regulatory framework that allowed the creation of the regulatory sandbox for fintechs was Joint Resolution No. 1, of February 4, 2021. This resolution was issued jointly by the National Monetary Council (CMN), the Central Bank of Brazil (Bacen), the Securities and Exchange Commission (CVM) and the Superintendence of Private Insurance (Susep). The resolution establishes the guidelines for the implementation of the experimental regulatory environment, known as the regulatory sandbox.

Joint Resolution No. 1/2021 defines the criteria and procedures for the selection and monitoring of companies participating in the sandbox, as well as the requirements for entry and exit from this controlled regulatory environment. The initiative aims to promote innovation in the financial sector by allowing fintechs to test new products and services under the supervision of regulators, ensuring consumer protection and the integrity of the financial system.

In addition to this resolution, the Central Bank of Brazil also issued Resolution BCB No. 29, of October 26, 2020, which establishes the specific conditions for the creation and operation of the regulatory sandbox within the scope of Bacen. This resolution details the criteria for the admission of fintechs into the sandbox, the obligations of participating companies and the supervision and control mechanisms.

begins to define a testing environment where financial products and services are tested in isolation and evaluated for their safety and effectiveness before being offered to the public<sup>20</sup>

In terms of security and compliance, the Central Bank establishes strict standards for the protection of customer data and the prevention of illicit activities. The General Data Protection Law (LGPD), enacted in 2018, and the BCB's guidelines on cybersecurity and risk management, as per Resolution No. 4,658 of 2018,<sup>21</sup> impose obligations on payment fintechs to ensure the confidentiality, integrity and availability of user information. These security standards are essential to mitigate risks and ensure consumer trust in the services provided by fintechs.

### 3. Challenges and Opportunities in Fintech Regulation Payment

The regulatory and compliance challenges faced by payment fintechs are substantial and multifaceted. In a constantly evolving financial environment, fintechs need to adapt to a regulatory framework that, while intended to ensure the security and stability of the financial system, can also impose significant barriers to innovation and growth. The need to comply with strict legal and regulatory requirements imposes a considerable burden on these companies, which often operate with more agile and less robust structures than traditional financial institutions.<sup>22</sup>

One of the main regulatory challenges lies in the need to comply with current legislation, which includes complex and detailed rules on money laundering prevention, data protection and cybersecurity. Payment fintechs must implement robust policies and procedures to ensure that their operations comply with Law No. 9,613/1998, which regulates the crimes of “laundering” or concealment of assets,

20. SQUASSONI, Christian. The Regulatory Sandbox and the new role of the financial regulator. In: EROLES, Pedro (coord.). *Fintechs, Digital Banks and Payment Methods: Regulatory Aspects of new Financial Technologies*. São Paulo: Quartier Latin, 2019. p. 157-178.

21. RESOLUTION No. 4,658, OF APRIL 26, 2018 Provides for the cybersecurity policy and the requirements for contracting data processing and storage and cloud computing services to be observed by financial institutions and other institutions authorized to operate by the Central Bank of Brazil.

22. PELLEGRINO, Maria Beatriz. The evolution of sub-accreditors in the Brazilian Payment System (SPB). In: EROLES, Pedro (coord.). *Fintechs, digital banks and payment methods: regulatory aspects of new financial technologies*. São Paulo: Quartier Latin, 2019, p. 109.

rights and values, as well as the General Data Protection Law (LGPD), which establishes guidelines for the processing of personal data. These requirements require significant investments in technology and human resources, in addition to continuous monitoring and updating of internal processes<sup>23</sup>.

Furthermore, regulation poses challenges related to transparency and accountability. Payment fintechs must maintain detailed records of their operations and be prepared to provide accurate and timely information to regulatory authorities. Circular No. 3,682 of 2013 of the Central Bank of Brazil, for example, establishes obligations to provide periodic information, which requires the adoption of efficient and reliable management systems. Failure to comply with these obligations can result in severe sanctions, including substantial fines and, in extreme cases, revocation of the authorization to operate.<sup>24</sup>.

Another relevant challenge is the need for risk management and implementation of adequate internal controls. Payment fintechs operate in a dynamic environment that is susceptible to various forms of risk, including operational, credit and market risks. Resolution No. 4,658 of 2018 of the National Monetary Council, which establishes the cybersecurity policy and the requirements for contracting data processing and storage services, imposes on fintechs the responsibility to adopt measures to mitigate risks and protect the integrity and confidentiality of customer information. Implementing an effective compliance program, which includes regular internal audits and ongoing employee training, is essential to mitigate these risks.<sup>25</sup>.

Furthermore, the regulatory environment can be a source of uncertainty for payment fintechs. The constant evolution of financial technologies and changing consumer expectations often precede the update of regulatory standards. This gap between innovation and regulation can create legal and operational uncertainties, making it difficult for fintechs to predict and strategically plan. The creation of a flexible and adaptable regulatory framework that allows experimentation and testing of new business models in a controlled environment, such as the regulatory sandbox implemented by the

23. SQUASSONI, Christian. The Regulatory Sandbox and the new role of the financial regulator. In: EROLES, Pedro (coord.). *Fintechs, Digital Banks and Payment Methods: Regulatory Aspects of new Financial Technologies*. São Paulo: Quartier Latin, 2019. p. 157-178.

24. OIOLI, Erik Frederico; SILVA, Rafael Toni; ZILIOTI, Matheus. Fintechs and the regulation of the national financial system. In: OIOLI, Erik Frederico (coord.). *Law manual for startups*. 2nd ed. São Paulo: Thomson Reuters Brasil, 2020, p. 187-210.

25. DINIZ, Bruno. *The Fintech phenomenon: everything about the movement that is transforming the financial market in Brazil and the world*. Rio de Janeiro: Alta Books, 2019.

funded by the Central Bank, is a positive response to this challenge, although its effective implementation and scope are still in the process of development.<sup>26</sup>

## Final considerations

Payment fintechs present numerous opportunities to drive innovation and promote financial inclusion in Brazil. Proper regulation, while challenging, also paves the way for a safer and more trustworthy environment where innovation can flourish and new business models can be tested and implemented, benefiting both businesses and consumers.

Technological innovation is one of the biggest opportunities provided by the growth of payment fintechs. With the digitalization of financial services, fintechs can offer more efficient, accessible and convenient solutions. The use of advanced technologies such as artificial intelligence, machine learning and blockchain enables the creation of innovative products and services that meet the specific needs of consumers, improving the user experience and increasing competitiveness in the financial market. The introduction of digital wallets, contactless payments and integrated payment platforms are examples of how fintechs are revolutionizing the sector.

Furthermore, fintechs play a crucial role in promoting financial inclusion. In Brazil, a significant percentage of the population is still unbanked or underbanked, facing difficulties in accessing traditional financial services. Payment fintechs, with their digital solutions, have the ability to reach these marginalized populations, offering them access to basic financial services, such as payment accounts, money transfers and microcredit. This financial inclusion is essential for economic and social development, providing people with greater autonomy and ability to manage their finances.

The regulatory environment also offers significant opportunities for fintechs. The implementation of open banking in Brazil, for example, is an initiative that aims to foster innovation and competition in the financial sector. Open banking allows the secure sharing of financial data between different

26. SQUASSONI, Christian. The Regulatory Sandbox and the new role of the financial regulator. In: EROLES, Pedro (coord.). Fintechs, Digital Banks and Payment Methods: Regulatory Aspects of new Financial Technologies. São Paulo: Quartier Latin, 2019. p. 157-178.

these institutions, with the customer's consent, promoting the creation of new personalized and integrated services. Fintechs can take advantage of this infrastructure to develop more competitive solutions adapted to the needs of consumers, improving market efficiency and transparency.

Another important opportunity is the regulatory sandbox, an initiative by the Central Bank that allows fintechs to test technological innovations in a controlled and supervised environment. This experimental space allows new ideas to be evaluated and adjusted before being fully implemented in the market, reducing risks and increasing the chances of success. The regulatory sandbox not only encourages innovation, but also makes it easier for fintechs to adapt to regulatory requirements, promoting a constructive dialogue between regulators and innovators.

The growing demand for sustainable and socially responsible solutions also presents opportunities for payment fintechs. Fintechs can develop financial products that promote environmental sustainability and positive social impact, aligning with the expectations of modern consumers and investors. Examples include investment platforms for sustainable projects, microcredit services for small businesses, and financial education initiatives. By integrating social responsibility criteria into their operations, fintechs can earn the trust of consumers and contribute to more equitable and sustainable development.

In conclusion, payment fintechs in Brazil have a wide range of opportunities to drive innovation and promote financial inclusion. The digitalization of financial services, the promotion of open banking, the use of the regulatory sandbox and the development of sustainable solutions are just some of the ways in which fintechs can transform the financial market. Adequate regulation, far from being an obstacle, can be a catalyst for innovation and growth, creating an environment where fintechs can thrive and offer significant benefits to society.

## References

CENTRAL BANK OF BRAZIL. Financial stability: fintechs. Brasília, DF: Central Bank of Brazil, 2020a. Available at: <https://www.bcb.gov.br/estabilidadefinanceira/fintechs> . Accessed on July 15, 2024.

BASTOS, Luiz Felipe Pereira. Chronology of fintechs in Brazil: a look at the transformation of the financial sector. Conclusion work of the Higher Education Course in Business Management Technology. Fatec São Carlos, São Carlos, 2023.

BRAZIL. Law No. 12,865, of October 9, 2013. Provides for payment arrangements and payment institutions that are part of the Brazilian Payment System (SPB), among others. Brasília, DF: Presidency of the Republic, [2020]. Available at:[http://www.planalto.gov.br/ccivil\\_03/\\_ato20112014/2013/lei/l12865 . htm](http://www.planalto.gov.br/ccivil_03/_ato20112014/2013/lei/l12865.htm). Accessed on: July 18, 2024.)

BRAZIL. Law No. 4,595 of December 31, 1964. Provides for Monetary, Banking and Credit Policy and Institutions, Creates the National Monetary Council and contains other provisions. Brasília, DF: Presidency of the Republic, [2017], art. 18. Available at:[http://www.planalto.gov.br/ccivil\\_03/leis/L4595compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/L4595compilado.htm) . Accessed on: July 18, 2024).

BRAZIL. Ministry of Finance. Central Bank of Brazil. Circular No. 3,682, of November 4, 2013. Approves the regulation governing the provision of payment services within the scope of payment arrangements that are part of the Brazilian Payment System (SPB), establishes the criteria according to which payment arrangements will not be part of the SPB, and contains other provisions. Official Gazette of the Union: section 1, Brasília, DF, year 150, no. 216, p. 18-20, November 6, 2013b. Available at:<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=06/11/2013&jornal=1&pagina=18> . Accessed on: July 18, 2024.

BRAZIL. Ministry of Finance. Central Bank of Brazil. Resolution No. 4,282 of November 4, 2013. Establishes the guidelines that must be observed in the regulation, monitoring and supervision of payment institutions and payment arrangements that are part of the Brazilian Payment System (SPB), as set out in Law No. 12,865 of October 9, 2013. Official Gazette of the Union: section 1, Brasília, DF, year 150, no. 216, p. 16, November 6, 2013c. Available at:<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=06/11/2013&jornal=1&pagina=16> . Accessed on: July 18, 2024.

LIMA, Talison Layala Praxedes de. Analysis of the regulatory scenario for fintechs in Brazil. Federal Rural University of Semiárido. Center for Applied Social Sciences and Humanities Law Course 2020. Available at:<https://repositorio.ufersa.edu.br/server/api/core/bitstreams/754509b-9-d274-415f-be7d-c84861ac2bb2/content> Accessed on July 18, 2024.

MISSAGIA, Caio Rezende; AMATO, Lucas Fucci. Experimental regulatory environments: the sandbox in the Brazilian financial system. *Brazilian Journal of Sociology of Law*, v. 10, n. 3, p. 143-171, 2023.

MENDONÇA, Saulo Bichara; DE PAULA IVO, Felipe. Administrative Council for Economic Defense and Central Bank of Brazil: analysis of the conflict of jurisdiction. *Law Review*, v. 12, n. 1, p. 4, 2020.

MILIAN, Eduardo Z.; SPINOLA, Mauro de M.; CARVALHO, Marly M. Fintechs: A literature review and research agenda. *Electronic Commerce Research and Applications*, vol. 34, p. 100833, 2019

OIOLI, Erik Frederico; SILVA, Rafael Toni; ZILIOTI, Matheus. Fintechs and the regulation of the national financial system. In: OIOLI, Erik Frederico (coord.). *Law manual for startups*. 2nd ed. São Paulo: Thomson Reuters Brasil, 2020, p. 187-210.

PELLEGRINO, Maria Beatriz. The evolution of sub-accreditors in the Brazilian Payment System (SPB). In: EROLES, Pedro (coord.). *Fintechs, digital banks and payment methods: regulatory aspects of new financial technologies*. São Paulo: Quartier Latin, 2019, p. 109.

RESOLUTION No. 4,658, OF APRIL 26, 2018 Provides for the cybersecurity policy and the requirements for contracting data processing and storage services.

data and cloud computing to be observed by financial institutions and other institutions authorized to operate by the Central Bank of Brazil.

SILVA, Lucas Leão. LISBON, Erika Farias. FERREIRA, Luciene Braz. VERSIANI, Ângela França. SOUSA, Paulo Renato. CORDEIRO, Marcelo Lisboa. Financial institutions and their relationship with fintechs in Brazil. *Economics & Management Journal*, v. 20, n. 55, 2020.

SILVA, Christian Feliciano da. Dial 100 – Implementation of regulatory policies: the case of Open Finance from the Central Bank of Brazil. 2023. 42 p., ill. Course Completion Work (Bachelor's Degree in Public Policy Management) — University of Brasília, Brasília, 2023.

SQUASSONI, Christian. The Regulatory Sandbox and the new role of the financial regulator. In: ERO-LES, Pedro (coord.). *Fintechs, Digital Banks and Payment Methods: Regulatory Aspects of new Financial Technologies*. São Paulo: Quartier Latin, 2019. p. 157-178.

WÓJCIK, D. Financial Geography I: Exploring FinTech –Maps and concepts. *Progress in Human Geography*, 45(3), 566-576. 2021.

**Blockchain as  
feminine noun: a  
gender analysis as  
to the rising use of  
blockchain technology**

Carolina Freitas

Summary: Introduction. 1. What will be the values of value technology? 2. How distributed is the distributed finance system? 3. Can we trust the future of women to the technology of trust? Final considerations. References.

## Introduction

For the Priberam Dictionary of the Portuguese Language (DPLP), blockchain, a masculine noun, is “technology that uses a non-centralized database, with information coming from a large network, linked by encryption algorithms, generally used for cryptocurrency transactions.”<sup>2</sup>

The choice of a dictionary translation for masculine, while an interesting grammatical question, serves as a starting point for a deeper question: how masculine is blockchain technology?

It seems that the grammatical choice confirms a reality: blockchain is a system, up until now, built from a male perspective. The article, however, seeks to highlight possible applications so that the technology can reduce, and not contribute to, the intensification of gender inequalities.

Thus, the objective of this article is to analyze how this emerging technology interacts with gender inequalities in different contexts. By addressing these issues, the article aims to broaden the understanding of the intersection between gender and technology in the digital age, highlighting possible applications of the technology. To this end, an approach that includes a literature review, documentary analysis and study of previously documented cases will be used.

Blockchain technology has emerged as a revolutionary innovation, promising to transform a range of sectors, from finance to government. However, despite its growing adoption and potential impact, gender issues related to this technology remain largely unexplored. In the literature, a literature review by FGV researchers on the application of blockchain from a gender perspective found only 21 articles in the Scopus, Web of Science, Scielo, Ebsco and Google Scholar databases up to August 2023, with only one focusing on the Brazilian case.<sup>3</sup>

1. Master's degree in State Law from the Faculty of Law of the University of São Paulo (USP). Postgraduate student in Digital Law at UERJ/ITS. Visiting researcher at Queen's University, Canada. Author of the book “Digital Constitutional Courts” and the book “Women's Original Constituent Power in Brazil”.

2. PRIBERAM DICTIONARY. *Blockchain*. Available at: <https://dicionario.priberam.org/blockchain> . Accessed on: July 20, 2024.

3. SANTOS, Vanessa Martins dos; DINIZ, Eduardo Henrique; MORAES, Tricia Karla Lacerda; CERNEV, Adrian Kemmer; LOURENÇO, Carlos Eduardo. *Blockchain and gender (in)equality: a systematic literature review*. AMCIS 2024 Proceedings, 2024. Available at: [https://aisel.aisnet.org/amcis2024/span\\_lacais/span\\_lacais/5](https://aisel.aisnet.org/amcis2024/span_lacais/span_lacais/5) . Accessed on: July 7, 2024.

Thus, the choice of the theme is justified by the still incipient academic literature on the subject. That is, although blockchain technology is increasingly important and has the potential to transform various sectors of society, analyses that consider its gender implications are still rare.

The article is structured in three topics. The first topic discusses how male power structures have shaped access to technologies since their inception and the possible impact of a lack of gender perspective on the application of new technologies, such as blockchain. The second topic will present examples of initiatives that use blockchain to promote gender equality in access to property and financial resources, with the aim of exploring how this technology can impact gender inequalities in global economic systems. The last topic, in turn, will present blockchain-based solutions to address gender inequalities on a global scale and in different social contexts.

## 1. What are the values of value technology?

The internet as we know it today is a reflection of a world historically shaped by patriarchal structures. The early architecture of the internet was built in a cultural environment where male voices predominated, influencing both technical development and accessible content. As a result, online platforms often reproduce and amplify existing power dynamics, perpetuating gender stereotypes and marginalizing female voices. This creates a digital space that is, in many cases, neither safe nor inclusive for women.

The advent of blockchain promises a revolution in online value exchange and property. However, the promise of a fairer and more inclusive system faces significant challenges related to the reproduction of the same gender inequalities observed in society and replicated and intensified in the development of the internet.

If the internet has grown rapidly and brought with it social problems from the physical world into the digital space, blockchain technology is likely to follow a similar path, but at a faster pace. This is worrying, considering that gender exclusion dynamics may intensify in an environment where the distribution of value and property is central.

As will be discussed in this topic, although blockchain is often promoted as a neutral technology, the reality is that its implementation and development occur in a social context that still carries

There are profound gender disparities. Furthermore, the blockchain and cryptocurrency industry is still predominantly male, with significantly low female representation in leadership and technology development positions. This inequality can result in products and solutions that do not adequately consider women's needs and perspectives.

The blockchain space is widely recognized for its male dominance, often characterized by the term "Bitcoin bros." This reality is evident at industry-related events, which often end up discouraging female participation.

One notorious example occurred in 2018 during the North American Bitcoin Conference, where 85 of the speakers were men and only three were women. The event was widely criticized after organizers invited the 5,000 attendees to an official evening networking opportunity at a large strip club in Miami. Until 11 p.m., when the event technically ended, guests were served by women in lingerie. Women who attended the conference said they left the club when the *strippers* showed up and criticized the event online. Jeff Scott, a New York-based cryptocurrency trader who attended the conference, commented: "We're a bunch of guys in our 20s with a lot of money. We like naked girls. If you don't like it, that's fine, but don't expect us to change."<sup>4</sup>

In 2022, at the Miami Bitcoin Conference, which attracted over 25,000 attendees, Rachel Siegel, known online as @CryptoFinally, experienced a harassment incident that highlighted persistent sexism in the community. During the event, Siegel, who was interacting with other attendees, had her photo taken without permission by an attendee identified as @bitcoin\_fuckboi. The image, posted on social media, showed an unflattering angle of Siegel and was accompanied by sexually aggressive comments and insults about her body. When Siegel tried to report the incident to the conference organizers, she was met with resistance and an insufficient response. Even after identifying the harasser on social media and discovering that he had taken selfies with other prominent attendees, the organizers failed to take meaningful action. One of the organizers, who used the pseudonym @Chairforce, even liked some of the offensive tweets.<sup>5</sup>

4. MURDOCK, Jason. *We like naked girls': Bitcoin bros slammed as major crypto conference uses strip club*. 2018. Available at: <https://www.ibtimes.co.uk/we-like-naked-girls-bitcoin-bros-slammed-major-crypto-conference-uses-strip-club-1658353>. Accessed on: August 6, 2024

5. PARDES, Arielle. *Miami's Bitcoin Conference Left a Trail of Harassment*. 2022. Available at: <https://www.wired.com/story/bitcoin-2022-conference-harassment/> Accessed on: August 6, 2024

To try to overcome this situation, initiatives focused on education and the creation of networks of women in blockchain have been developed. In 2022, Gwyneth Paltrow and Mila Kunis hosted an event to introduce their new cryptocurrency club, called BFF. Initiatives such as Women in Blockchain and the Black Women Blockchain Council also aim to support women in the broader cryptocurrency ecosystem. Another example is Ladies in Bitcoin, which organizes events and workshops aimed at educating women interested in Bitcoin.<sup>6</sup>

Examining blockchain technology through a gender lens is crucial to understanding how this innovation can be used to promote equality or, alternatively, reinforce existing disparities.

At the current stage of exploring the potential of blockchain, the literature highlights at least four specific areas of risk related to the application of technology from a gender perspective. These are: (i) the lack of gender analysis in the planning phases of projects that use blockchain; (ii) unequal access to technology; (iii) the lack of representation and participation of women and girls in the design and implementation of applications; and (iv) concerns about the protection of human rights, including gender-based violence.<sup>7</sup>

Firstly, with regard to gender analysis, the use of blockchain technology cannot be considered in isolation, but must reflect the underlying limitations of the specific contexts in which it will be applied. It would therefore be necessary to conduct a gender impact analysis for any proposed use of blockchain technology to anticipate some of the key areas of concern and risks that need to be addressed before its introduction.

When it comes to unequal access to technology, the disparity in access to smartphones and connectivity is a highly gendered issue. Women often face greater difficulties in accessing information and media, and the gender digital divide means that women in low- and middle-income countries are 10% less likely to own a mobile phone and 23% less likely to use mobile internet. In places like the Kakuma refugee camp in Kenya, although smartphone ownership and internet access are growing, only 12% of women own smartphones, compared to 37% of men. This makes

6. PARDES, Arielle. *Miami's Bitcoin Conference Left a Trail of Harassment*. 2022. Available at: <https://www.wired.com/story/bitcoin-2022-conference-harassment/> Accessed on: August 6, 2024

7. THYLIN, T., DUARTE, MFN *Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls*. *Gender & Development*, p. 317-336. 2019.

women often rely on men's smartphones rather than having their own, limiting women's access to online services and apps.<sup>8</sup>

Regarding the lack of representation and participation of women and girls in the design and implementation of technology, it is essential to listen to and consider the diverse perspectives, needs, aspirations and concerns of women and girls to ensure that they not only have access to and benefit from technology, but are also able to exercise their autonomy and utilize blockchain technology in ways that empower them. The data, however, demonstrates the disparity of women in this market.

Regarding who owns startups related to the use of blockchain, research by the Bitget brokerage found that only 8% of startups are led by women.<sup>9</sup>

A survey conducted by Forex reveals worrying data on the gender disparity in the crypto and blockchain sector, highlighting the male dominance in leadership positions. According to the study, 94% of CEOs in the sector are men, with 47 male CEOs and only 3 women holding this position. This difference clearly illustrates the male dominance in the industry.<sup>10</sup>

In addition to analyzing CEOs, Forex's research examined leadership positions in general, finding that of the 259 leadership roles identified, 201 were held by men and 58 by women. This represents 78% of the roles held by men and only 22% by women. Another highlight is the analysis of the top 50 crypto influencers on Twitter, where Forex found that only 14% were women.<sup>11</sup>

Finally, regarding the fourth aspect and the possible gender-based violence caused by technology, Thylin and Duarte point out that any humanitarian application of blockchain technology must comply with international humanitarian law, which can be challenging when the interests of private companies conflict with humanitarian interests. A central concern with new technologies is the issue

8. THYLIN, T., DUARTE, MFN Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

9. BITGET. *Bitget Report: Blockchain Market Funding Shows Limited Gender Diversity, Female-led Startups Raise Only 6% Of Overall Funds*. Available at: <https://www.bitget.com/blog/articles/bitget-report-the-gender-gap-in-blockchain-startup-funding>. Accessed on August 3, 2024.

10. FOREX. *Women in Crypto: What role are women playing in crypto in 2024?* Available at: <https://forexsuggest.com/women-in-crypto/> Accessed on July 11, 2024

11. FOREX. *Women in Crypto: What role are women playing in crypto in 2024?* Available at: <https://forexsuggest.com/women-in-crypto/> Accessed on 11. Jul. 2024

of data protection and privacy, which can lead to severe human rights violations. While the full range of potential violations is not yet clear, keeping information on the blockchain private and secure from potential attacks is one of the most concerning issues regarding blockchain technology, and the gender dimensions of these data protection and privacy risks need to be explored.<sup>12</sup>

Given the evidence of disproportionate gender impacts related to the implementation of blockchain systems, it is essential that this new technology, which is expected to reshape the exchange of values, has gender equality as one of its fundamental principles. Therefore, it is imperative that academia analyze the possible risks and applications of blockchain, as its reach expands, and starting this research agenda in the following topics we will highlight some possible applications already recorded in the literature.

## 2. How distributed is the distributed finance system?

“Women, consider cryptocurrencies. Otherwise, men will take all the wealth again.” This famous warning was made by investor Alexia Bonatsos on Twitter.<sup>13</sup>

Indeed, in the offline world, women have historically faced significant barriers to property ownership and access to financial resources. For centuries, laws in many countries have denied women the right to own property, restricting their economic and social autonomy. Even after legal advances that guarantee women the right to own property, substantial inequalities persist that hinder women’s access to finance and investment.

The promise of blockchain technology is to democratize access to property and value, but data shows that there is no gender distribution in the distributed finance system. This can be analyzed by a few aspects, such as the number of women investing in cryptocurrencies or the number of women who are able to leverage their assets using blockchain-related technologies.

According to data provided by the Federal Revenue Service, between 2021 and 2023, operations with crypto assets carried out by women fluctuated on average

12. THYLIN, T., DUARTE, MFN Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

13. BUSINESS TIME. *Women seek their space in the Blockchain industry*. Available at: < <https://epocanegocios.globo.com/Carreira/noticia/2018/02/mulheres-buscam-seu-espaco-na-industria-do-blockchain.html> > Accessed on: July 6, 2024

between 10% and 20%. In the best-case scenario, recorded in December 2022, men still represented more than 70% of operations.<sup>14</sup>

Regarding the receipt of investments, a study carried out by the brokerage Bitget shows that there is a clear correlation between the founder's gender and investment volumes, as statistics indicate that blockchain startups led by women raised only 6% of the total value of investments in the market, proving the existence of a gender bias.<sup>15</sup>

This unequal history reinforces the importance of studying blockchain technology from a gender perspective so that this technology can develop in a way that includes and empowers women and gender minorities. This chapter discusses the potential of blockchain as a financial instrument capable of mitigating gender inequalities in the financial market.

A Brazilian example of the application of blockchain technology with gender impact is the platform *Seeds Currency*. This platform facilitates access to microfinance for female entrepreneurs who have projects with social impact. Using blockchain and its own digital tokens, *Seeds Currency* creates an ecosystem where investors from all over the world can quickly and transparently contribute to sustainable growth. The platform is designed to support financial inclusion and gender equality, especially for women who face difficulties in accessing credit from traditional banks. In addition to financial support, selected projects receive management assistance to optimize their operations and promote long-term sustainable practices.<sup>16</sup>

Another example is the *VipiCash*, an application that uses blockchain technology to enable secure money transfers between women, ensuring that they have full control over their own financial resources, independent of male family members. Olivier Mukuta and his team developed this solution and were awarded at the first blockchain hackathon co-organized by *UN Women and Innovation Norway* in July 2017, with the aim of empowering women in humanitarian crisis situations.<sup>17</sup>

14. FEDERAL REVENUE. *Cryptoassets: Open Data Report and General Information*. Available at: [https://www.gov.br/receita-federal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos/arquivos/criptoativos\\_dados\\_abertos\\_25092023.pdf](https://www.gov.br/receita-federal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos/arquivos/criptoativos_dados_abertos_25092023.pdf) Accessed on: July 25, 2024

15. BITGET. *Bitget Report: Blockchain Market Funding Shows Limited Gender Diversity, Female-led Startups Raise Only 6% Of Overall Funds*. Available at: < <https://www.bitget.com/blog/articles/bitget-report-the-gender-gap-in-blockchain-startup-funding> > Accessed on August 3, 2024.

16. KANEGAE, LC; CERNEV, AK; DINIZ, E. Moeda Seeds: E-Commerce and Crypto Solutions for Development. *Journal of Contemporary Administration*, v. 25, no. spe, p. e200224, 2021.

17. A WOMEN. *From where I stand: Using blockchain technology to empower women*. 2018. Available at: <https://www.unwomen.org/en/news/stories/2018/2/from-where-i-stand-olivier-mukuta> Accessed on: 6 Jul. 2024

For women in humanitarian crises, lack of access to financial systems and the inability to transfer assets are critical issues. This is often linked to a lack of identification documents, as in low-income countries, for example, over 45% of women lack basic identification, compared to 30% of men. Furthermore, the majority of unbanked adults are women, accounting for 56% of the unbanked, compared to 44% of men. In countries affected by humanitarian crises, women are 30% less likely to have an individual financial account than men, such as in Lebanon, where 62% of men and 33% of women have a bank account.<sup>18</sup>

When a crisis strikes, the ability to send and receive funds quickly can be crucial. Blockchain technology can support humanitarian efforts to increase the use of cash transfers in emergency responses and is already being explored in humanitarian programs.<sup>19</sup>

An example is the *Building Blocks*, a project of the World Food Programme (WFP) considered the largest blockchain-based cash distribution system in the humanitarian sector, used to provide efficient and secure assistance to refugees and people in vulnerable situations. Operating in countries such as Bangladesh, Jordan, Lebanon and Ukraine, the project allows the distribution of financial aid through a collaborative network that brings together several humanitarian organizations. Since its inception, the project has processed more than 555 million dollars in money transfers, saving 3.5 million dollars in bank fees, which can be redirected to serve more people in need.<sup>20</sup>

Through blockchain hubs operated by multiple organizations, the platform enables coordination of aid distribution, addressing needs such as food and reproductive health simultaneously. Families receive vouchers that can be redeemed at local points of sale, simplifying the process and eliminating the need to visit multiple locations to obtain aid. This frees up resources for other needs, such as education, and provides protection against diseases common in environments without adequate sanitation.<sup>21</sup>

18. THYLIN, T., DUARTE, MFN Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

19. THYLIN, T., DUARTE, MFN Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

20. WORLD FOOD PROGRAMME. *Building Blocks: Blockchain network for humanitarian assistance*. Available at: [https://innovation.wfp.org/project/building-blocks?\\_ga=2.191649962.1216090504.1723029544-45489905.1723029543](https://innovation.wfp.org/project/building-blocks?_ga=2.191649962.1216090504.1723029544-45489905.1723029543) Accessed on August 4, 2024

21. MATAK, Vincent. *How blockchain can power efforts to empower women and girls in Bangladesh*. 2022. Available at: <https://www.wfp.org/stories/how-blockchain-can-power-efforts-empower-women-and-girls-bangladesh> Accessed on July 4, 2024.

UN Women has also partnered with WFP to innovate on blockchain to support Syrian refugee women participating in paid work programs in Za'atari and Azraq refugee camps in Jordan. Under the joint initiative, women beneficiaries who previously received their monthly benefit at UN Women's Oasis centers in cash on a specific date can now withdraw cash at their convenience from various supermarkets, as cashback at the checkout.

In the program, a virtual wallet is created for each beneficiary, recording the amount of money owed to her for her work, and once a purchase is made, the blockchain records the amount to be debited. What's more, instead of requiring any additional identification, women can do so with an iris scan that validates their identity at the supermarket. This makes transactions for women in refugee camps much faster and safer to monitor.<sup>22</sup>

In addition, UN Women is strengthening its programming to enhance the digital and financial literacy of refugee women beneficiaries. At its four Oasis centers, the UN is offering additional trainings and seminars on expense tracking and budgeting so that beneficiaries can view their accounts and Building Blocks history online.<sup>23</sup>

It is important to note, however, that there are reservations regarding the adoption of the program. First, criticism has been leveled that, as it is a private blockchain, its transformative potential would be limited. The fact is that, before the partnership with UN Women, WFP managed all the nodes in the system, reducing its credibility. UN Women has started to operate an independent node, which allows for mutual validation of transactions, and the expectation is that, by demonstrating effective collaboration around a neutral blockchain network, other humanitarian organizations will realize the benefits and join the common network, bringing the system closer to the characteristics of a public network.<sup>24</sup>

Furthermore, blockchain technology faces several challenges, including high technical complexity, lack of regulation, and high environmental costs associated with its use. Blockchain still requires considerable infrastructure and

22. THYLIN, T., DUARTE, MFN Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

23. THYLIN, T., DUARTE, MFN Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

24. THYLIN, T., DUARTE, MFN Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

resources, which can be problematic in humanitarian contexts. Furthermore, countries less involved in the exploration of the technology and smaller humanitarian actors may not fully benefit from blockchain, exacerbating global inequalities.<sup>25</sup>

Thus, in different ways, some initiatives that use blockchain technology to encourage women's access to the banking and financial system can already be mapped. Technology, however, also has the power to influence other social relationships, as highlighted below.

### 3. We can trust women's future to technology of trust?

Blockchain is known as a technology of trust because the transfers recorded on it can be considered trustworthy and immutable. Using this analogy, this topic seeks to explore whether it is possible to trust that blockchain technology can have good applications when it comes to women's access to services and policies. In this topic, some possible applications of the technology are presented.

In terms of career advancement, the scarcity of women in leadership positions in blockchain startups, as already mentioned, demands the creation of strategies aimed at promoting gender equality in technology spaces. And blockchain platforms themselves present themselves as viable instruments for increasing female participation in the market, from the hiring process, eliminating biases and allowing impartial assessments based on candidates' qualifications, to career management, promoting women's participation and advancement.<sup>26</sup>

In the literature, for example, the possibility of creating a recruitment platform in which each candidate has a unique identity is already advocated, eliminating the possibility of prejudice and allowing candidates to be evaluated solely on the basis of their qualifications. In the study by Obu et al., a hiring platform based on

25. THYLIN, T., DUARTE, MFN Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

26. SANTOS, Vanessa Martins dos; DINIZ, Eduardo Henrique; MORAES, Tricia Karla Lacerda; CERNEV, Adrian Kemmer; LOURENÇO, Carlos Eduardo. *Blockchain and gender (in)equality: a systematic literature review*. AMCIS 2024 Proceedings, 2024.

on blockchain, which has been intentionally adjusted to prevent hiring based on gender and other discriminatory factors.<sup>27</sup>

In addition to encouraging women to advance in their careers, blockchain can play a vital role in protecting women from violence and abuse by providing technological solutions that enable anonymous and secure reporting of harassment and gender-based violence. These solutions not only increase victims' confidence in reporting, but also ensure that evidence is preserved in a secure and immutable manner.

Blockchain technology is being used in mobile apps to anonymously record and report sexual harassment cases. These apps ensure that reports are treated confidentially and that digital evidence is securely stored.

The application *Hehopin France*, reduction of *Help for Hope*, uses blockchain to enable victims of domestic violence to collect and store digital evidence of abuse, which can be used in legal proceedings. The technology ensures that evidence is secure and tamper-proof, providing a powerful tool for victims to access the judiciary.<sup>28</sup>

In Brazil, the Glória Project is an example, in which blockchain is integrated with artificial intelligence and analytics to improve the collection, analysis and provision of data on violence against women. With this data, the aim is to develop educational content, implement public policies and establish a support network equipped with the tools necessary to achieve social improvements.<sup>29</sup>

A third application would be to encourage women in the cultural sector through the use of non-fungible tokens (NFTs) in the art market. NFTs are digital assets that exist on the blockchain with a unique signature and, among other possibilities, allow the promotion of digital art. With the potential of NFTs to transform the art world, the lack of female representation in the NFT and blockchain space has begun to occupy the agenda of artists focused on social missions and has led some artists to begin strategically occupying their space in

27. OBU, U.; AMBEKAR, Y.; LINGAM, R.; BORIKAR, Y.; YADAV, R.; DONGRE, S.. *Blockchain system against gender bias and other discriminatory practices in workplaces*. Proceedings of the 2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal Impact using Marketing, Entrepreneurship and Talent (TEMSMET), p. 1-6, 2023.

28. WELSH, Chris. *An app to put domestic abusers on trial*. 2021. Available at: <https://www.eib.org/en/stories/domestic-violence-evidence-app> Accessed on 5 Jul 2024.

29. VICENTE, Beatriz Freitas Alves. *Blockchain technology for women*. 2022. Available at: <https://www.conjur.com.br/2022-abr-04/beatriz-vicente-blockchain-favor-mulher/> Accessed on: July 3, 2024

a male-dominated market, through different initiatives and projects.<sup>30</sup>

An example is *World of Women* (WoW), an NFT art project launched in 2021. It features a collection of diverse female tokens, with the first collection called WoW and an expansion released in 2022 called *WoW Galaxy*. WoW aims to create an inclusive and diverse Web 3.0 by promoting equal participation in the NFT space. The project team supports causes related to female empowerment, initially donating 7.5% of sales from its first collection to institutions such as *She's The First, Too Young to Wed* and *Strange Cintia*.<sup>31</sup>

Similarly, the project *Women Rise* is an NFT art project created by visual artist Maliha Abidi and released in 2021. The collection *Women Rise* is made up of 10,000 unique, randomly generated digital tokens. To help in the pursuit of gender equality, 2.5% of sales are donated to *Malala Fund* and 7.5% to organizations that support gender equality, women's education, and mental health in marginalized communities. In addition, the *Women Rise* is one of the first NFT projects to commit to the 2030 Agenda for Sustainable Development, integrating the Sustainable Development Goals (SDGs) into its artwork and donations.<sup>32</sup>

Another use of NFT is proposed by the literature to modify security in practices *sexting* and the unauthorized sharing of intimate photos, which mainly affects girls and women. Franco et al. explore the use of blockchain technology and specifically NFTs to combat the non-consensual dissemination of user-generated intimate images and highlight that traditional messaging applications used for sexting are insecure as they allow for the easy sharing of personal content. By implementing decentralized blockchain-based solutions, the authors aim to create a safer and more trustworthy environment where the presence of malicious nodes is mitigated, ensuring better performance, scalability and privacy compared to centralized systems.<sup>33</sup>

A risk regarding gender-related data and its insertion into blockchain technology, in turn, is raised by Shahaab et al. who advocate that

30. SYULEYMANOGLU, B. *Call for diversity in Web 3.0: case study of NFT art projects World of Women (WoW) and Women Rise*. Malmö University, Faculty of Culture and Society (KS), School of Arts and Communication (K3). 2022.

31. SYULEYMANOGLU, B. *Call for diversity in Web 3.0: case study of NFT art projects World of Women (WoW) and Women Rise*. Malmö University, Faculty of Culture and Society (KS), School of Arts and Communication (K3). 2022.

32. SYULEYMANOGLU, B. *Call for diversity in Web 3.0: case study of NFT art projects World of Women (WoW) and Women Rise*. Malmö University, Faculty of Culture and Society (KS), School of Arts and Communication (K3). 2022.

33. FRANCO, M.; GAGGI, O.; GUIDI, B.; MICHIEZI, A.; PALAZZI, C. E A decentralized messaging system robust against the unauthorized forwarding of private content. *Future Generation Computer Systems*, v. 145, p. 211-222, 2023.

Blockchain can play a crucial role in building digital identity and protecting personal data online, however, personal data should not be considered “static” and should never be stored in an immutable form, as this could have serious consequences for trans people.<sup>34</sup>

Thus, this topic sought to highlight that, in addition to typical applications related to the financial market, there are already discussions in the literature about possible applications and risks of blockchain technology in different social contexts.

## Final considerations

This article explored the various ways in which blockchain technology can be leveraged to address issues of gender inequality, considering the lack of academic work addressing the topic, especially in Portuguese.

The first topic highlighted how the promise of democratization of blockchain technology still faces significant challenges to fully fulfill its transformative potential in terms of gender equality.

In the second topic, the gender distribution in the distributed financial system was discussed. The analysis of the data revealed that women still face significant barriers in accessing and using crypto assets and investments, demonstrated by the gender disparity in blockchain startups and the lower female participation in cryptocurrency operations. However, through examples such as *Seeds Currency* and the *VipiCash*, it has been shown that technology can give women greater control over their financial resources and facilitate access to microfinance. Furthermore, initiatives such as *Building Blocks* demonstrate how blockchain can be used to offer innovative solutions in humanitarian contexts.

The last topic presented blockchain solutions for impartial recruitment, NFTs in the art market and applications for reporting violence that offer a glimpse of how technology can be used in innovative ways to address social issues.

If there is potential for using technology from a gender perspective, it is crucial to ensure that these solutions are implemented with attention to ethical considerations and the needs of women, recognizing

34. SHAHAAB, A.; MAUDE, R.; HEWAGE, C.; KHAN, I. Managing gender change information on immutable blockchain in context of GDPR. *The Journal of British Blockchain Association*, p. 1-8, 2020.

that technology alone will not solve systemic inequalities. It is concluded that it is essential that technological developments are accompanied by a holistic approach that includes public policies, education and awareness to create a more inclusive environment.

Only through collaboration between governments, the private sector and civil society will it be possible to maximize the positive impact of blockchain technology on women's lives, ensuring that it becomes a true feminine noun.

## References

BITGET. Bitget Report: Blockchain Market Funding Shows Limited Gender Diversity, Female-led Startups Raise Only 6% Of Overall Funds. Available at:<https://www.bitget.com/blog/articles/bitget-report-the-gender-gap-in-blockchain-startup-funding> . Accessed on August 3, 2024.

PRIBERAM DICTIONARY. Blockchain. Available at:<https://dicionario.priberam.org/blockchain> . Accessed on: July 20, 2024.

ÉPOCA NEGÓCIOS. Women seek their space in the Blockchain industry. Available at:<https://epocanegocios.globo.com/Carreira/noticia/2018/02/mulheres-buscam-seu-espaco-na-industria-do-blockchain.html> . Accessed on: July 6, 2024.

FOREX. Women in Crypto: What role are women playing in crypto in 2024? Available at:<https://forexsuggest.com/women-in-crypto/> . Accessed on: July 11, 2024.

FRANCO, M.; GAGGI, O.; GUIDI, B.; MICHIEZI, A.; PALAZZI, CE A decentralized messaging system robust against the unauthorized forwarding of private content. *Future Generation Computer Systems*, vol. 145, p. 211-222, 2023.

KANEGAE, LC; CERNEV, AK; DINIZ, E. Moeda Seeds: E-Commerce and Crypto Solutions for Development. *Journal of Contemporary Administration*, v. 25, n. spe, p. e200224, 2021.

MATAK, Vincent. How blockchain can power efforts to empower women and girls in Bangladesh. 2022. Available at:<https://www.wfp.org/stories/how-blockchain-can-power-efforts-empower-women-and-girls-bangladesh> . Accessed on: July 4, 2024.

MURDOCK, Jason. 'We like naked girls': Bitcoin bros slammed as major crypto conference uses strip club. 2018. Available at:<https://www.ibtimes.co.uk/we-like-naked-girls-bitcoin-bros-slammed-major-crypto-conference-uses-strip-club-1658353> . Accessed on: August 6, 2024.

OBU, U.; AMBEKAR, Y.; LINGAM, R.; BORIKAR, Y.; YADAV, R.; DONGRE, S. Blockchain system against gender bias and other discriminatory practices in workplaces. *Proceedings of the 2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal Impact using Marketing, Entrepreneurship and Talent (TEMSMET)*, p. 1-6, 2023.

PARDES, Arielle. Miami's Bitcoin Conference Left a Trail of Harassment. 2022. Available at:<https://www.wired.com/story/bitcoin-2022-conference-harassment/> . Accessed on: August 6, 2024.

FEDERAL REVENUE. Cryptoassets: Open Data Report and General Information. Available at: [https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos/arquivos/criptoativos\\_dados\\_abertos\\_25092023.pdf](https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos/arquivos/criptoativos_dados_abertos_25092023.pdf) . Accessed on: July 25, 2024.

SANTOS, Vanessa Martins dos; DINIZ, Eduardo Henrique; MORAES, Tricia Karla Lacerda; CER-NEV, Adrian Kemmer; LOURENÇO, Carlos Eduardo. Blockchain and gender (in)equality: a systematic literature review. AMCIS 2024 Proceedings, 2024. Available at: [https://aisel.aisnet.org/amcis2024/span\\_lacais/span\\_lacais/5](https://aisel.aisnet.org/amcis2024/span_lacais/span_lacais/5) . Accessed on: July 7, 2024.

SHAHAAB, A.; MAUDE, R.; HEWAGE, C.; KHAN, I. Managing gender change information on immutable blockchain in context of GDPR. The Journal of British Blockchain Association, p. 1-8, 2020.

SYULEYMANOGLU, B. Call for diversity in Web 3.0: case study of NFT art projects World of Women (WoW) and Women Rise. Malmö University, Faculty of Culture and Society (KS), School of Arts and Communication (K3). 2022.

THYLIN, T.; DUARTE, MFN Leveraging blockchain technology in humanitarian settings—opportunities and risks for women and girls. Gender & Development, p. 317-336, 2019.

UN WOMEN. From where I stand: Using blockchain technology to empower women. 2018. Available at: <https://www.unwomen.org/en/news/stories/2018/2/from-where-i-stand-olivier-mukuta> . Accessed on: July 6, 2024.

VICENTE, Beatriz de Freitas Alves. Blockchain technology in favor of women. 2022. Available at: <https://www.conjur.com.br/2022-abr-04/beatriz-vicente-blockchain-favor-mulher/> . Accessed on: July 3, 2024.

WELSH, Chris. An app to put domestic abusers on trial. 2021. Available at: <https://www.eib.org/en/stories/domestic-violence-evidence-app> . Accessed on: July 5, 2024.

WORLD FOOD PROGRAM. Building Blocks: Blockchain network for humanitarian assistance. Available at: <https://innovation.wfp.org/project/building-blocks?ga=2.191649962.1216090504.1723029544-45489905.1723029543> . Accessed on: August 4, 2024.

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

Axis III

# Protection of data and security digital

## AUTHORS

Giovana Sant'Anna

Mariana de Souza

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

16

# **Risk and Cybersecurity in Brazil: a regulatory analysis aiming at data protection**

Giovana Sant'Anna

Summary: Introduction. 1. The Risk Society and the Information Society. 2. Cyber Weaknesses and Cybersecurity. 3. Current Legislative Panorama. Final Considerations. Bibliographic References.

## Introduction

It cannot be said that concern about the use of the Internet is something new for the current generation. Since the 1980s and the constant and gradual democratization of computers, the term virus<sup>2</sup> was already becoming popular among users, system administrators and, in general, within organizations. The risks arising from the use of the Internet already existed at the time, but today cyber attacks are increasingly sophisticated and difficult to detect, leaving us to find the most varied ways to mitigate them, mainly in a predictive way.<sup>3</sup>

Social evolution resulting from the increasing use of technologies has brought a bias towards digital structures to personal relationships, which, in turn, demands the constant use of numerous personal and sensitive data.<sup>4</sup> This drew attention to the topic of Information Security.<sup>5</sup> and digital security<sup>6</sup>, themes that have become frequent focuses of debates and discussions encouraged by the media perspective mainly after inci-

1. Lawyer graduated in Law from the São Bernardo do Campo Law School in 2018. Postgraduate student at the Rio de Janeiro Institute of Technology (ITS Rio).

2. A computer virus is *malware*, that is, invasive software or code created with the aim of infecting, damaging or accessing computer files, self-replicating and infecting other files and documents. For more details see: LATTO, Nica. *What is a computer virus and how does it work?* Avast Academy, 2020. Available at: <https://www.avast.com/en-us/c-computer-virus#:~:text=A%20computer%20virus%20at%20the%20memory%20of%20other%20files%20or%20documents> . Accessed on: July 17, 2024.

3. ALMEIDA, John Emilio de. *Cybersecurity: from risk prevention to incident management*. RISTI - Iberian Journal of Information Systems and Technologies, Porto, ed. 43, p. 1-4, September 30, 2021. p. 1-4. Available at: <https://scielo.pt/pdf/rist/n43/1646-9895-rist-43-1.pdf>. Accessed on: May 2, 2024.

4. In short, according to Law 13.709/2018, personal data is considered to be any information related to a person that makes them identified or identifiable, and sensitive personal data is any information that deals with ethnic or racial origin, religion, political opinion, membership in unions or religious, philosophical or political organizations, health or sexual life, genetic or biometric data. For more details, see: BRAZIL. Law No. 13.709, of August 14, 2018. General Personal Data Protection Law (LGPD). *Official Gazette of the Union*. Brasília: Presidency of the Republic. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm) .

5. For Belli et al, information security is a dimension of cybersecurity. For more details see: BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B. *Cybersecurity: A systemic vision towards a regulatory framework proposal for a digitally sovereign Brazil*. 1st ed. Rio de Janeiro: Rio de Janeiro: FGV Law School Rio, Ag. 2023. Available at: <https://diretorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistematica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil> . Accessed on: June 24, 2024.

6. SHIRA, Fer; JANCZ, Carla. *Strategic Barricades and Collectivity: A Digital Security Primer for Organizations*. Marialab, São Paulo, December 1, 2022. p. 3. Available at: <https://www.marialab.org/wp-content/uploads/2020/12/Barricadas-estrategias-coletividade.pdf> . Accessed on: July 13, 2024.

teeth involving major information leaks, putting the rights of thousands of users around the world at risk<sup>7</sup>.

Today, targets are not limited to private companies or individuals. Cyberattacks are aimed at government organizations and even directly at countries, an example of which is the controversial 2016 US presidential election, which brought the terms “cyberterrorism” and “military attack” through cybernetic means to the fore. In other words, technological advances have brought with them an enormous burden: the pecuniary valuation of information and its use as an influential weapon of social, political and economic control.<sup>8</sup>

Beck<sup>9</sup> highlights that globalization brings new risks to the surface. Risk is not restricted to physical threats, but to social and environmental dangers arising from technological progress and can range from nuclear accidents to privacy and data security. These are global and transcendental risks capable of affecting individuals and societies and challenging traditional structures that will necessarily have to start discovering new methods of risk management, the digital ones.

Therefore, the intense transformation resulting from the last decades of unbridled technological advancement culminated in the emergence of a new era for humanity, characterized by attractive technology<sup>10</sup>. Thus, the Theory of Law was forced to rethink its foundations in order to incorporate technological impacts, creating boundaries and rules capable of halting the -until then- unknown technological development and keeping up with human and social redefinition, ensuring the protection of the rights of users who own data.<sup>11</sup>

Teffe<sup>12</sup> understands that it is up to the Law to act preventively in the protection of data, without failing to reflect the autonomy of individuals and the imposition of duties on agents. This is how the term “Digital Law” originates, coming from the Law itself, which encompasses its most varied areas, the impasses of the so-called

7. FICHTNER, Laura. What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, Germany, v. 7, p. 1-19, 15 May 2018. DOI 10.14763/2018.2.788. Available at: <https://policyreview.info/articles/analysis/what-kind-cyber-security-theorising-cyber-security-and-mapping-approaches> . Accessed on: June 3, 2024.

8. ALMEIDA, João Emílio de. Cybersecurity: from risk prevention to incident management. *RISTI - Iberian Journal of Information Systems and Technologies*, Porto, ed. 43, p. 1-4, September 30, 2021. P. 1-4. Available at: <https://scielo.pt/pdf/rist/n43/1646-9895-rist-43-1.pdf> . Accessed on: May 2, 2024.

9. BECK, Ulrich. *Risk Society towards another modernity*. New York: Routledge, 2014, pp. 25-28.

10. LUCCA, Newton de. Human dignity and electronic risks. *Galileo - Journal of Economics and Law*, v. XVII, n.1. 2012. p. 283.

11. BITTAR, Eduardo CB Theory of Law, the Digital Age and the Post-Human: the new status of the body under a technological regime and the emergence of the Post-Human Subject of Law. *Law and Praxis*, v. 10, n. 2, 2019, p. 935.

12. TEFFÉ, Chiara de. *Sensitive personal data: Qualification, processing and good practices*. Indaiatuba, São Paulo, 2022. np Available at: [https://www.google.com.br/books/edition/Dados\\_Pessoais\\_Sens%C3%ADveis/atCLEAAQBAJ?hl=ptBR&-qbpv=1](https://www.google.com.br/books/edition/Dados_Pessoais_Sens%C3%ADveis/atCLEAAQBAJ?hl=ptBR&-qbpv=1) . Accessed on: June 28, 2024.

the information society and the current technological expansion<sup>13</sup>. It can be seen that the issue of regulation for the virtual world and the advent of digital law translate much more into a political than a legal vision, since the internet represents a direct domain for economic and social development.<sup>14</sup>

In the domestic scenario, we have verified the existence of some legislative frameworks that seek to protect the individual rights and data of internet users, among which the following stand out: The Cybercrimes Law (Law 12,737/2012), the Internet Civil Framework (Law 12,965/2014) and the General Data Protection Law (Law 13,709/2018)<sup>15</sup>. However, the regulation of cybersecurity measures is still unclear and fragmented. This article will be developed within this area, seeking to elucidate the concept of risk in the digital society, the importance of preventive action through governance measures and what are the current regulations applicable to the topic of cybersecurity and data protection in Brazil until the publication of the unprecedented - and recent - National Information Security Policy, enacted by Decree No. 11,856 in December 2023.

## 1. The Risk Society and the Information Society

The digital era poses unprecedented challenges to the Science of Law due to intense social transformations, the imposition of “algorithms” and digital operationalization, that is, the attribution of a new social (technological) dynamic that has outlined necessary processes of adaptation of the legal matter, aiming at the effective guarantee in the protection of the rights of data subjects.<sup>16</sup> Digital law arises from the very need for regulation prompted by technological obstacles and dilemmas characteristic of the Information Society<sup>17</sup>. In today's society, information is considered a valuable product, a financial asset, and must be understood as such, and therefore must be treated, cared for and protected. Information systems are essential for organizing this data and play an important role in risk analysis and mitigating possible information leak incidents.<sup>18</sup>

13. PIMENTEL, José ES Introduction to Digital Law. *ESMP-SP Law Journal*, v. 13, 2018, p. 18.

14. LUCCA, Newton. Human dignity and electronic risks. *Galileu – Journal of Economics and Law*, v. XVII, n.1. 2012. p. 283.

15. GOLDONI, Luiz RF; RODRIGUES, KF; MEDEIROS, BP What is the future of cybersecurity governance in Brazil. *Contemporary Brazil*. São Paulo, v. 29., 2024. p. 4.

16. BITTAR, Eduardo CB The Theory of Law, the Digital Age and the Post-Human: the new status of the body under a technological regime and the emergence of the Post-Human Subject of Law. *Law and Praxis*, v. 10, n. 2, 2019, p. 935.

17. PIMENTEL, José ES Introduction to Digital Law. *ESMP-SP Law Journal*, v. 13, 2018, p. 18.

18. SAMPAIO, Dhiego RLA *study on information security risks at the UFC campus in Quixadá based on the ISO/IEC 27005 standard*. 2014. 45 p. Monograph (Bachelor's Degree in Information Sciences)–Federal University of Ceará, Quixadá, 2014.

In a broad view, Digital Law emerges with the objective of regulating the virtual environment, the interactions arising from this environment, the storage and processing of digital data to actively protect society against violations of its subjective rights. By Lucca<sup>19</sup> conceptualizes that, if the parallel between the two eras (Industrial Revolution and Digital Revolution) were plausible, the difference would be substantiated by the speed of the transformations caused by the digital era. While the Industrial Revolution is based on the amount of work invested in products and services, the Digital Revolution is based on the amount of information and knowledge of products and services. The high amount and speed of transmission of this information are hallmarks of the digital era, which has as its production model the massification of information, the speed of dissemination and the decentralization of the sources of this information<sup>20</sup>.

Information present in a dangerous or uncertain environment poses risks<sup>21</sup>, therefore it generates insecurity. Digital insecurity must be combated by implementing controls that can be implemented to ensure that risks are reduced to an acceptable level.<sup>22</sup> It is also important to consider that the processing of data by the State, through the use of digital technologies, can lead to institutional violence against communities. Users are considered the weakest link in any digital system, so social empowerment is – without a doubt – considered essential, since it is one of the effective means of curbing these new forms of social violence and the fragility of individual rights.<sup>23</sup> It is worth noting that the large amount of data resulting from the use of the Internet has become an extremely valuable currency in today's society, which highlights a severe risk to the privacy of data subjects.<sup>24</sup>

German sociologist Ulrich Beck<sup>25</sup> proposes with the “Theory of the (Industrial) Risk Society” a rupture in the core of society as a consequence of

19. LUCCA, Newton. Human dignity and electronic risks. *Galileu – Journal of Economics and Law*, v. XVII, n.1. 2012. p. 283-285.

20. PIMENTEL, José ES Introduction to Digital Law. *ESMP-SP Law Journal*, v. 13, 2018, p. 19-20.

21. According to ISO/IEC 27005, information security risk is predicted based on the possibility of an incident and its consequences and, when managed, it is possible to change its possibility and consequences.

22. SAMPAIO, Dhiego RLA *study on information security risks at the UFC campus in Quixadá based on the ISO/IEC 27005 standard*. 2014. 45 p. Monograph (Bachelor's Degree in Information Sciences) – Federal University of Ceará, Quixadá, 2014.

23. BELLI, Lucca; Bakonyi Erica; Chen Larissa, et al. Cybersecurity: a systemic vision towards a regulatory framework proposal for a digitally sovereign Brazil. Rio de Janeiro: *FGV Law School Rio*, 2023, p. 15-16.

24. LORENZON, Laila N. Comparative analysis between personal data regulations in Brazil and the European Union (LGPD and GDPR) and their respective enforcement instruments. *Journal of the European Union Law Programme*, 2021, p. 40.

25. BECK, Ulrich. *Risk Society towards another modernity*. New York: Routledge, 2014, p.

industrial and scientific development and, inherent to these, risks. The author determines that the Risk Society is intrinsically catastrophic, since in it the exceptional state of insecurity and threat are normalized. Furthermore, he defines that current risks are direct impacts of modernization and differentiates them from the industrial risks of the 19th and 20th centuries, since these were limited to certain areas and specific groups, but the risks arising from modernization are transnational and will inevitably reach border barriers and even those who produced them or profit from them.

Beck<sup>26</sup> mentions that these risks contain an effect *boomerang*, that is, not even the most powerful social class is effectively safe and shielded from them. The sociologist also proposes that risks, like wealth, are objects of distribution and this distribution does not occur in an egalitarian manner. While wealth is shown as a product, risks or threats are qualified as the byproduct of modernization<sup>27</sup>. Therefore, it is necessary to pay attention to the distribution of risks in today's society so that we do not place ourselves in an unfair and unbalanced structure of risk distribution, directly threatening the fundamental rights of data subjects. In this sense, Gomes<sup>28</sup> highlights the asymmetry between the State, Data Controllers and Data Subjects in the distribution of risks, underlining the need to rethink this distribution to improve data protection. Historically, there have been abuses of rights related to the use of data for state surveillance, intensifying the already existing asymmetry and making data protection extremely fragile for data subjects.

Niklas Luhmann<sup>29</sup> teaches that the concept of risk was already present since the mid-16th century. Its emergence would have occurred from the invention of maritime insurance, being seen as a probability of losses and gains throughout voyages. Thus, it would involve the interaction between systems, society and the uncertainties arising from this relationship, being inherent, therefore, to a complex social construction. Luhmann<sup>30</sup> It also establishes that depending on the social area involved, the risk will be different and will entail different challenges and results. As an example, the political aspect will demand different risks and results from the economic and legal areas in society. As for technological risk, we can understand it as a result of the development itself.

26. BECK, Ulrich. *Risk Society towards another modernity*. New York: Routledge, 2014, pp. 25-30.

27. Ibid.

28. GOMES, Maria Cecília O. Between method and complexity: understanding the notion of risk in the LGPD. In Current issues in data protection. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brazil, 2020, p. 255.

29. LUHMANN, Niklas. *A Sociological Theory*. New York: Routledge, 2017, p. 8-9.

30. Ibid. pp. 30-35.

systemic development, capable of involving risks of technical failures, cyber attacks and even social and environmental consequences that have not yet been mapped. However, risks must be assessed and mitigated, that is, managed, in order to guarantee the security of society in general when using the Internet.

Lhumann<sup>31</sup> distinguishes the concepts of risk, security and danger. The first two are seen by him as antagonistic, with risk being associated with decisions made on a daily basis and security being associated with the state that we constantly seek socially, even though in the contemporary world scenario it is practically impossible to fully mitigate all types of risks. As for danger, the author relates this concept to a situation of damage that is not caused by the agent that suffers the consequences, as in the case of natural disasters.

In this sense, a historical reflection is relevant: before anthropocentrism, events were often attributed to forces external to human will. However, after the Renaissance, there was a significant change with the rationalization of decision-making, when we gradually began to assume responsibility for the results of these decisions.<sup>32</sup> Therefore, digital risks will be present as long as social and technological changes produce unforeseen consequences. We can therefore consider risks as the uncertain side of modernity. This does not mean that life today is riskier than in previous times, but that for today's society, both laypeople and experts will have to carry out the daily and permanent task of weighing and managing risks.<sup>33</sup>

Over the years, there has been a gradual advancement of society establishing rational risk calculations. Initially, risk calculation was based on a dualistic view of failure. *versus* success, but later this calculation was better developed with robust metrics based on mathematics and probability, generating greater control over the results of risks. However, when addressing the issue of risk we must always remember that we are faced with a vast range of human experiences, which places us before an eternal unknown and makes it impossible to predict or control all risks, even with the most robust methods developed to date.<sup>34</sup> Furthermore, science and technology bring with them several

31. Ibid. p. 19.

32. GOMES, Maria Cecília O. Between method and complexity: understanding the notion of risk in the LGPD. In Current issues in data protection. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brazil, 2020, p. 252.

33. GIDDENS, Anthony. *Modernity and Identity*. New York: Routledge, 2002, p. 32.

34. GOMES, Maria Cecília O. Between method and complexity: understanding the notion of risk in the LGPD. In Current issues in data protection. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brazil, 2020, p. 252.

benefits and facilities, despite forcing us to face risks and dangers. Therefore, it is advantageous that we evaluate and manage risks rationally so that we can reap the benefits of postmodern society<sup>35</sup>.

In the early 2000s, cases of data invasion and violation of user privacy became more frequent due to the emergence of *spams*<sup>36</sup> from website databases that sold and shared user information<sup>37</sup>. This rapid social transformation caused by high digitalization, with the focus on data as a model of wealth, has brought to light the need for greater investment in cybersecurity. As there is a growing technological market, with qualified professionals in the area, there is also a growing criminal market requiring constant updating on the subject. Thus, the demand for legal protection of data comes from the economic importance that data plays in the current reality, and the high volume of data stored by public and private entities highlights the high risk to users' privacy, making it clear the need for legislative updates to guarantee the protection of the fundamental rights of civil society.<sup>38</sup>

## 2. Cyber vulnerabilities and cybersecurity

As already mentioned, the large number of people connected has resulted in a significant increase in cybercrimes and in greater attention from society to the pressing need to develop rules of conduct and limit state and private action in controlling the information they process and store.<sup>39</sup> First of all, cybersecurity is a multifaceted ecosystem that requires the implementation of a governance mechanism and a set of regulations that are capable of communicating with each other and with the different sectors of society, in order to ensure efficient and effective application. This requires a formalized national alignment through

35. GIDDENS, Anthony. *Modernity and Identity*. New York: Routledge, 2002, p. 32.

36. Spam comes from the English term "*Sending and Posting Advertisement in Mass*", that is, it can be interpreted as sending and posting mass advertisements. For more details see: LINKNACIONAL. What is spam? Link Nacional, Oct. 20, 2023. Available at: <https://www.linknacional.com.br/blog/o-que-e-spam/>. Accessed on: June 24, 2024.

37. BRAGA, Noelson Araujo. *Cybersecurity and the Right to Privacy: A study on the cyber construction in Brazil and the European Union from a realist perspective*. 2021. 35 p. Monograph (Bachelor's Degree in International Relations) – University of Brasília UNB, Brasília, 2021.

38. LORENZON, Laila N. Comparative analysis between personal data regulations in Brazil and the European Union (LGPD and GDPR) and their respective enforcement instruments. *Journal of the European Union Law Programme*, 2021, p. 40.

39. BRAGA, Noelson Araujo. *Cybersecurity and the Right to Privacy: A study on the cyber construction in Brazil and the European Union from a realist perspective*. 2021. 35 p. Monograph (Bachelor's Degree in International Relations) – University of Brasília UNB, Brasília, 2021.

of a regulation capable of establishing minimum operational standards, principles and the governance system with risk mitigation<sup>40</sup>.

Cybersecurity must be considered a real concern in order to draw up a plan to face challenges and prevent risks and threats from occurring. Reactive action – decision-making after accidents

– can cause substantial losses and enormous financial, legal and reputational damage to companies and public authorities<sup>41</sup>. In the private organizations scenario, it is inevitable to increase defense systems and anticipate frequent digital attacks. These attacks usually consist of theft or hijacking of information.<sup>42</sup>, as occurs in *ransomware*<sup>43</sup>. We can, therefore, understand cybersecurity as a set of regulations that establishes procedures and practices aimed at the security of systems, information and digital risks, with information security being just one of the layers of cybersecurity.

Cybersecurity incidents, although often linked to failures or direct attacks, also refer to insecure behavior by technology developers or users, which can compromise the basic principles of confidentiality, integrity, authenticity, authentication and access.<sup>44</sup>. There are recent and notable cases that have directly affected the provision of public services in Brazil, with emphasis on the incident involving the vaccination control of the Brazilian population and attacks on court systems that force the extension of deadlines and the suspension of the provision of public services to citizens.<sup>45</sup>.

In 2021, two emblematic cases marked the Brazilian reality in terms of cybersecurity: the invasion of the ConectSUS application<sup>46</sup> and the sale of data from the Comptroller General of the Union on internet forums. The Conect-SUS application was hacked in December 2021 and caused, in addition to the impossibility

40. BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GAS-PAR, Walter B. Cybersecurity: A systemic vision towards a regulatory framework proposal for a digitally sovereign Brazil. 1st ed. *FGV Law School Rio*, Ag. 2023. p. 22. Available at: <https://diretorio.fgv.br/publicacao/cybersecurity-a-systemic-vision-towards-a-proposal-for-a-regulatory-framework-for-brazil>. Accessed on: June 24, 2024.

41. Ibid.

42. ALMEIDA, João E. de. Cybersecurity: from risk prevention to incident management. *RISTI – Iberian Journal of Information Systems and Technologies*. Porto, 2021, p.2.

43. A form of attack that consists of blocking or hijacking information or systems of organizations in which the release only occurs upon payment of a ransom. For more details see: ibdi. p. 19.

44. BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GAS-PAR, Walter B. Cybersecurity: A systemic vision towards a regulatory framework proposal for a digitally sovereign Brazil. 1st ed. *FGV Law School Rio*, Ag. 2023. p. 24-25. Available at: <https://diretorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil>. Accessed on: June 24, 2024.

45. Ibid.. p. 19.

46. *Problems with ConecteSUS: before the hacker attack, the system was controversial due to data changes and failures*. Available at: < <https://g1.globo.com/saude/noticia/2021/12/10/problemas-no-conectesus-antes-de-ataque-hacker-sistema-teve-polemica-com-alteracao-de-dados-e-falhas.ghtml> >.

of issuing vaccination certificates, the data of several users was changed. Some vaccine doses simply disappeared from the system and users reported that their data (name, mother's name and nationality) had been changed. The Ministry of Health reported at the time that it had taken the appropriate measures and even shut down access to the ConectSUS application<sup>47</sup>. Still in 2021 there was a widespread invasion of public services of the Brazilian government, Federal Administration credentials were found for sale on forums *dark web*, logins and passwords of the Comptroller General of the Union and the Ministry of Health were leaked<sup>48</sup>.

Furthermore, in November 2020 the Superior Court of Justice experienced a cyber attack<sup>49</sup> which became known by the Court itself as the worst cyber attack ever carried out against a Brazilian public institution<sup>50</sup>. The attack prevented millions of people from accessing the STJ platform, including the Ministers themselves, causing chaos in the judiciary and the suspension of procedural deadlines for almost an entire week. The years 2020 and 2021, therefore, were marked by major data leaks in Brazil, leaks capable of affecting a number greater than the national population itself, since they exposed data from more than 220 million people.<sup>51</sup> This fact reflects an important current characteristic: the dependence of public and private organizations on the Internet.<sup>52</sup>

This shows that, in the current scenario, in which being connected is an essential act in various social classes, cyber insecurity threatens society as a whole, even putting the democratic perspective at risk.<sup>53</sup> Private companies, public bodies and entities are still the biggest target of attacks, however society in general must always be concerned and contribute to the protection of its rights. It is worth noting that attacks

47. *Problems with ConecteSUS: before the hacker attack, the system was controversial due to data changes and failures.* Available at: < <https://g1.globo.com/saude/noticia/2021/12/10/problemas-no-conectesus-antes-de-ataque-hacker-sistema-teve-polemica-com-alteracao-de-dados-e-falhas.ghtml> >.

48. *CRIMINALS sell data from the CGU and Ministry of Health on the dark web.* [S. l.], 21 Dec. 2021. Available at: <https://canaltech.com.br/seguranca/criminosos-vendem-dados-do-cqu-e-ministerio-da-saude-na-dark-web-204985/> . Accessed on: June 27, 2024.

49. G1. STJ calls on PF to investigate possible hacker attack on the court system. *G1*, 4 Nov. 2020. Available at: <https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataque-de-hackers-ao-sistema-do-tribunal.ghtml> . Accessed on: July 2, 2024.

50. MARCON, Daniele Verza. *Cyber Risk Insurance: challenges to define the guarantee and promote cybersecurity in the digital age.* 2023. Dissertation (Master's Degree in Legal and Social Sciences) - Federal University of Rio Grande do Sul, [S. l.], 2023. Available at: <https://lume.ufrgs.br/handle/10183/267969> . Accessed on: July 3, 2024.

51. Ibid.

52. Ibid.

53. BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GAS-PAR, Walter B. *Cybersecurity: A systemic vision towards a regulatory framework proposal for a digitally sovereign Brazil.* 1st ed. *FGV Law School Rio*, Ag. 2023. p. 19. Available at: <https://diretorio.fgv.br/publicacao/cybersecurity-a-systemic-vision-towards-a-proposal-for-a-regulatory-framework-for-brazil> . Accessed on: June 24, 2024.

Cybercrimes do not only occur as a result of active attacks, but also occur passively, due to the fragility or absence of basic security measures and lack of user training.<sup>54</sup>

In 2023 Brazil led the *ranking* of countries with the largest volume of leaked data, surpassing India, the United States and Indonesia in terms of the volume of compromised information. Among the leaked information, names, emails, addresses and passwords stored by the *cookies*<sup>55</sup> saved in the browsers of Brazilian users<sup>56</sup>. Such incidents demonstrate that Brazilian society still suffers from lack of control over its own information, which can be interpreted as a breach of the data subject's right to privacy, who is unable to exercise their power of decision, processing and transmission of their information.<sup>57</sup>

In view of the high risk of federal public organizations, in 2022 the Federal Court of Auditors published a booklet highlighting five cybersecurity control measures that would need to be implemented urgently by the Brazilian public administration, namely: inventory and controls of corporate information technology assets; inventory and controls of corporate information technology assets; *software*; ongoing vulnerability management; security awareness and skills training; and incident response management<sup>58</sup>.

This was part of a series of measures taken in response to the episodes highlighted here, as they brought to light the high-risk vulnerability of the national public administration. In addition to the booklet published by the Federal Court of Auditors, these events also encouraged the publication of a new cybersecurity framework in December 2023, the National Cybersecurity Policy (PNCiber) - Presidential Decree No. 11,856. This Decree, which acts as an immediate response to the current worrying scenario<sup>59</sup>, will be analyzed in the next chapter.

54. SHIRA, Fer; JANCZ, Carla. *BARRICADES STRATEGIES AND COLLECTIVENESS: A digital security primer for organizations*. Marialab, São Paulo, December 1, 2022. Available at: <https://www.marialab.org/wp-content/uploads/2020/12/Barricas-collective-strategies.pdf>. Accessed on: July 13, 2024.

55. *Cookies* These are files created by websites to collect information about users' internet browsing. They can be used for user convenience, storing logins and passwords and items added to virtual shopping carts, for example. For more details, see: G1. *What are internet cookies and how do they work?*. G1, 09 Jun. 2024. Available at: [https://g1.globo.com/tecnologia/noticia/2024/06/09/o-que-sao-cookies-na-internet-e-como-eles-trabalhom.ghtml](https://g1.globo.com/tecnologia/noticia/2024/06/09/o-que-sao-cookies-na-internet-e-como-eles-trabalham.ghtml). Accessed on: June 24, 2024.

56. *CRIMINALS sell data from the CGU and Ministry of Health on the dark web*. [S. l.], 21 Dec. 2021. Available at: <https://canaltech.com.br/seguranca/criminosos-vendem-dados-do-cgu-e-ministerio-da-saude-na-dark-web-204985/>. Accessed on: June 27, 2024.

57. TEFFÉ, Chiara de. *Sensitive personal data: Qualification, processing and good practices*. Indaiatuba, Sao Paulo, 2022. np

58. Federal Court of Auditors. *Five Cybersecurity Controls for Yesterday*/Federal Court of Auditors. -Brasília: TCU, 2022. 36 pp1. Available at: <https://portal.tcu.gov.br/5-controles-de-seguranca-cibernetica.htm>. Accessed on: July 6, 2024.

59. GOLDONI, Luiz RF; RODRIGUES, KF; MEDEIROS, BP What is the future of cybersecurity governance in Brazil. *Contemporary Brazil*. São Paulo, v. 29., 2024. p. 8-10.

### 3. Current Legislative Panorama

Cyber policies are essential in a governance approach that demands institutional structures aimed at solving public problems in an undefined context of attributions and responsibilities. In this scenario of multiple actors, the role of public administration must be to direct and guide actions. These mechanisms must act by defining clear objectives, assigning responsibilities and developing improvements in actions and policies to promote information security. In other words, it is necessary for the Federal Government to standardize guidelines, promote public policies and assign responsibilities to the competent bodies and entities.<sup>60</sup>

The National Cybersecurity Policy (PNCiber) was implemented precisely to respond reactively to the current insecurity scenario through the development of regulatory and inspection mechanisms, international cooperation strategies, development of training and education in cybersecurity, among others.<sup>61</sup> However, it is essential to emphasize that other measures were adopted before the publication of PNCiber, and it is necessary to clarify them to enable a more precise analysis of this scenario in Brazil.

Firstly, it is worth highlighting that in the context of data protection in Brazil, Article 5 of the Federal Constitution stands out, which provides for the inviolability of people's private life, privacy, honor and image.<sup>62</sup>; the Civil Code, which provides for the inviolability of private life<sup>63</sup>; and the Internet Civil Rights Framework – Law 12,965/2014 –, a pioneer in establishing rights and duties for the use of the internet<sup>64</sup>. The latter already provided for the protection of personal data as a principle of internet use in its article 3, paragraphs II and III.<sup>65</sup> However, even with its enactment, the need for specific and consolidated regulations on the processing of personal data still loomed over Brazil.<sup>66</sup>

60. Ibid. 2-3.

61. Ibid. pp. 10-11.

62. BRAZIL. [Constitution (1988)]. *Constitution of the Federative Republic of Brazil*. Brasília, DF: Senado Federal, 2016. 496 p. Available at: [planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://planalto.gov.br/ccivil_03/constituicao/constituicao.htm) . Accessed on June 1, 2024.

63. BRAZIL. Law 10,406, of January 10, 2002. Institutes the Brazilian Civil Code. *Official Gazette of the Union*. Brasília: Presidency of the Republic. Available at: [planalto.gov.br/ccivil\\_03/leis/2002/l10406compilada.htm](http://planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm) . Accessed on January 5, 2024.

64. LORENZON, Laila Neves. Comparative analysis between personal data regulations in Brazil and the European Union (LGPD and GDPR) and their respective enforcement instruments. *Journal of the European Union Law Programme*, [S. l.], p. 1-14, 15 Mar. 2021. p. 41-42.

65. BRAZIL. Law No. 12,965, of April 23, 2014. Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil. *Official Gazette of the Union*. Brasília: Presidency of the Republic. Available at: [https://www.planalto.gov.br/ccivil\\_03/ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm) . Accessed on: June 7, 2023.

66. MENDES, Laura Schertel. Protection of personal data: basis, concepts and application model. *Internet Sector Overview*, [S. l.], year 11, n. 2, p. 1-20, Jun. 2019. p. 2-4. Available at: [https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama\\_setorial\\_ano-xi\\_n\\_2\\_privacidade\\_e\\_dados\\_pessoais.pdf](https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf) . Accessed: Jul. 2024.

This is why the General Data Protection Law (LGPD) was enacted in 2018, with the aim of establishing minimum cybersecurity standards in Brazil (Pinheiro, 2024). This important legislation, which preceded the PNCiber (Brasil, 2018a), proved to be a major pioneering instrument in the Brazilian scenario by establishing a standard of conduct to be adopted by personal data processors in favor of protecting fundamental rights, human dignity, and the right to privacy of data subjects (Lóssio, 2020). It came as an instrument capable of ensuring the protection of personal data, which until then had not been effectively ensured by other instruments. In addition, the LGPD supported the development of public policies to control the processing of this data, since an insecure scenario in the digital environment is becoming increasingly unacceptable, nationally or internationally. The aforementioned legislation also brought as a novelty the protection of users' privacy against companies that store excessive amounts of information (Braga, 2021).

Even so, the LGPD presented some problems. Its late implementation, for example, resulted in a considerable level of data circulation, and it can be said that the lack of attention to cybersecurity at the beginning of the 21st century culminated in a lag that still does not keep up with the exponential technological growth (Braga, 2021). Nevertheless, when establishing a practical analysis of risk analysis in the LGPD, it is much more a practice of regulatory adequacy aimed at achieving the *accountability*<sup>67</sup> and reduce the likelihood of imposing sanctions than an effective concern about possible harm to users' rights. Therefore, the overlap that occurs during the analysis of the risks of a search for technical and regulatory adequacy instead of protecting users' fundamental rights is a valid concern.<sup>68</sup>

Because of this, several Decrees originated in the Brazilian scenario, among them E-Digital (Decree 9,319/2018)<sup>69</sup>; Decree No. 10,046/2019<sup>70</sup>, which provides for governance in data sharing within the federal public administration; the Digital Government Strategy for the years of

67. Set of practices aimed at holding the entire data processing chain accountable. For more details see: MEN-DES, Laura Schertel. Personal data protection: basis, concepts and application model. *Internet Sector Overview*, [S. l.], year 11, n. 2, p. 1-20, Jun. 2019. Available at: [https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama\\_setorial\\_ano\\_xi\\_n\\_2\\_privacidade\\_e\\_dados\\_pessoais.pdf](https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano_xi_n_2_privacidade_e_dados_pessoais.pdf). Accessed: Jul. 2024.

68. GOMES, Maria Cecília O. Between method and complexity: understanding the notion of risk in the LGPD. In Current issues in data protection. PALHARES, Felipe (Coord.). São Paulo: *Thomson Reuters Brazil*, 2020, pp 245-271. p. 258.

69. BRAZIL. Decree No. 9,319 of March 14, 2018. Amends Decree No. 8,777 of May 11, 2016, which establishes the National Consumer Protection and Defense Policy. Official Gazette of the Union, Brasília, March 15, 2018. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/decreto/D9319.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.htm). Accessed on: June 1, 2024.

70. BRAZIL. Decree No. 10,046 of September 30, 2019. Amends Decree No. 9,203 of November 22, 2017, which regulates Law No. 13,334 of September 13, 2016. Official Gazette of the Union, Brasília, October 1, 2019. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/decreto/d10046.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm). Accessed on: June 1, 2024.

2020 to 2022 (Decree No. 10,332/2020)<sup>71</sup>; the publication of the National Cybersecurity Strategy, or E-Ciber (Decree 10,222/2020)<sup>72</sup>; and the approval of the National Security and Critical Infrastructure Plan, through Decree No. 11,200<sup>73</sup>. E-Digital is a landmark in the area of cybersecurity, as it proposes significant improvements to Brazil's cyber infrastructure.<sup>74</sup> Promotes adequate access to technology and digital inclusion throughout the national territory, in urban and rural areas, proposes development and innovation initiatives, in addition to determining the protection of users' rights and privacy and fostering the need for security in the digital environment, encouraging education and professional training.<sup>75</sup>

The PNCiber was also preceded by the publication of Decree 9,637/2018, which established the National Information Security Policy (PNSI), updated in 2021 by Decree No. 10,641. The PNSI was an important policy at the national level, with the scope of strengthening the culture of information security in society and encouraging professional qualification in the area of information security.<sup>76</sup> We can interpret it as the basis of cyber governance in Brazil, as it established information security on a large scale, incorporated the principles of integrity, confidentiality and guaranteed availability of information. Furthermore, it encouraged the creation of a national cybersecurity policy with the participation of the public and private sectors.<sup>77</sup>

In this sense, the PNSI foresees the importance of creating a national information security strategy (E-Cyber)<sup>78</sup>. The national strategy, together with the national plans, constituted the instruments of the PNSI that established the participation of society, public bodies and entities and assigned

71. BRAZIL. Decree No. 10,332 of April 28, 2020. Provides for the creation of the National Program to Support Employment and Income Generation. Official Gazette of the Union, Brasília, April 29, 2020. Available at:[https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/deceto/d10332.htm#:~:text=DECRETO%20N%C2%BA%2010.332%2C%20DE%2028,fundamental%20e%20d%C3%A1%20others%20provid%C3%AAs](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/deceto/d10332.htm#:~:text=DECRETO%20N%C2%BA%2010.332%2C%20DE%2028,fundamental%20e%20d%C3%A1%20others%20provid%C3%AAs). Accessed on: June 7, 2024.

72. BRAZIL. Decree No. 10,222, of February 5, 2020. Approves the National Cybersecurity Strategy. Official Gazette of the Union, Brasília, 2020. Available at:[https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/deceto/d10222.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/deceto/d10222.htm). Accessed on: June 7, 2024.

73. GOLDONI, Luiz RF; RODRIGUES, KF; MEDEIROS, BP What is the future of cybersecurity governance in Brazil. *Contemporary Brazil*. São Paulo, v. 29., 2024. p. 4-8.

74. Ibid.

75. Decree No. 9,319 of March 21, 2018. (2018). Institutes the National System for Digital Transformation and establishes the governance structure for the implementation of the Brazilian Strategy for Digital Transformation. Brasília, DF.

76. Ibid.

77. GOLDONI, Luiz RF; RODRIGUES, KF; MEDEIROS, BP What is the future of cybersecurity governance in Brazil. *Contemporary Brazil*. São Paulo, v. 29., 2024. p. 5.

78. BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B. Cybersecurity: A systemic vision towards a regulatory framework proposal for a digitally sovereign Brazil. 1st ed. *FGV Law School Rio*, Ag. 2023. Available at:<https://diretorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil>. Accessed on: June 24, 2024. p.12.

as the competence and responsibility of the institutional security office of the Presidency of the Republic the preparation and publication<sup>79</sup>. Article 6 of the PNSI determines the structure of the National Information Security Strategy, divided into the following modules: cyber defense; security of critical infrastructures; security of confidential information; and protection against data leaks. The PNSI was also concerned with ensuring the protection of users' fundamental rights against possible data leaks, establishing as one of its principles the protection of personal data and privacy throughout its article 3, item II.<sup>80</sup>

The National Critical Infrastructure Security Plan (Decree No. 11.200/2022)<sup>81</sup> addresses the essential nature of risk management for the security of critical infrastructures, with the determination of a systemic methodology to identify, assess and treat risks. Due to the amount of information, it establishes the need for constant monitoring and timely action in crisis scenarios to adopt appropriate measures. It also promoted the need for integration and cooperation between the public and private sectors and established an Integrated Critical Infrastructure and Security Data System, through which the Security of Brazil's Critical Infrastructure will be permanently monitored and tracked, through specific methodologies for identifying, monitoring and providing data on risk alerts and analyses.<sup>82</sup>

However, Belli et al<sup>83</sup> highlights that for Brazil to become a digitally sovereign nation, it is essential to create a digital sovereignty strategy based on cybersecurity and strategic investments. Because of this, in May 2023 a draft was published by the Institutional Security Office providing for the creation of the PNCiber. This draft was extensive, more than the published Decree, and contained in its content the need to unify the “patchwork” of the Brazilian reality of cybersecurity regulation<sup>84</sup>.

79. Decree No. 9,319 of March 21, 2018. (2018). Institutes the National System for Digital Transformation and establishes the governance structure for the implementation of the Brazilian Strategy for Digital Transformation. Brasília, DF.

80. Ibid.

81. BRAZIL. Decree No. 11,200, of September 30, 2022. Provides for the regulation of public policies. Official Gazette of the Union: Brasília, DF. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_Ato2019-2022/2022/Decreto/D11200.htm#:~:text=DECREE%20N%C2%BA%2011.200%2C%20DE%2015,de%20Seguran%C3%A7a%20de%20Infraestruturas%20Cr%C3%ADticas](https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm#:~:text=DECREE%20N%C2%BA%2011.200%2C%20DE%2015,de%20Seguran%C3%A7a%20de%20Infraestruturas%20Cr%C3%ADticas). Accessed on: June 1, 2024.

82. Ibid.

83. BELLI, Lucca; Bakonyi Erica; Chen Larissa, et al. Cybersecurity: a systemic vision towards a regulatory framework proposal for a digitally sovereign Brazil. Rio de Janeiro: *FGV Law School Rio*, 2023, p. 13.

84. GOLDONI, Luiz RF; RODRIGUES, KF; MEDEIROS, BP What is the future of cybersecurity governance in Brazil. *Contemporary Brazil*. São Paulo, v. 29., 2024. p. 9.

Therefore, PNCiber was created with the aim of guiding national cybersecurity activities through the establishment of governance methods, guidelines and actions aimed at cybersecurity in Brazil.<sup>85</sup> The principled part of PNCiber is embodied in the guarantee of fundamental rights, sovereignty and national interests, the resilience of public and private organizations, education and technological development and cooperation, both between public and private entities and internationally, on the subject of cybersecurity.<sup>86</sup>

As already explained, the LGPD itself has previously supported the protection of the fundamental rights of civil society in the use of the internet by establishing practices to be adopted by all those who process user data.<sup>87</sup> In this way, the policy in question rectified the importance of protectionism for the fundamental rights of users, also being concerned with the need to maintain national sovereignty, technological education and cooperation among the entire social class.<sup>88</sup>

Among the objectives of the National Policy, preventive actions focused on training and education of society in general, the promotion of scientific research, technological development, innovation in the area of cybersecurity, the need for coordinated action and the exchange of information on cybersecurity between the three Powers (Legislative, Executive and Judiciary), between the Federative Entities (States, Union, Municipalities and Federal District), between the public and private sectors and between society in general stand out.<sup>89</sup> In other words, PNCiber has a strong focus on preventive actions against incidents, not only to train public agents and private organizations, but society in general, promoting education and technical training as ways of providing society with knowledge in cybersecurity.<sup>90</sup>

Thus, the PNCiber establishes objective principles and also institutes in its article 5 the National Cybersecurity Committee (CNCiber) to promote

85. PINHEIRO, Patricia PG *Cybersecurity, Society and the Future*. Computing Brazil, [S. l.], p. 67-70, 1 jun. 2024.p. 69.

86. Decree No. 11,856 of December 26, 2023. (2023). *Establishes the National Cybersecurity Policy and the National Cybersecurity Committee*. Brasilia, DF.

87. BRAZIL. Law No. 13,709, of August 14, 2018. *General Personal Data Protection Law (LGPD)*. Official Gazette of the Union. Brasília: Presidency of the Republic. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm) . Accessed on: November 7, 2023.

88. Decree No. 11,856 of December 26, 2023. (2023). *Establishes the National Cybersecurity Policy and the National Cybersecurity Committee*. Brasilia, DF.

89. Ibid..

90. Ibid..

the unification of measures in this area<sup>91</sup>. Pine tree<sup>92</sup> highlights that the influence that the Internet exerts on the global economy demands the application of robust cybersecurity standards, and it was this need that gave rise to the intention of creating a cybersecurity ecosystem through CNCiber. This committee aims to implement, promote and update the measures provided for in the National Policy, since cybersecurity needs to be continually adapted and readjusted through the application of ethical development principles and the adoption of preventive measures<sup>93</sup>. The Committee, therefore, is responsible for evaluating and proposing measures on the topic of cybersecurity in Brazil, formulating proposals for the prevention of cyber incidents, promoting education and dialogue on cybersecurity and international cooperation in this area.<sup>94</sup>.

However, it is important to note that the draft that provided for the creation of PNCiber did not address the main instruments that already existed, such as PNSI and E-Ciber, and was silent on vital points for the implementation of governance measures for Brazilian cybersecurity. This is a symptom of the current Brazilian legislative reality in cybersecurity, which is numerous and full of scattered legislation and decrees, but not necessarily guiding, clear and objective.<sup>95</sup>.

In other words, this shows that current legislation is still not capable of expressly relating regulatory content to each other in pursuit of a common objective.<sup>96</sup>, highlighting the importance of the advent of PNCiber, which brought with it a new direction for rapid and coordinated action among all those responsible, with a guiding bias towards cybersecurity in Brazil, based on governance and risk management guidelines and methods<sup>97</sup>. It is true that any diagnosis regarding the National Cybersecurity Policy is still immature, given its recent publication, but it is immediately possible to observe that it seeks to achieve a standardization of action in the Brazilian cybersecurity scenario, assigns responsibilities to competent bodies and entities and promotes social education and preventive actions against cyber incidents.

91. Ibid..

92. PINHEIRO, Patricia PG *Cybersecurity, Society and the Future*. Computing Brazil, [S. l.], p. 67-70, 1 jun. 2024.p. 68.

93. Ibid. p. 69.

94. Decree No. 11,856 of December 26, 2023. (2023). *Establishes the National Cybersecurity Policy and the National Cybersecurity Committee*. Brasilia, DF.

95. GOLDONI, Luiz RF; RODRIGUES, KF; MEDEIROS, BP What is the future of cybersecurity governance in Brazil. *Contemporary Brazil*. São Paulo, v. 29., 2024. p. 11.

96. Ibid.

97. PINHEIRO, Patrícia PG *Cybersecurity, Society and Future*. Computing Brazil, [S. l.], p. 67-70, 1 jun. 2024.p. 69-70.

## Final Considerations

From all of the above, it is possible to understand that there is no ready-made recipe to be followed in the scope of cybersecurity and data protection that can be applied indiscriminately and that will ensure the existence of a scenario of full digital security, especially because, in view of the constant technological development, the assessment and management of digital risks becomes an almost uninterrupted practice. However, general action should be based on the awareness of social classes about the need to follow basic precepts of cybersecurity, knowing how to properly identify what is a risk, how to mitigate it and which fundamentals should be observed and legislative mandates when processing and storing data, so as not to incur a high-risk scenario, with greater vulnerability to valuable information in today's society.

Over the last decade, a true ecosystem has been built to regulate technologies and actions in the digital environment in Brazil. From the enactment of the Brazilian Internet Bill of Rights - which this year completes its first decade of validity - to the LGPD, which has been a true milestone in data protection nationwide, to the publication of Decrees in the area of cybersecurity as already mentioned throughout the third chapter, which culminated in the publication of the PNCiber. In other words, measures that seek, broadly speaking, to standardize procedures, raise awareness in the public and private spheres about the need for professional training, the importance of the joint efforts of all those involved in the issue and the urgency of adopting predictive measures, in addition to bringing to civil society the idea of urgent acculturation and education about the use of the internet in everyday life, including preventive actions for cybersecurity and protection of data, but which must be put into practice with a focus on the true protection of rights rather than mere procedural and regulatory adaptation.

In order to reach a more comfortable scenario in terms of cybersecurity, it is essential that the public itself is aware that there is a real and imminent threat, since it is up to each of us, as users, developers or system administrators, to adopt preventive actions, good practices, attention to possible vulnerabilities and governance mechanisms capable of supporting the analysis, monitoring and contingency of existing risks. It is no coincidence that the entire Brazilian regulatory framework mentioned throughout this work contains provisions regarding the promotion of education and training of users. In addition, it is clear

the ongoing need to develop legal mechanisms, as they actively contribute to preventing digital security incidents, and the concern with the actual application of risk analysis by those responsible, going beyond the sphere of mere regulatory adequacy.

Today, we are able to view cybersecurity as an international issue that seeks to mitigate the risks inherent to its use and, as a result of technology, crosses borders and affects a range of disciplines with serious economic, political, legal and social impacts on the mitigation of fundamental rights. Thus, cybersecurity is just one layer of internet governance that concerns itself with technological, political and legal standards and rules; it is also an ongoing and multidisciplinary process. In short, the significant changes brought about by the increased use of the internet in the 21st century have led to important transformations in human interactions and have implied the need to adapt the concept of risk and global regulations to protect user data, ensure support in the event of incidents, assign those responsible and adopt measures to continually mitigate digital risks capable of causing serious harm to civil society and the public sector and private organizations.

There is no denying the high number of Brazilian regulations on cybersecurity and data protection, constituting a truly broad regulatory scenario, but without much interrelation and assertiveness in protecting the rights of data subjects. In this sense, the recently published National Policy aims to unify guidelines and orientations in order to guarantee the application of good practices and preventive actions for possible incidents and provide effective protection of fundamental rights. Finally, we cannot forget the need for risk assessment to be carried out in a manner that is faithful to the protection of those who are inherently more vulnerable, the data subjects, avoiding an unfair distribution of these risks to society, which can cause social disasters and harm the basic rights of users.

## Bibliographic References

ALMEIDA, João Emílio de. Cybersecurity: from risk prevention to incident management. *RISTI - Iberian Journal of Information Systems and Technologies*, Porto, ed. 43, p. 1-4, 30 Sep. 2021. DOI 10.17013/risti.43.1-4. Available at: <https://scielo.pt/pdf/rist/n43/1646-9895-rist-43-1.pdf> . Accessed on: May 2, 2024.

BECK, Ulrich; *Risk society: towards another modernity*. New York: Routledge, 2011.

BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B. *Cybersecurity: A systemic vision towards a regulatory framework proposal for a digitally sovereign Brazil*. 1st ed. Rio de Janeiro: Rio de Janeiro: FGV Direito Rio, Ag. 2023. Available at:<https://diretorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil> . Accessed on: June 24, 2024.

BITTAR, ECB Theory of Law, the Digital Age and the Post-Human: the new status of the body under a technological regime and the emergence of the Post-Human Subject of Law. *Law and Praxis Journal*, v. 10, no. 2, p. 933–961, jun. 2019.

BRAGA, Noelson Araujo. *CYBERSECURITY AND THE RIGHT TO PRIVACY: A Study on Cybernetic Construction in Brazil and the European Union from a Realist Perspective*. 2021. Monograph (Bachelor's Degree in International Relations)-UNIVERSITY OF BRASILIA INSTITUTE OF INTERNATIONAL RELATIONS, [S. l.], 2021. Available at:[https://bdm.unb.br/bitstream/10483/30829/3/2021\\_NoelsonAraujoBraga\\_tcc.pdf](https://bdm.unb.br/bitstream/10483/30829/3/2021_NoelsonAraujoBraga_tcc.pdf) . Accessed on: July 3, 2024.

BRAZIL. [Constitution (1988)]. Constitution of the Federative Republic of Brazil. Brasília, DF: Federal Senate, 2016. 496 p. Available at:[planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://planalto.gov.br/ccivil_03/constituicao/constituicao.htm) . Accessed on June 1, 2024.

BRAZIL. Law 10,406, of January 10, 2002. Institutes the Brazilian Civil Code. *Official Gazette of the Union*. Brasília: Presidency of the Republic. Available at:[planalto.gov.br/ccivil\\_03/leis/2002/l10406compilada.htm](http://planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm) . Accessed on January 5, 2024.

BRAZIL. Law No. 12,965, of April 23, 2014. Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil. *Official Gazette of the Union*. Brasília: Presidency of the Republic. Available at:[https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm) . Accessed on: June 7, 2023.

BRAZIL. Law No. 13,709, of August 14, 2018. General Personal Data Protection Law (LGPD). *Official Gazette of the Union*. Brasília: Presidency of the Republic. Available at:[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm) . Accessed on: November 7, 2023.

CRIMINALS sell data from the CGU and the Ministry of Health on the dark web. [S. l.], 21 Dec. 2021. Available at:<https://canaltech.com.br/seguranca/criminosos-vendem-dados-do-cgu-e-ministerio-da-saude-na-dark-web-204985/> . Accessed on: June 27, 2024.

Decree No. 9,319 of March 21, 2018. (2018). *Institutes the National System for Digital Transformation and establishes the governance structure for the implementation of the Brazilian Strategy for Digital Transformation*. Brasilia, DF.

Decree No. 10,222 of February 5, 2020. (2020). *Approves the National Cybersecurity Strategy*. Brasilia, DF.

Decree No. 10,046 of September 30, 2019. *Amends Decree No. 9,203 of November 22, 2017, which regulates Law No. 13,334 of September 13, 2016*. Official Gazette of the Union, Brasília, October 1, 2019. Available at:[https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/decreto/d10046.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm) . Accessed on: June 1, 2024.

Decree No. 10,641 of March 2, 2021. (2021). Amends Decree No. 9,637 of December 26, 2018, which institutes the National Information Security Policy, provides for information security governance, and amends the Decree No. 9,637, which regulates the provisions of art. 24, caput, item IX, of Law No. 8,666 of June 21, 1993, and provides for the waiver of bidding in cases that may compromise national security. Brasília, DF.

Decree No. 11,200 of September 15, 2022. (2022). *Approves the National Critical Infrastructure Security Plan*. Brasilia, DF.

Decree No. 11,856 of December 26, 2023. (2023). *Establishes the National Cybersecurity Policy and the National Cybersecurity Committee*. Brasilia, DF.

FICHTNER, Laura. What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, Germany, v. 7, p. 1-19, 15 May 2018. DOI 10.14763/2018.2.788. Available at: <https://policyreview.info/articles/analysis/what-kind-cyber-security-theorising-cyber-security-and-mapping-approaches> . Accessed on: June 3, 2024.

G1. STJ calls on PF to investigate possible hacker attack on the court system. *G1*, 4 Nov. 2020. Available at: <https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataque-de-hackers-ao-sistema-do-tribunal.ghtml> . Accessed on: July 2, 2024.

G1. What are cookies on the internet and how do they work? *G1*, June 9, 2024. Available at: <https://g1.globo.com/tecnologia/noticia/2024/06/09/o-que-sao-cookies-na-internet-e-como-they-work.ghtml> . Accessed on: June 24, 2024.

GIDDENS, A.; PLINIO DENTZIEN. *Modernity and identity*. New York, NY: Routledge, 2002.

GOLDONI, LRF; RODRIGUES, KF; MEDEIROS, BP What is the future of cybersecurity governance in Brazil? *Public Management and Citizenship Notebooks*, v. 29, p. e90972–e90972, 17 Apr. 2024.

GOMES, Maria Cecília O. Between method and complexity: understanding the notion of risk in the LGPD. *In Current data protection topics*. PALHARES, Felipe (Coord.). New York: Thomson Reuters, 2020, pp. 245-271.

LATTO, Nica. *What is a computer virus?* [S. l.], 12 Feb 2020. Available at: <https://www.avast.com/pt-br/c-computer-virus#:~:text=Um%20v%C3%ADrus%20de%20computer%20%C3%A9,a%20others%20arquivos%20ou%20documentos> . Accessed on: July 17, 2024.

LHUMANN, Niklas. *Risk: A sociological Theory*. 1st ed. New York: [sn], 2017. Available at: [https://www.researchgate.net/publication/345677301\\_Risk\\_A\\_Sociological\\_Theory](https://www.researchgate.net/publication/345677301_Risk_A_Sociological_Theory) . Accessed on: June 8, 2024.

LINKNATIONAL. *What is spam?* National Link, October 20, 2023. Available at: <https://www.linknacional.com.br/blog/o-que-e-spam/> . Accessed on: June 24, 2024.

LORENZON, Laila Neves. Comparative analysis between personal data regulations in Brazil and the European Union (LGPD and GDPR) and their respective enforcement instruments. *Journal of the European Union Law Programme*, [S. l.], p. 1-14, 15 Mar. 2021.

LOSSIUS, Claudio Joel Brito. *Digital compliance and data protection: preserving rights in the information society*. Dissertation (Master in Law) - Autonomous University of Lisbon

Luís de Camões, Lisbon, 2020. Available at:<https://repositorio.ual.pt/handle/11144/4621> . Accessed on: July 10, 2024.

LUCCA, Newton de. Human dignity and electronic risks. *Galileu - Journal of Law and Economics*, [s.l], v. 7, p. 283-312, Jan. 2012. Available at:<https://journals.ual.pt/galileu/wp-content/uploads/2019/02/Galileu-XVII-1-2-2012-Miolo-FINAL.pdf> . Accessed on: July 17, 2024.

MARCON, Daniele Verza. *Cyber Risk Insurance: challenges to define the guarantee and promote cybersecurity in the digital age*. 2023. Dissertation (Master in Legal and Social Sciences) - Universidade Federal do Rio Grande do Sul, [S. l.], 2023. Available at:<https://lume.ufrgs.br/handle/10183/267969> . Accessed on: July 3, 2024.

MENDES, Laura Schertel. Protection of personal data: basis, concepts and application model. *Internet Sector Overview*, [S. l.], year 11, n. 2, p. 1-20, Jun. 2019. Available at:[https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama\\_setorial\\_ano\\_xi\\_n\\_2\\_privacidade\\_e\\_dados\\_pessoais.pdf](https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano_xi_n_2_privacidade_e_dados_pessoais.pdf) . Accessed: Jul. 2024.

PIMENTEL, José Eduardo de Souza. Introduction to Digital Law. *Legal Journal of the Higher School of the Public Prosecutor's Office of São Paulo*, v. 13, no. 1, p. 16-39, 17 Sept. 2018.

PINHEIRO, Patricia Peck Garrido. CYBERSECURITY, SOCIETY AND THE FUTURE. *Computing Brazil*, [S. l.], p. 67-70, June 1, 2024.

*Problems with ConecteSUS: before the hacker attack, the system was controversial due to data changes and failures*. Available at: <<https://g1.globo.com/saude/noticia/2021/12/10/problemas-no-conectesus-antes-de-ataque-hacker-sistema-teve-polemica-com-alteracao-de-dados-e-falhas.ghtml> >.

SAMPAIO, Dhiego Rhubens Lima. *A STUDY ON INFORMATION SECURITY RISKS ON THE UFC CAMPUS IN QUIXADÁ BASED ON THE ISO/IEC 27005 STANDARD*. 2014. Monograph (Bachelor's Degree in Information Systems) - Federal University of Ceará, Quixadá, CE, 2014. Available at: <https://repositorio.ufc.br/handle/riufc/25039> . Accessed on: June 7, 2024.

SHIRA, Fer; JANCZ, Carla. BARRICADES STRATEGIES AND COLLECTIVITY: A digital security primer for organizations. *Marialab*, São Paulo, December 1, 2022. Available at:<https://www.marialab.org/wp-content/uploads/2020/12/Barricas-estrategias-coletividade.pdf> . Accessed on: July 13, 2024.

Federal Court of Auditors. *Five Cybersecurity Controls for Yesterday*/Federal Court of Auditors. - Brasília: TCU, 2022. 36 p. Available at:<https://portal.tcu.gov.br/5-controles-cyber-security.htm> . Accessed on: July 6, 2024.

TEFFÉ, Chiara de. *Sensitive Personal Data: Qualification, Treatment and Good Practices*. Indaiatuba, SP: Foco, 2022. 304 p. Available at:[https://www.google.com.br/books/edition/Dados\\_Pessoais\\_Sens%C3%ADveis/atCLEAAQBAJ?hl=ptBR&qbpv=1&dq=inauthor:%22Chiara+Spadaccini+de+Teff%C3%A9%22&printsec=frontcover](https://www.google.com.br/books/edition/Dados_Pessoais_Sens%C3%ADveis/atCLEAAQBAJ?hl=ptBR&qbpv=1&dq=inauthor:%22Chiara+Spadaccini+de+Teff%C3%A9%22&printsec=frontcover) . Accessed on: June 28, 2024.

**Cyberchildhood and  
Social Cybersecurity: In Search of  
Improvement  
protecting children and  
adolescents on the Internet**

Ligia Maria de Souza Lopes Reis

Summary: Introduction. 1. General framework: context and data. 2. Regulatory framework. 2.1. Differentiated data collection. 2.2. Excessive exposure. 3. Future framework. 3.1. Digital cybersecurity and regulatory future. Final considerations. Bibliographical References

## Introduction

This article aims to analyze how Brazil has advanced in the construction of a regulatory framework that aims to protect children and adolescents in digital environments, seeking to shed light on possible normative contributions to the improvement of social cybersecurity. Based on the study of Laws 12.965/2014 (Civil Rights Framework for the Internet) and 13.709/2018 (General Data Protection Law), it presents advances, gaps and impacts of these regulations on the use of digital platforms by these groups. In addition, it seeks to understand Brazilian Bill 2628/2022 and the American legislative proposal *Kids Online Safety Act (Kosa)*, analyzing whether they actually offer the intended improvement in both digital protection and cybersecurity. Thus, the discussion is structured in three parts: the current scenario of children and adolescents on social networks, the impact of these platforms on their lives and regulatory proposals aimed at a safer digital future.

## 1. Big picture: context and data

Brazilian children and teenagers have been accessing the internet at an increasingly early age. According to TIC Kids Online Brasil 2023<sup>2</sup>, 24% of children and adolescents in the country report having started using the world wide web in early childhood, that is, before the age of six<sup>3</sup>. Sum-  
- to this other alarming finding. A study conducted by Nielsen<sup>4</sup>, on request

1. Communications expert with a master's degree in Regulatory Communication Policies from the University of Brasília (UnB). Specialist in International Relations from UnB and Public Administration from the National School of Public Administration (Enap). Federal civil servant of the National Council of the Public Prosecutor's Office (CNMP) since 2011, seconded to work at the Federal Supreme Court (STF). Currently studying a postgraduate degree in Digital Law (partnership between the Rio Institute of Technology and Society and the Center for Studies and Research in Law at the State University of Rio de Janeiro) and a degree in Law.

2. Carried out by the Regional Center for Studies for the Development of the Information Society (Cetic.br), of the Information and Coordination Center of Ponto BR (NIC.br), linked to the Internet Steering Committee in Brazil (CGI.br), since 2012. For the 2023 edition, the survey interviewed, in person, 2,704 children and adolescents between the ages of 9 and 17, in addition to parents or guardians, throughout the national territory in 2022.

3. INFORMATION AND COORDINATION CENTER OF THE BR POINT (NIC.br). Research on Internet use by children and adolescents in Brazil: TIC Kids Online Brazil 2023 [electronic book]. ed. São Paulo: Brazilian Internet Steering Committee, 2024.

4. American company that performs measurement, data collection and global audience analysis of traditional and digital media to assess trends and behaviors.

from Google, reveals low adherence of parents and guardians to parental controls<sup>5</sup> in Brazil, guaranteed in the national regulatory system since the enactment of Law 12,965/2014. In 2023<sup>6</sup>, only 17% of adults interviewed in the survey knew about and used technological means of access control.

Unsupervised online browsing, low literacy and low awareness of these users involve numerous risks, some of which have already been mapped by experts, such as excessive data collection, overexposure of images and encouragement of consumption. These actions affect users without the necessary digital skills, such as knowledge of rights and cybersecurity tools.<sup>7</sup>, something essential for the conscious and defensive use of networks. After all, children and adolescents are people in formation and, therefore, they have specific constitutional protection in Brazil, stated in article 227 of the CRFB. The text states:

It is the duty of the family, society and the State to ensure that children, adolescents and young people, with absolute priority, have the right to life, health, food, education, leisure, professional training, culture, dignity, respect, freedom and family and community life, *as well as protecting them from all forms of neglect, discrimination, exploitation, violence, cruelty and oppression*.<sup>8</sup>

In an attempt to address the effects caused by the acceleration of contemporary changes, the Public Authorities have issued regulations specifically aimed at the digital environment, such as Law 12,965/2014, better known as the Internet Civil Rights Framework (MCI) and Law 13,709/2018, known as the General Data Protection Law (LGPD), just to name a few.<sup>9</sup> In addition to these measures, there is the action of public bodies, such as the National Secretariat for the Rights of Children and Adolescents, of the Ministry of Human Rights and Citizenship, and the National Data Protection Authority (ANPD), which in 2023 issued a statement to standardize the interpretation of the LGPD regarding the legal hypotheses that authorize the processing of data from children and adolescents. Despite these efforts, inconsistencies and paradoxes are perceived.

5. Parental control is a mechanism used by adults to control children's access to different websites, operating systems or computers. Through this, it is possible to monitor browsing, restrict content that is inappropriate for minors, and block pages or users that may pose a threat to children.

6. Available at <https://bit.ly/3VRHPyr>

7. According to the Gartner glossary, cybersecurity is the combination of people, policies, processes and technologies employed by an organization to protect its cyber assets against digital attacks and threats.

8. BRAZIL. Federal Constitution, art. 227, *caput*.

9. In January 2024, Law 14.811/2024 was enacted, the purpose of which is to protect children and adolescents against violence, especially in educational or similar environments. The regulation includes specific measures that aim to increase the safety of young people in virtual environments, as it adds new provisions on digital crimes against these groups to the Penal Code.

According to the *Global Digital Report 2024*<sup>10</sup>, Brazil occupies the second position in the *ranking of countries with users over 16 who spend the most time online and the fifth place globally in Instagram usage*. The behavior of older people is replicated by younger people: in addition to starting their digital life at an increasingly early age, Brazilian children under 13 prefer TikTok<sup>11</sup>.

The finding is surprising, since this social network is classified as 12+ years old in the stores that provide the application for *download*. And this limit is not, by any means, a random cut. According to the Statute of Children and Adolescents (ECA), a child is considered to be any person up to twelve years of age and adolescents, and from that age up to 18 years of age, they are - if you consider her a teenager.

The use of social media by children and adolescents has seen notable growth in Brazil in recent years. According to the CGI, in 2021, 78% of young people aged 9 to 17 who used the internet accessed social media, which represents an increase of ten percentage points compared to 2019, when it was recorded 68%. For comparison purposes, a study carried out in the United Kingdom in 2021 by Ofcom - an acronym in English for *The Office of Communications*<sup>12</sup>-, indicated that 33% of children aged 5 to 7 have their own profiles on social networks. This number rises to 60% among children aged 8 to 11, 89% among those aged 12 to 15 and 94% among adolescents aged 16 to 17.

## 2. Regulatory framework

To say that the internet is not regulated in Brazil is untrue and misleading. The fact is that different regulations apply to the digital environment, such as the LGPD and the MCI. Depending on the subject, other regulations may apply to the digital environment, such as the one that deals with copyright. In the case of the rights of children and adolescents, an important set of rules can be invoked to protect them.

### 2.1 Differentiated data collection

The advancement of the 21st century and new communication technologies has brought not only changes to the flow of information and the production of knowledge,

10. WE ARE SOCIAL. Digital 2024: 5 billion social media users. Full content in English at <https://bit.ly/3VRTYUf>.

11. According to the *TIC Kids Online Brazil 2023*, This is the preferred social network for 46% of respondents aged 11 to 12 (CETIC.BR, 2023).

12. This is the UK communications regulatory agency, the content of which is cited at <https://bit.ly/Ofcom2024>.

ment, but it also changed people's behavior, including children's.

Living in an increasingly digital world, young people have found digital networks, online games, and social media platforms *streaming*, other ways to distract themselves, inform themselves and have fun, different from those sought by their parents. Still according to the *TIC Kids Online Brazil 2023*, 95% of the population aged 9 to 17 declared being an internet user in the country, which represents 25 million people. The main means for this is the cell phone, according to the response of 97% of these users<sup>13</sup>.

Regarding data collection on the internet, the General Data Protection Law can be understood as a general and transversal rule, which permeates different processing agents and affects several categories of data subjects, among which are those who require special regulation and protection - children and adolescents. The combination of articles 5, item X and LXXIX, and 227, of the CRFB, with article 17, of the ECA, gave rise to a chapter of the LGPD entirely dedicated to addressing these groups.

Law 13.709/2018 determines that the processing of personal data of children and adolescents be carried out in their best interest (art. 14). Here, the best interest refers to the reflection on the vulnerability and the need for care, by the family, society and the State, of children and adolescents (art. 227, *caput*, of the Federal Constitution of 1988, combined with art. 4 of the ECA). This general law also establishes that the controller<sup>14</sup>, in collecting data from these groups, will act

only through practices that promote and protect their rights, provided for in the national and international legal system, with absolute priority, abstaining from practices that exploit the vulnerability of children and adolescents, including commercial ones<sup>15</sup>.

The best interests must be respected in the context of personal data protection, since this guarantee refers to personality rights. Thus, "its indiscriminate use [data collection] is capable of objectifying people, affecting personality development, promoting manipulation

13. INFORMATION AND COORDINATION CENTER OF THE BR POINT (NIC.br). Research on Internet use by children and adolescents in Brazil: TIC Kids Online Brazil 2023 [electronic book]. ed. São Paulo: Brazilian Internet Steering Committee, 2024.

14. Natural or legal person, under public or private law, responsible for decisions regarding the processing of personal data, as stated in art. 5, item VI, of the LGPD.

15. HENRIQUES, I.; PITA, M.; HARTUNG, P. Protection of personal data and child vulnerability. São Paulo: Editora ABC, 2022, p. 213.

and generate discrimination”<sup>16</sup>. And when risks involve the primordial phases of human development,

the issue must be addressed taking into account, also, the special legal protection afforded to children and adolescents, who, by constitutional force, must have their rights assured with absolute priority<sup>17</sup>.

The LGPD also requires that the processing of children's personal data must be carried out with the specific and prominent consent given by at least one of the parents or legal guardian (art. 14, § 1). The doctrine clarifies that parental consent must be given as a free, informed, unequivocal manifestation and also comply with the principle of purpose, as established in art. 5, XII, of the legal system, “regardless of whether it is carried out by mothers, fathers or legal guardians”<sup>18</sup>.

There are only two cases in which personal data of children and adolescents may be processed without the consent of at least one of their parents or legal guardian: 1) when the collection is necessary to contact them, but this may occur only once and without storage; and 2) when it is necessary to protect the life of the child or adolescent. However, in no case may the data be passed on to a third party without the consent of one of the aforementioned guardians (art. 14, §3).

The general law also establishes that the controller has the duty to make all reasonable efforts to verify that consent has been given by the person responsible for the child, considering the available technologies (art. 14, § 5). Additionally, this processing agent must keep public information about the types of data collected, the way they are used and the procedures for the full exercise of the rights of these data subjects (art. 14, § 2), which complies with the principle of transparency and purpose, since it provides them with full awareness of the procedures and uses of what belongs to them, namely, their data.

As these are people in training, information about data processing must be provided in a simple, clear and accessible manner, taking into account the physical-motor, perceptive, sensory, intellectual and mental characteristics of the user. Audiovisual resources must be used when

16. MENDES, SARLET, RODRIGUES JR. *Personal Data Protection Treaty*. São Paulo: Ed. ABDR, 2023, p.211.

17. *Ibid.*, p.211.

18. *Ibid.*, p.214.

appropriate, in order to provide the necessary information to the parents or legal guardian and adequate to the child's understanding (art. 14, §6º). Furthermore, controllers must not condition the participation of children and adolescents in games, internet applications or other activities on the provision of personal information, beyond that strictly necessary for the activity (art. 14, §4º).

Regarding the rights of data subjects, as set out in art. 18 of the LGPD and which also reach this audience, five of the nine clauses set out in the standard stand out: 1) confirmation of the existence of processing for complete and unequivocal knowledge of at least one of the parents or legal guardian; 2) correction of incomplete, inaccurate or outdated data, considering especially the development of the data subject; 3) anonymization, blocking or deletion of unnecessary, excessive data or data processed in non-compliance with the LGPD, given the aspect of the transience of the relationship; 4) deletion of personal data processed with the consent of the data subject; and 5) information on the possibility of not providing consent and on the consequences of refusal.

The exercise of these rights must be aligned with the principles of the LGPD, among which five of the ten present in the law are listed, as they are considered especially important in the processing of data of children and adolescents: 1) adequacy, which is the compatibility of the processing with the purposes informed to the data subject, according to the context of the processing; 2) purpose, which aims to meet legitimate, specific, explicit purposes informed to the data subject, without the possibility of subsequent processing in a manner incompatible with these purposes; 3) necessity, which refers to the limitation of the processing to the minimum necessary to achieve its purposes, with coverage of pertinent, proportional and non-excessive data in relation to the purposes of the data processing; 4) transparency, that is, the guarantee offered to the data subjects of clear, precise and easily accessible information about the performance of the processing and the respective processing agents, observing commercial and industrial secrets; and 5) accountability and rendering of accounts, referring to the demonstration, by the agent, of the adoption of effective measures capable of proving observance and compliance with personal data protection standards and, including, the effectiveness of these measures.

It is worth noting that the most current doctrine defends more restrictive rules for the management of personal data of these groups.

Restrictive interpretations, which make the protection of children's data equivalent to 'consent to data processing',

exempt states, companies and other organizations from liability for the harmful use of personal data and privacy violations. There is a power imbalance between the efforts of data collectors to capture greater amounts of data and the ability of families and children to protect themselves in an increasingly complex digital world<sup>19</sup>.

## 2.2 Overexposure

Uncontrolled exposure of children to social networks generates phenomena and behaviors that require reflection. One of them is preference profiling, which, in short, means offering content and products based on the user's browsing on the platform. Another is the risk of isolating this person who is still developing in discussion bubbles, which can contribute to the worsening of social and political polarization and the reduction of diversity of opinions,<sup>20</sup> increased intolerance, spread of misinformation, among other social effects.

Far beyond improving existing economic strategies, such as classifications and profiling (*profiling*) and how the *targeting marketing*, the processed data have implications that can lead to the total modification of the economic, social and political scenario<sup>21</sup>.

The unassisted presence of these users, lacking educational tools and skills for reflection and criticism, can mean opening virtual doors to criminals. There are already reports of new methods, such as “digital kidnapping,” which occurs when someone steals photos of children from the Internet and publishes them as if they were of their own children. Ten years ago, these crimes had not yet become issues to be resolved when the first and main legal instrument aimed at the Internet, the Internet Civil Rights Framework (MCI), was issued. And it is not that it should deal with crimes, since the MCI is a regulation for civil relations, as can be inferred. However, it is the first specific Brazilian law on the Internet and, as such, it could have looked more closely to the future, which necessarily involves the protection and

19. Free translation of text taken from the document *The Case for Better Governance of Children's Data: A Manifesto*, published by the United Nations Children's Fund (UNICEF, 2021). Available at <https://bit.ly/3RQXpJG>.

20. Experts have drawn attention to content generated by artificial intelligence (AI) aimed at children, which circulates on social media and is distributed by algorithms. These products are considered to be of low quality, in terms of content and pedagogy, and contain biases and little diversity.

21. FRAZÃO, A. In: FERNANDES, E.; TEFFÉ, CS de; BRANCO, S. (Coords.). *Privacy and Data Protection of Children and Adolescents*. Rio de Janeiro: Rio de Janeiro Institute of Technology and Society; Obliq, 2021, p.87.

protection of the life and development of children and adolescents. But that is not what is seen in the text.

Law 12.965/2014 is the first legislation to establish principles, guarantees, rights and duties for the use of the internet in Brazil. It consists of 32 articles and is structured in five chapters, but there is no specific one to deal with children, as in the LGPD. However, the MCI sought, in a certain way, to contribute to the creation of a safer digital environment for children and adolescents. Article 26 states that the fulfillment of the constitutional duty of the State in providing education, at all levels of education, includes training, integrated with other educational practices, for the safe, conscious and responsible use of the internet as a tool for the exercise of citizenship, the promotion of culture and technological development.

The MCI can also be used to protect children and adolescents in cases of flagrant sexual violence, such as intimate images or scenes of nudity. And not because of the literal meaning of the rule, but as a consequence of the interpretation, since in these cases the ECA is applied in conjunction with article 21 of the MCI.<sup>22</sup> Case law considers that any dissemination of images of children and adolescents in situations of nudity or with sexual connotations constitutes a serious crime, as provided for in article 241-A of the ECA. It also understands that it is the responsibility of the internet provider to remove the infringing content, even if produced by third parties. This is what can be read in the case law of the Superior Court of Justice (STJ)<sup>23</sup>.

The application provider is civilly liable if, after being notified, it does not remove offensive content involving minors, regardless of a court order, as the principle of full protection of children and adolescents prevails over the Internet Civil Rights Framework.<sup>24</sup>

Another provision that deserves mention is article 19, whose constitutionality analysis awaits judgment, within the scope of the Extraordinary Appeal (RE)

22. The text states that the internet application provider that makes content generated by third parties available will be held subsidiarily liable for the violation of privacy resulting from the disclosure, without the authorization of its participants, of images, videos or other materials containing scenes of nudity or sexual acts of a private nature when, after receiving notification from the participant or their legal representative, they fail to diligently promote, within the scope and technical limits of their service, the unavailability of such content.

23. See Jurisprudence in Theses, Edition No. 224. Available at <https://bit.ly/3WdtIVO>. In order to complete, it is worth highlighting that, according to the STJ, pornographic exposure without consent, as stated in the Internet Civil Rights Framework, is not limited to total nudity, nor to sexual acts that only involve carnal intercourse, but to conduct that may cause harm to the victim's personality.

24. The text refers to the following provisions: article 19 of Law 12,965/2014; articles 17 and 18 of the ECA; and articles 5, X, and 227 of the Federal Constitution. See REsp 1,783,269/MG, available at <https://bit.ly/3xO7Pmr>

1,037,396 of the Federal Supreme Court (STF)<sup>25</sup>. The provision states that, in order to ensure freedom of expression and prevent censorship, the internet application provider may only be held civilly liable for damages resulting from content generated by third parties if, after a specific court order, it fails to take steps to, within the scope and technical limits of its service and within the specified timeframe, make the content identified as infringing unavailable, except for legal provisions to the contrary. This legal basis treats the provider's liability as subjective, assessing it by its omission when it fails to remove the offensive content from the air, after due judicial notification. It is worth remembering that the STJ has already stated that “the liability of internet application providers for content generated by third parties is subjective and becomes joint and several when, after judicial notification, the removal of the offensive material is denied or delayed”<sup>26</sup>.

Regarding the protection of the groups studied here and the literalness of the text, the MCI states that the user will have the option of free choice in the use of a computer program on his terminal to exercise parental control of content that he understands as inappropriate for his minor children, as long as the principles of the ECA (Law 12.965/2014, art. 29) are respected. Considering that only 17% of all parents interviewed in the aforementioned Nielsen study<sup>27</sup> having declared that they know and use technological means of access control as a way of making the experience of minors safer, this device alone seems to be insufficient to deal with the challenges imposed on children and young people in the current reality.

Finally, it is noted that the term “child” appears only twice in the MCI and occurs in the final provisions – almost as if, finally, the legislator had remembered to look to the future. According to the text, it is up to the public authorities, together with internet connection and application providers and civil society, to promote education and provide information on the use of computer programs provided for in the MCI. *caput* of article 29, as well as for the definition of good practices for the digital inclusion of children and adolescents. A text that is as principled as it is vague, as can be seen.

25. This is RE 1,037,396, Topic 987 of general repercussion, reported by Justice Dias Toffoli, and discusses whether Article 19 of the Brazilian Civil Rights Framework for the Internet is constitutional or not. This article requires that a specific court order be issued before websites, internet providers and social media applications are held liable for harmful content published by other people.

26. See Jurisprudence in Theses, Edition No. 222. Available at <https://bit.ly/3RUyDYR>

27. See comment on footnote 3.

### 3. Future framework

As we have seen, Brazil has regulations in place to protect children and adolescents in the digital environment, but progress is still needed. Building a safe environment depends on individual and collective decisions that protect both groups and social structures. From this perspective, regulatory innovations are now being addressed.

#### 3.1 Digital cybersecurity and regulatory future

One of the most consensual concepts of cybersecurity was developed by the Telecommunications Standardization Sector of the UN's International Telecommunication Union, known by its English acronym ITU-T. According to the specialized agency of the United Nations (UN), the term refers to the set of tools, policies, security concepts, guidelines, risk management approaches, actions, training, best practices, guarantees and technologies that can be used to protect the assets of the cyber environment, the organization and its users.<sup>28</sup>

Thus, when understood from technical aspects, cybersecurity refers to the protection of computers, networks, software applications and operating systems from possible digital threats. However, when interpreted from other fields, such as applied social sciences<sup>29</sup>, the term can include meanings that encompass measures to defend the sovereignty (including digital) of countries, respect for fundamental human rights, and impacts on people's well-being and mental health.

Social cybersecurity would then be an emerging field that arises in response to digital threats and cybersecurity challenges, focusing on

characterize, understand, and predict changes in human behavior and social, cultural, and political outcomes mediated by cyber environments; and build a societal cybersecurity infrastructure that enables the essential character of a society to persist in a cyber-mediated information environment characterized by changing conditions, threats of

28. From the ITU-T glossary, available at <https://encurtador.com.br/uEcAn>

29. Sandra Friberg, professor of civil law at *Uppsala University*, argues that cybersecurity is not just a technical issue and recalls that the topic is highlighted in different points of EU legislation, including the new Artificial Intelligence Act (*AI Act*) and other legislation around the world. The researcher notes that these regulations aim to create measures and defenses against cyber threats that challenge countries' sovereignty and respect for fundamental human rights. For this reason, she believes that broad collaboration between technical experts, lawyers and other social scientists is necessary to understand the issue. Available at <https://encurtador.com.br/o6D0u>

actual or imminent social cybersecurity threats, and cyber-mediated threats<sup>30</sup>.

This is an emerging subdomain of cybersecurity and national security that arises in response to the growing impact of cyber influence on today's societies, in which beliefs, opinions, behaviors and trends are significantly shaped by digital dynamics and interactions.<sup>31</sup> From this, social cybersecurity has objectives aimed at anticipating phenomena, such as 1) characterizing, understanding and predicting changes, mediated by technologies, in human behavior and in social, cultural and political dynamics and 2) building a *social cyber infrastructure (highlighted)* that allows society to preserve its essential character in an information environment mediated by technologies<sup>32</sup>.

Another meaning considers cybersecurity as a broad field of study that encompasses others, in addition to including essential dimensions, such as supervision and governance, research, operation and maintenance, protection and defense, also dedicating itself to the protection of life, property and information security, as defended by Aguilar and Fonseca.<sup>33</sup>

By studying the technological impacts in the school context, the authors advocate a broader understanding and training in cybersecurity, focused on the conscious and healthy use of the internet, especially in childhood and adolescence.

This conceptual expansion is what allows for the didactic, informed and coordinated action of parents, the school community and other members of the context. It is based on teaching and appropriation of guidelines for the use and security of networks, definition of browsing times at school and at home, safety rules and prevention of social engineering actions and combating online violence, among other measures.

The actors in the process can work with different types of knowledge, both theoretical, scientific and technological, as well as

30. BESKOW, DM; CARLEY, KM Social cybersecurity: an emerging science. 2019, p.1. *The original text in English says the following: "As noted by the National Academies of Science NAS (2019): Social cybersecurity is an applied computational social science with two objectives - 'characterize, understand, and predict cyber-mediated changes in human behavior and in social, cultural, and political outcomes; and build a social cyber infrastructure that will allow the essential character of a society to persist in a cyber-mediated information environment that is characterized by changing conditions, actual or imminent social cyberthreats, and cyber-mediated threats'".*

31. *Idem*, p.3.

32. *Ibid.*.

33. ASTORGA-AGUILAR, C.; SCHMIDT-FONSECA, I. *Dangers of social networks: How to educate our young men and women in cyber security. Educare*[online], v. 23, no. 3, p. 339-362, 2019. Epub 30 Oct. 2019.

those provided by the groups participating in the process and by society itself. In terms of teaching and knowledge, it is necessary for children and adolescents to acquire knowledge about cybersecurity applied to social networks, but, above all, to appropriate and internalize this learning, so that this information passes to their cognitive structures, in order to identify dangers on the network<sup>34</sup>.

According to the *The Global Risk Report 2024 - 19th edition*<sup>35</sup>, cyber risk will be the fourth biggest threat to countries in the next two years and the eighth in the next ten. In the context of contemporary society and its complex problems, the perspective of social cybersecurity offers, for example, the possibility of using “computational social science techniques to identify, combat and measure (or evaluate) the impact of communication objectives”<sup>36</sup>, and it is even possible to use it to analyze and promote safer and healthier digital environments for children and adolescents.

This is why governments around the world are increasingly interested in developing national cybersecurity strategies (NCS) that are capable and effective in addressing and preventing a wide range of cybersecurity issues in an integrated and efficient manner. According to the Organization of American States (OAS), developing a NSC is essential to dealing with cyber threats and developing desirable measures to prevent them.<sup>37</sup> In Brazil, the national cybersecurity strategy, created in 2020, is undergoing review and, at the end of 2023, was incorporated into the National Cybersecurity Plan (PNCiber), with the publication of Decree 11,856/2023.

There are also researchers who relate social cybersecurity to the protection of information systems and networks against attacks by criminals, whose social engineering techniques<sup>38</sup> exploited human vulnerabilities. Thus, this new area of research would respond to the cybernetic effects of current

34. *Idem*. Free translation of the original text in Spanish: *The actors of the process can work with different types of knowledge, both theoretical, scientific and technological, as well as those that contribute to the groups participating in the process and society itself. In relation to teaching and knowledge, it is required that children and adolescents obtain knowledge about cyber security applied to social networks, but mainly they take ownership and interiorize with learning, in a way that provides information to their cognitive structures in order to identify dangers online.*

35. WORLD ECONOMIC FORUM. *The Global Risks Report 2024* [e-book]. Cologny/Geneva: World Economic Forum, 2024.

36. BESKOW, DM; CARLEY, KM Social cybersecurity: an emerging science. 2019, p.2. In the original, the text says: “*Social cybersecurity uses computational social science techniques to identify, counter, and measure (or assess) the impact of communication objectives.*”

37. See the proposed OAS cybersecurity program at <https://www.oas.org/ext/en/security/proq-cyber>

38. Social engineering refers to tactics used to manipulate people into revealing confidential information or taking actions that compromise security. Examples include phishing, pretexting, and other forms of deception that aim to influence human behavior. More information at <https://bit.ly/3L8Iih8>

ality using applied research and different areas of knowledge, such as communication, data science, law, behavioral economics, statistics, among others, in order to analyze new technologies and respond to internet phenomena.

Social cybersecurity can also investigate how influence and manipulation of beliefs, behaviors and public trust take place within digital platforms, and how social groups can be protected from this. Methods and results from this research domain can be critical for policymakers and academics, as their applied theoretical components have the potential to constitute high-dimensional network analyses.<sup>39</sup>, machine learning, natural language processing and agent-based simulation<sup>40</sup>.

Along these lines, Wu *et al.* define social cybersecurity as a field that studies behaviors and threats to security and privacy in an ecosystem of interconnectivity and social influence, recognizing the domain of social interactions and seeking to create security systems that are more aligned with the practices and social needs of users. Among other issues, they explain that families and households exhibit complex practices when it comes to sharing content, including that of their children. And that conceptions about what is sensitive or not vary between families, which also differ on access control mechanisms to combat violations that affect the sensitivity of children and adolescents.<sup>41</sup>

However, users often iteratively adapt their ideal access control policies rather than conforming to those initially reported, suggesting that access control policies, *a priori*, may be insufficient in the domestic context<sup>42</sup>.

39. High-dimensional network analysis is a technique and method used to study and understand complex networks that involve multiple dimensions or attributes. These networks are not limited to simple connections between nodes (as in a common social network), but consider several layers of data and types of interactions, in addition to their complexities and dimensions. They use mathematical models and algorithms and can be applied to social networks and cybersecurity.

40. In the field of regulation of emerging technologies, the case of *AI Act* European that mentions cybersecurity 45 times in its text. In one of the passages the European authority states that *Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behavior, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities*. Available at [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf)

41. U, YW; EDWARDS, K.; DAS, S. SoK: Social Cybersecurity. In: 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022, p. 1863-1879, p. 4. Here is the original text, in English: *However, users often iteratively adapt their ideal access control policies rather than settle on the initial ones they reported, suggesting that a priori access control policies may be insufficient within the household context*

42. *Idem*.

The authors conclude that ignoring human social behaviors when designing systems and regulations can lead to inappropriate behaviors and reduced safety, while designing and using human social behaviors in these contexts can mean increased effectiveness and action of these systems and regulatory standards.

On this topic, Bill 2628/2022, authored by Senator Alessandro Vieira, is currently being processed in the National Congress, which proposes more protective measures for children and adolescents in digital environments. Among the suggested changes, the following stand out: the requirement that digital platforms adopt, by default, strict settings for data collection; the determination that technology services aimed at children and adolescents offer simple and effective parental control mechanisms; the prohibition of the practice of reward boxes (*loot boxes*) in electronic games and advertising to children - which is already prohibited by the Consumer Protection Code, but the text restricts communication elements that may induce consumption; the provision of creating mechanisms for reporting and removing content that violates the rights of children and adolescents, regardless of a court order. The proposal faces criticism regarding the technical feasibility of measures such as age verification on social networks and content monitoring, in addition to possible interference with family autonomy.

Another example is the US legislative proposal *Kids Online Safety Act (Kosa)*, an unprecedented and historic proposition that defends the improvement of online security for children and adolescents through the modification of the *design* of the platforms, something quite adherent to social cybersecurity. It also proposes the non-use of recommendation systems based on algorithms and the creation of a new responsibility or duty of care<sup>43</sup> for applications and digital platforms, specifically with regard to content that is unsuitable for minors.

The bill, which has been in the US legislature for over two years, is divided between supporters in the Senate and significant opposition from human rights organizations and internet freedom groups. Amendments to the bill sought to appease detractors, but were not considered sufficient. Critics believe that the bill still has some flaws.

43. Expression that refers to the legal obligation of digital platforms to take reasonable measures to protect users from harm, ensuring that their operations do not cause harm and that any harmful content or behavior is properly monitored and managed. This includes preventing abuse, protecting privacy, ensuring security against exploitation, and promoting a safe digital environment. The "duty of care" is also contemplated in Bill 2628/2022, as it provides for a more protective configuration by default, child monitoring, creation of mechanisms for reporting and removal of content that violates the rights of children and adolescents without the need for a court order, among other things.

ta risks of censorship and excessive restrictions, especially for marginalized communities<sup>44</sup>. Opponents like the *Center for Democracy and Technology* and the *Electronic Frontier Foundations* say they fear that the bill's vague language could lead to excessive content moderation and, consequently, harm vulnerable communities<sup>45</sup>, such as LGBTQ+ youth.

That said, it is stated that the *Kosa* can be considered a social cybersecurity instrument, since it addresses both technical security and the social and behavioral aspects of online safety for children and adolescents. Among other objectives aligned with social cybersecurity to protect human interactions in the digital environment, the document addresses, for example: 1) the regulation of content and design, as already mentioned, with a view to helping create a safer online environment, in which potentially harmful content is less likely to be promoted; 2) education and awareness, as it proposes the inclusion of guidance from a diverse group of stakeholders, including parents, academic experts, health professionals and young social media users, in addition to recognizing the need to equip users with the knowledge and tools to navigate safely in the digital environment<sup>46</sup>; and 3) protection against manipulation and misinformation, through the implementation of security mechanisms and the requirement that social networks adopt specific measures to protect young users.

## Final considerations

The increasing integration of children and adolescents into the digital universe requires a transdisciplinary, multifaceted and multidimensional approach, encompassing education, regulation, technology, cybersecurity, and other dimensions that enable the paving of paths oriented towards protection and healthier and more human digital experiences. This requires strengthening the regulatory environment, with specific standards, policies and plans, that

44. "The Kids Online Safety Act, if passed, would require social media platforms to reduce online dangers by changing their design or opting out of algorithm based recommendation systems.[5] It aims to create liability or a "duty of care" for apps and social networking platforms for specific content that may not be suitable for minors. If the entities behind these Internet platforms fail to filter said content from minors, they might be open for legal action against them". Available at <https://abre.ai/katO>

45. "Rather than protecting children, this could impact access to protected speech, causing a chilling effect for all users and incentivizing companies to filter content on topics that disproportionately impact marginalized communities," said Prem M Trivedi, policy director at the Open Technology Institute, which opposes Kosa. In "New text, same problems: inside the fight over child online safety laws". Available at <https://abre.ai/katP>

46. It is worth noting that the proposal is similar to Article 29, sole paragraph, of the Brazilian Civil Rights Framework for the Internet. The text states that "[i]t is the responsibility of the public authorities, together with Internet connection and application providers and civil society, to promote education and provide information on the use of computer programs provided for in the caput, as well as to define good practices for the digital inclusion of children and adolescents."

not only prohibit specific harmful practices, such as excessive data collection and profiling carried out by algorithms, but also promote a digital culture more favorable to human development.

In view of this, even if subject to criticism, regulatory innovations such as those proposed in PL 2628/2022 and in *Kosac* can be seen as social cybersecurity instruments, because they seek to address digital threats beyond technological issues. However, it should not be forgotten that the effectiveness of regulations will depend on the capacity for implementation and monitoring. Specific regulatory standards can certainly contribute to improving the protection of these groups in the digital environment, but they will certainly lack measures, protocols and policies that help develop connections and ecosystems that are favorable to the presence of young people.

In this regard, it is important to highlight the importance of collaboration between governments, educators, parents and digital service providers to create a safer and more enriching digital environment for children and adolescents, something stated in the Internet Civil Rights Framework but not yet implemented in Brazil. As technology continues to evolve, so must the understanding, means and instruments for protecting people's well-being, especially the most vulnerable, such as children and adolescents. Only this coordination between these social agents will be able to offer both young people and their families the security and confidence necessary for digital experiences.

Integrating social cybersecurity into the debate on cyberchildhood is essential, as children and adolescents are particularly vulnerable to content, influences, and manifestations in the digital ecosystem. They are frequently exposed to algorithms, disinformation, and digital manipulation, so protection strategies for these groups must include not only technical measures, but also social and behavioral measures, in addition to digital education initiatives that address the social nature of cyber threats. Educational programs that prioritize digital literacy and promote awareness of technological risks can positively address other emerging challenges beyond digital networks, such as the use and applications of artificial intelligence.

Thus, it was observed that social cybersecurity, although it is an emerging field of research, must be studied and explored in order to formulate and propose a combination of lenses, concepts, approaches, methods of applied social sciences and computational engineering to build infrastructures.

and more resilient, conscious and adherent social instruments to user behavior. As a result, it is possible to protect society and its groups more effectively, as well as to keep its dynamics and institutions free (or less vulnerable) from technological risks.

## References

ASTORGA-AGUILAR, C.; SCHMIDT-FONSECA, I. *Dangers of social networks: How to educate our young men and women in cyber security*. Educare [online], v. 23, n. 3, p. 339-362, 2019. Epub Oct. 30, 2019. Available at: <https://bit.ly/PeligrosRedes2019> . Accessed: June 2024.

BRAZIL. *Federal Constitution*. Available at: <https://l1nk.dev/Qzkdl> . Accessed: June 2024.

\_\_\_\_\_. *Law No. 12,965, of April 23, 2014*. Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm) . Accessed: June 2024.

\_\_\_\_\_. *Law No. 8,098 of September 11, 1990*. Provides for consumer protection and other measures. Available at: [https://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm) . Accessed: Jul. 2024.

\_\_\_\_\_. *Decree No. 7,962 of March 15, 2013*. Regulates Law No. 8,078 of September 11, 1990, to provide for contracting in electronic commerce. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/decreto/d7962.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm) . Accessed: Jul. 2024.

\_\_\_\_\_. *Law No. 13,709, of August 14, 2018*. General Data Protection Law (LGPD). Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm) . Accessed: Jul. 2024.

\_\_\_\_\_. *Law No. 13,257, of March 8, 2016*. Legal Framework for Early Childhood. Available at: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2016/lei/l13257.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13257.htm) . Accessed: May 2024.

\_\_\_\_\_. *Bill 2628/2022*. Protection of children and adolescents in digital environments. Available at: <https://www25.senado.leg.br/web/atividade/materias/-/materia/154901> . Accessed: Jul. 2024.

\_\_\_\_\_. *PL 2630/2020*. Fake News Law. Available at: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944> . Accessed: Jul. 2024.

\_\_\_\_\_. *SUPERIOR COURT OF JUSTICE*. Jurisprudence in Theses, Edition No. 222. Available at: [https://scon.stj.jus.br/SCON/jt/doc.jsp?livre=%27222%27.tit.&\\_gl=1%2a1tyc6aj%2a\\_ga%2aMTU2MzYxNzq0OS4xNjQ2MzQ5MDAy%2a\\_ga\\_F31N0L6Z6D%2aMTY5NjQ1NTI4OS-40MTguMS4xNjk2NDU](https://scon.stj.jus.br/SCON/jt/doc.jsp?livre=%27222%27.tit.&_gl=1%2a1tyc6aj%2a_ga%2aMTU2MzYxNzq0OS4xNjQ2MzQ5MDAy%2a_ga_F31N0L6Z6D%2aMTY5NjQ1NTI4OS-40MTguMS4xNjk2NDU) . Accessed: June 2024.

\_\_\_\_\_. *SUPERIOR COURT OF JUSTICE*. Jurisprudence in Theses, Edition No. 224. Available at: <https://scon.stj.jus.br/SCON/jt/doc.jsp?livre=%27224%27.tit> . Accessed: June 2024.

ALANA, Institute. *Child and Consumption Program*. Available at: <https://criancaeconsumo.org.br/> . Accessed: June 2024.

\_\_\_\_\_. *About Alana Institute*. Available at: <https://alana.org.br/> .

ANGELINE, K.; BARBOSA, A.; SENNE, F.; DINO, LA *Privacy and Data Protection of Children and Adolescents*. Rio de Janeiro: Rio de Janeiro Institute of Technology and Society; Obliq, 2021. Available at: <https://d26k070p771odc.cloudfront.net/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf> . Accessed: May 2024.

BELLI, L.; COUTO, N.; CHEN, L.; FRANQUEIRA, B.; BAKONYI, E.; CHANG, S.; DA HORA, N.; GAS-PAR, W. *Cybersecurity [electronic resource]: a systemic vision towards a regulatory framework proposal for a digitally sovereign Brazil*. Rio de Janeiro: FGV, Rio Law, 2023.

BESKOW, D.M.; CARLEY, K.M. *Social cybersecurity: an emerging science*. 2019. Available at: <https://apps.dtic.mil/sti/citations/AD1108494> . Accessed: June 2024.

FGV, Getulio Vargas Foundation. *Guide to the Processing of Data on Children and Adolescents*. Available at: [https://portal.fgv.br/sites/portal.fgv.br/files/criancas\\_e\\_adolescentes.pdf](https://portal.fgv.br/sites/portal.fgv.br/files/criancas_e_adolescentes.pdf) . Accessed on: [access date missing].

FRAZÃO, A. In: FERNANDES, E.; TEFFÉ, C.S. de; BRANCO, S. (Coords.). *Privacy and Data Protection of Children and Adolescents*. Rio de Janeiro: Rio de Janeiro Institute of Technology and Society; Obliq, 2021. Available at: <https://bit.ly/3xGBo9v> .

HENRIQUES, I.; PITA, M.; HARTUNG, P. *Personal Data Protection Treaty*. New York: Routledge, 2023.

LATERÇA, PS; FERNANDES, E.; TEFFÉ, CS de; BRANCO, S. (Coords.). *Privacy and Data Protection of Children and Adolescents*. Rio de Janeiro: Rio de Janeiro Institute of Technology and Society; Obliq, 2021. Available at: <https://d26k070p771odc.cloudfront.net/wp-content/uploads/2021/10/Privacy-and-Data-Protection-of-Children-and-Teenagers-ITS.pdf> .

MEDIUM & MESSAGE. *Only 17% of parents use tools to monitor their children online*. Available at: <https://www.meioemensagem.com.br/midia/sobre-17-dos-pais-usam-ferramentas-para-monitorar-filhos-na-internet> . Accessed: May 2024.

NIELSEN. *Measurement, data collection and global audience analysis of traditional and digital media to assess trends and behaviors*. Available at: <https://www.tiktok.com/business/pt-BR/blog/tiktok-funciona-meta-analise-nielsen> . Accessed: May 2024.

BR POINT INFORMATION AND COORDINATION CENTER (NIC.br). *Research on Internet use by children and adolescents in Brazil: TIC Kids Online Brasil 2023 [e-book]= Survey on Internet use by children in Brazil: ICT Kids Online Brazil 2023*. 1st ed. São Paulo: Brazilian Internet Steering Committee, 2024. Available at: <https://bit.ly/TicKids2023> . Accessed: June 2024.

PRINSKY, M. *Digital Natives*. Available at: [https://pt.wikipedia.org/wiki/Nativo\\_digital](https://pt.wikipedia.org/wiki/Nativo_digital) . Accessed: May 2024.

SOUZA, J.; NOVELLI, A.; CASTRO, J. *Regulatory framework to combat fake news in Brazil: an analysis of legislative proposals*. Ibero-American Journal of Information. Available at: <https://periodicos.unb.br/index.php/RICI/article/view/45659/35275> . Accessed: May 2024.

TIKTOK. *Community Guidelines*. Available at: <https://www.tiktok.com/creators/creator-portal/pt-br/community-guidelines-and-safety-pt-br/diretrizes-da-comunidade/> . Accessed: May 2024.

UNICEF. *The Pulse Check on Digital Learning*. Available at: <https://www.unicef.org/media/132096/file/Pulse%20Check.pdf> . Accessed: June 2024.

WORLD ECONOMIC FORUM. *The Global Risks Report 2024 [eBook]*. Cologny/Geneva: World Economic Forum, 2024. Available at: <https://www.weforum.org/publications/global-risks-report-2024/> . Accessed: Jul. 2024.

WU, YW; EDWARDS, K.; DAS, S. *SoK: Social Cybersecurity*. In: 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022, p. 1863-1879. Available at: <https://ieeexplore.ieee.org/abstract/document/9833757> . Accessed: Jul. 2024.

UNICEF. *The Case for Better Governance of Children's Data: A Manifesto*. Available at: <https://ajudador.com.br/mD60s> . Accessed: June 2024.

WE ARE SOCIAL. *Digital 2024: 5 billion social media users*. Available at: <https://wearesocial.com/uk/blog/2024/01/digital-2024-5-billion-social-media-users/> . Accessed: June 2024.

DIÁLOGOS DA  
PÓS-GRADUAÇÃO  
EM DIREITO DIGITAL

18

**The legal bases in the system  
of collecting information on  
diversity in Health  
and in Digital Health**

Maira Lima de Souza

Summary: Introduction. 1. Health Information Systems and Digital Health. 2. Diversity information. 2.1. The trajectory of diversity as social information. 3. Methodology. 4. Legal bases and the incorporation of diversity in Health Systems. 4.1. The trajectory of diversity as social information. 4.2. Ethnicity. 4.3. Lesbians, Gays, Bisexuals, Transvestites and Transsexuals (LGBT). Final considerations. References.

## Introduction

This article discusses how the legal frameworks adopted by the Brazilian government influence the collection of information on diversity in electronic health records generated by the main national Information Systems (SIS) and how this influence impacts the quality of information in the context of Digital Health. In addition to influencing the collection, these legal frameworks also impact the official recognition of certain social categories.

Diversity information portrays the composition of a population in relation to categories such as ethnicity/racial identity, gender, sexual orientation, and migration/nationality, among others. The word “diversity” has been used as an umbrella term, broad enough to include minorities and vulnerable populations, as well as to recognize human differences<sup>2</sup>.

Diversity data can be categorized as cultural (e.g., shared norms and behaviors), biological (e.g., age, gender), and defined in personal terms (e.g., sexual orientation, religion)<sup>3</sup>.

Health information systems, through forms or registration forms, collect this information. However, this record does not follow

1. PhD in Knowledge Dissemination (UFBA), Master in Ethnic and African Studies (UFBA), graduated in Computer Science (UNIFACS) and certified in Privacy and Data Protection by Data Privacy Brasil (2024). I work in the field of science, technology and humanities, working on the themes: policy, governance and data management and decoloniality. I am also a member of the research group on Science and Network Theory, entitled *Gossip & Rumors* (<http://redessociaiscomplexas.org>). I am a Senior Data Curator (*data steward*), focusing on the treatment of sensitive data and diversity, and I lead the Data Curation Center of the Center for Data Integration and Knowledge for Health (Cidacs/Fiocruz BA), the center with the largest collection of government administrative data among all low- and middle-income countries in the world, linked to the Oswaldo Cruz Bahia Foundation. My work ranges from supervising a multidisciplinary team of curators, developing policies and sociotechnical models for data curation for public health projects, to curating research projects in compliance with the LGPD, defining measures that guarantee the safe use of data, in accordance with ethics and legislation.

2. BALESTRA, C.; Fleischer, L. *Diversity statistics in the OECD: how do OECD countries collect data on ethnic, racial and indigenous identities?*. OECD Statistics Working Papers, No. 2018/09, Paris: OECD Publishing, 2018. Available at: <https://doi.org/10.1787/89bae654-en>. Accessed on: April 21, 2023. P.6.

3. BALESTRA, C.; Fleischer, L. *Diversity statistics in the OECD: how do OECD countries collect data on ethnic, racial and indigenous identities?*. OECD Statistics Working Papers, No. 2018/09, Paris: OECD Publishing, 2018. Available at: <https://doi.org/10.1787/89bae654-en>. Accessed on: April 21, 2023. P.7.

a linear or uniform trajectory. Although the definition of the fields present in these forms is decisive for the collection, the connection of these fields with the identity process makes this process more complex.

Health information systems have functioned as instruments for the production of raw data for the construction of statistical indicators on the population. Examples include the Mortality Information System (SIM), the Live Birth Information System (SI-NASC) and the Notifiable Diseases Information System (SINAN). These systems are the most representative and are among the oldest in the context of the Unified Health System (SUS)<sup>4-5</sup>.

Individually, these systems allow the mapping of aspects such as mortality, birth and diseases in a given context. When combined, they capture comprehensive information about the life trajectory, from birth, through the onset of diseases and up to death. Within the scope of Digital Health, SIS can participate in interoperability and modernization strategies, such as those provided for in the e-SUS Linha da Vida Program.<sup>6</sup> Within the scope of e-Health, they feed the active transparency portals<sup>7</sup>.

Just as SIS do not serve the entire assistance system, since they were designed for specific health care purposes<sup>8</sup>, the legal bases that delimit the feeding of these systems can also isolate the collection of some diversity information, not guaranteeing its presence in all systems. There is no legal framework that standardizes the collection of this information; most of the formulations are decrees and ordinances.

The recording of information on race/color became mandatory in all health information systems in Brazil due to Ordinance No. 344/MS, of February 1, 2017, although it had been in force as an individual recognition attribute since Ordinance GM/MS No. 3,947, of November 25, 1998, which placed it among the attributes to be adopted by health systems.

4. COELHO NETO, GC ; CHIORO, A. After all, how many national Health Information Systems are there in Brazil? *Public Health Notebooks*, v. 37, n. 7, p. e00182119, 2021. Available at: <https://www.scielo.br/j/csp/a/RzNmviHqmLhPHZp-6gfcdC6H/?format=pdf&lang=pt>. Accessed on: April 29, 2024.

5. BRAZIL. Ministry of Health. *The Brazilian experience in health information systems*. Brasília: Ministry of Health Publishing House, 2009. (Series B. Basic Health Texts, v. 1 - Production and dissemination of health information in Brazil).

6. BRAZIL. Ministry of Health. Secretariat of Health Surveillance. Department of Strategic Coordination of Health Surveillance. *Health Surveillance Guide* [electronic resource] / Ministry of Health, Health Surveillance Secretariat. Department of Strategic Coordination of Health Surveillance. -5th ed. rev. and update. Brasília: Ministry of Health, 2022. 1,126 p.

7. BRAZIL. Ministry of Health. *Health care information systems: historical contexts, advances and perspectives in the SUS*. Brasília, DF: Graphic City and Publishing LTDA, Oct. 2015.

8. BRAZIL. Ministry of Health. *Health care information systems: historical contexts, advances and perspectives in the SUS*. Brasília, DF: Graphic City and Publishing LTDA, Oct. 2015.

existing at the time<sup>9</sup>. It is important to note that, as an indirect participant in the mandatory collection defined by Ordinance 344/MS, ethnicity is mixed with the collection of race/color because it is among the categories defined by the Brazilian Institute of Geography and Statistics (IBGE), the classification standard adopted. In this sense, the marking of ethnicity can also be linked to the classification of quilombola populations, treated as ethno-racial groups.

Information on sexual orientation and gender identity has been found in the Notifiable Injury Information System (SINAN) since 2014, specifically and only when there is a report of violence, whether interpersonal or self-inflicted.<sup>10</sup> It is noted that this information is related to the legislation on recording violence in Brazil, aiming to defend and guarantee rights.<sup>11</sup>.

Although there are national health policies for the Black, Lesbian, Gay, Bisexual, Transvestite and Transgender (LGBT) population and for Indigenous Peoples, in addition to legislation that favors migrants' access to health and the Federal Constitution of 1988 itself, which guarantees the right to health for everyone in Brazilian territory, health systems face limitations in capturing information about diversity.

The hypothesis is that the legal bases governing the collection of information on diversity come from the field that marks the social trajectory of a given category and that this legal framework, at some point, connects with health. With the main objective of gathering national legal standards that directly and indirectly influence the collection of information on diversity in health, the article is based on a documentary research carried out in technical publications made available by national official agencies. The selected material sought to answer the following question: what are the national standards that impact or have impacted the collection of information on diversity in health information systems?

The paper begins by presenting a brief overview of Health Information Systems and Digital Health. It then addresses information on

9. BRAZIL. Ministry of Health. Health Surveillance Secretariat. Department of Health Situation Analysis. *Legislation Relating to Mortality Information Systems (SIM) and Live Births Information Systems (SINASC)*. Brasília: Ministry of Health, 2004.

10. OLIVEIRA, DC Representation of the LGBTQIA+ population in epidemiological research, in the context of the National Policy for Comprehensive Health of Lesbians, Gays, Bisexuals, Transvestites and Transsexuals: expanding the production of knowledge in the SUS for social justice. *Epidemiology and Health Services*, v. 31, n. 1, e2022020, 2022.

11. LEAL, CHS ; SCALCO, MLA ; NUNES, RPD ; CONSORTII, ER ; KITAGAWA, BY Violence surveillance: considerations on information related to violence perpetrated against the LGBT population in the city of São Paulo. *Bis*, São Paulo, v. 2, n. 19, p. 55-61, Dec. 2018. Available at: <https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n2-diversidade-55-61.pdf> . Accessed on: April 19, 2024.

diversity and its trajectory in the field of social information. Finally, it presents an overview of the legal bases that regulate the use of this information in health and how they are incorporated into health systems. The article addresses the trajectory of the collection of information on race/color/ethnicity and the Lesbian, Gay, Bisexual and Transgender (LGBT) population.

## 1. Health Information Systems and Digital Health

Electronic health records are generated as part of the normal transactions of the government business and contain information on individuals who access public services, characterizing both individual and collective facts. Used as instruments of public administration and created for operational purposes, these data, which are of national scope, have come to be used to generate public information and statistics.

These records, as we know them today, come from the evolution of the process of systematizing government public services and their information, marked by the development of tools and methods. Highlights in this process include the incorporation of statistics as an element of scientific government and digitalization.<sup>12</sup> The first reinforced the call for the organization and systematization of information, a necessary condition for providing national statistics. The second, inserted in the scope of the administrative rationalization actions that occurred in the 1990s, emphasized a managerial public administration and made use of Information and Communication Technology (ICT) as an instrument for electronic government. This initiative was strengthened by the discursive association that brings information (and, consequently, ICTs) closer to governance and development.<sup>13-14</sup> At the time, with neoliberalism as a backdrop, it was important for developing countries to have “good public management governance” in order to secure international financial benefits.<sup>15</sup>

The potential to generate statistics and complement the knowledge produced about the population to which these records refer has expanded

12. BRAZIL. Ministry of Health. *The Brazilian experience in health information systems*. Brasília: Ministry of Health Publishing House, 2009. (Series B. Basic Health Texts, v. 1 - Production and dissemination of health information in Brazil).

13. WORLD BANK. *Managing development: the governance dimension*. Washington, DC: World Bank Group, 1991. Available at: <http://documents.worldbank.org/curated/en/884111468134710535/Managing-development-the-governance-dimension> . Accessed on: February 14, 2024.

14. PANZARDI, R.; CALCOPIETRO, C.; IVANOVIC, EF *New-economy sector study: electronic government and governance -lessons from Argentina*. Working paper. Washington, DC: World Bank, Jul. 2002. Available at: <https://documentos.bancomundial.org/es/publication/documents-reports/documentdetail/527061468769894044/new-economy-sector-study-electronic-government-and-governance-lessons-from-argentina> . Accessed on: February 14, 2024.

15. WORLD BANK. *Managing development: the governance dimension*. Washington, DC: World Bank Group, 1991. Available at: <http://documents.worldbank.org/curated/en/884111468134710535/Managing-development-the-governance-dimension> . Accessed on: February 14, 2024.

its adherence among researchers, governments and statistical agencies<sup>16,17,18</sup>. This is because the continuous collection of this information over time favors longitudinal analyses, enabling population approaches.

With regard to administrative health records, Brazil has invested in active transparency actions in recent years with the aim of expanding its position in data openness, encouraging the use and reuse of these (de-identified) records as secondary data for research and policy purposes.<sup>19</sup> In the national environment, there is a perception, brought from the United Kingdom, that these records are an invaluable resource for the common public good.<sup>20</sup> This value is increased by the possibility of interconnection between these records.

The scope of monitoring with a view to producing knowledge relevant to society can be expanded by actions such as:

- a) Linkage between databases (*Data Linkage*). The application of this statistical technique, which can be performed by probabilistic and deterministic methods<sup>21</sup>, enables the linking of data from different sources from common records and is disseminated as a surveillance strategy<sup>22-23</sup>.
- b) Interoperability. The ability to interconnect and communicate between information systems of different technologies. This strategy is incorporated into the National Policy on Health Information and Informatics (PNIIS)<sup>24</sup>, 2003, which advocates for the organization of the National Information System

16. SENRA, N. de C. The issue of administrative records vis-à-vis the generation of statistics. *Brazilian Journal of Population Studies*, [S. l.], v. 13, n. 2, p. 199-205, 1996. Available at: <https://rebeb.org.br/revista/article/view/437>. Accessed on: July 23, 2024.

17. FERREIRA, FPM Administrative records as a source of statistical data. *Public Informatics*, year 10, n. 1, p. 81-93, 2008.

18. MELLO, Janine. State production of evidence and use of administrative records in public policies. In: KOGA, Natália Massaco (Org.) et al. *Public policies and the use of evidence in Brazil: concepts, methods, contexts and practices*. Brasília: IPEA, 2022. p. 897-914.

19. BRAZIL. Ministry of Health. Secretariat of Health and Environmental Surveillance. Department of Epidemiological Analysis and Surveillance of Noncommunicable Diseases. *Surveillance Data: profiles of databases produced by Health Surveillance in Brazil*. Brasília: Ministry of Health, 2023. 127 p.: ill.

20. ADMINISTRATIVE DATA RESEARCH UK. *Administrative data is an invaluable resource for public good*. Let's use it. Annual Report 2018-19. 2019.

21. COELI, Cláudia Medina. Population data science. *Epidemiology and health services*; journal of the Brazilian Unified Health System, v. 31, n. 3, e2022119, 19 Dec. 2022. doi:10.1590/S2237-96222022000300001.

22. BRAZIL. Ministry of Health. Secretariat of Health Surveillance. Department of Strategic Coordination of Health Surveillance. *Health Surveillance Guide* [electronic resource] / Ministry of Health, Health Surveillance Secretariat. Department of Strategic Coordination of Health Surveillance. – 5th ed. rev. and update. Brasília: Ministry of Health, 2022. 1,126 p.

23. BRAZIL. Ministry of Health. Health Surveillance Secretariat. *Technical Note No. 34/2023: updates and recommendations for the surveillance of congenital anomalies in Brazil*. Brasília, DF, 2023. Available at: <http://plataforma.saude.gov.br/anomalies-congenitas/nota-tecnica-34-2023.pdf>. Accessed on: March 8, 2024.

24. BRAZIL. Ministry of Health. Executive Secretariat. SUS Information Technology Department. *National Policy on Health Information and Informatics: Proposal Version 2.0* (Includes deliberations of the 12th National Health Conference). 2004. Available at: [http://bvsmms.saude.gov.br/bvs/publicacoes/PoliticaInformacaoSaude29\\_03\\_2004.pdf](http://bvsmms.saude.gov.br/bvs/publicacoes/PoliticaInformacaoSaude29_03_2004.pdf). Accessed on: August 1, 2024.

Health System (SNIS) and its adaptation to the guidelines of the Brazilian Electronic Government Program (e-Gov) and the e-Health strategy<sup>25-26</sup>.

Both integration strategies involve actions to standardize information, with the creation of data models, and technology, with the definition of infrastructure and connection standards.

A survey found that between 2010 and 2018, there were 54 nationwide health information systems. Depending on their operating purpose, these systems are organized for the purposes of monitoring events relevant to public health, controlling and monitoring health programs of the Ministry of Health, registering users of care (population, professionals and health services) and supporting the electronic management of policies, processes and services. The systems classified in this category have horizontal characteristics and aim at the administrative rationalization of the SUS<sup>27</sup>.

The main problems identified in these systems are mainly linked to their fragmentation, a reflection of the tripartite structure of health administration, which involves states and municipalities in the management of the systems, and of technical specialization, which creates a system for each new need. As a result, the systems produce the same information, but are guided by different collection methods and rules.<sup>28</sup> In addition, changes in system versions for modernization and improvement purposes may lead to inconsistency in information, due to loss or discontinuity of data.<sup>29</sup> Information collection is also an issue, as few systems have incorporated electronic registration.

## 2. Diversity information

Diversity refers to social categories used to describe the differences between people who make up a given population. These data focus on characteristics such as race/ethnicity, citizenship, immigration status,

25. BRAZIL. Ministry of Health. *Ordinance No. 589 of May 20, 2015*. Institutes the National Policy on Health Information and Informatics (PNIIS). Official Gazette of the Union: issue 96, section 1, Brasília, DF, p. 72, May 22, 2015.

26. BRAZIL. Ministry of Health. *Ordinance No. 2,073 of August 31, 2011*. Regulates the use of interoperability and health information standards for health information systems within the Unified Health System, at the Municipal, District, State and Federal levels, and for private systems and the supplementary health sector. Official Gazette of the Union: section 1, Brasília, DF, p.63, September 1, 2011.

27. COELHO NETO, GC ; CHIORO, A. After all, how many national Health Information Systems are there in Brazil? *Public Health Notebooks*, v. 37, n. 7, p. e00182119, 2021. Available at: <https://www.scielo.br/j/csp/a/RzNmviHqm-LhPHZp6gfcD6H/?format=pdf&lang=pt>. Accessed on: April 29, 2024. P.9.

28. BRAZIL. Ministry of Health. *Health care information systems: historical contexts, advances and perspectives in the SUS*. Brasilia, DF: Graphic City and Publishing LTDA, Oct. 2015.

29. BRAZIL. Ministry of Health. *Consolidation of the Live Birth Information System*. General Coordination of Epidemiological Information and Analysis. 2011.

religion, gender (including gender identity), age, social class, disability, sexual orientation, marital status, among others. The relevance and impact of each category varies according to society, time and context<sup>30</sup>. This type of information has the role of highlighting diversity as a positive aspect of society, going beyond the mere description of the existence of differences.<sup>31</sup>

Information on diversity is part of a broader debate on: 1) minority rights and monitoring compliance with human rights obligations; 2) the application of anti-discrimination legislation; and 3) monitoring progress towards achieving the goals of sustainable development and social equality, among others.<sup>32</sup> However, more forcefully, it is a debate about citizenship, centered on reflections on the multi-ethnic composition of a nation.<sup>33 34 35</sup>.

In Brazil, social considerations about diversity are based on categories such as race/color; ethnic-racial groups; traditional peoples and communities, such as quilombolas, indigenous peoples, gypsies, terreiro communities, rubber tappers, artisanal fishermen, among others; Lesbians, Gays, Bisexuals, Transvestites and Transsexuals (LGBT); and the migrant, refugee and stateless population.<sup>36 37</sup>

In the health field, these groups participate directly or transversally in national policies, such as the National Food and Nutrition Policy (1999), the National Policy for Reducing Morbidity and Mortality due to Accidents and Violence (2001), the National Policy for Emergency Care, the National Policy for Health Care for Indigenous Peoples (2002) and the National Policies for Comprehensive Health of Specific Populations, such as those for the black population (2009) and the LGBT population (2011).<sup>38</sup>

30. ROSENSTREICH, G. et al. *Diversity Data Collection: Exploratory Mapping & Reflection*. Una Europa, 2022. Available at: <https://una-europa.imgix.net/resources/Diversity-Data-Collection-Exploratory-Mapping-Reflection.pdf>. Accessed on: February 14, 2024.

31. BOTOKO CLAEYSEN, Catherine et al. *Diversity Data Collection: Exploratory Mapping & Reflection: Una Europa Diversity Council Action Group Data Collection Final Report 2022*. Una Europa, 2022. Available at: <https://paris1.hal.science/hal-03930967/>. Accessed on: March 8, 2024.

32. EC-EUROPEAN COMMISSION, Directorate-General for Justice and Consumers, FARKAS, L. *Analysis and comparative review of equality data collection practices in the European Union*. EC: Data collection in the field of ethnicity, Publications Office, 2017.

33. DE OLIVEIRA, Jane Souto. *Brazil shows its face: images of the Brazilian population in the demographic censuses from 1872 to 2000*. Rio de Janeiro: National School of Statistical Sciences, 2003. 75 p. ISSN 1677-7093; n. 6.

34. COSTA, Fabiana Claudia Viana. *Designation and enunciative reference of the 2000 Demographic Census. 2004*. Dissertation (Master's in Linguistics)–UNICAMP, Institute of Language Studies, State University of Campinas, Campinas, São Paulo, 2004.

35. LOVEMAN, M. The politics of a transformed data landscape: ethnoracial statistics in Brazil in a regional comparative perspective. *Sociologies*, v. 23, no. 56, p. 110–153, Jan. 2021.

36 ARRUTI, José Maurício. Ethnicity. In: SANSONE, L.; ALVES FURTADO, C. (org.). *Critical dictionary of the social sciences of Portuguese-speaking countries*. Salvador: EDUFBA, 2014. p. 199-2013.

37. MIGUEL, Nadya Maria Deps. *The Brazilian Profile constructed by IBGE: a discursive memory of the Demographic Censuses from 1940 to 2010*. Thesis (Postgraduate Program in Social Memory) – Federal University of the State of Rio de Janeiro, Rio de Janeiro, 2012.

38. BRAZIL. Ministry of Health. Secretariat of Health Care. *Technical Note No. 18/2014*. Review of the National Health Promotion Policy. Brasília, 2014. Available at: <https://www.conass.org.br/biblioteca/wp-content/uploads/2014/01/NT-18-2014-Politica-de-Promo%CC%A7a%CC%83o-da-Sau%CC%81de.pdf>. Accessed on: April 29, 2024.

## 2.1 The trajectory of diversity as social information

The production of information on diversity within official systems began in the late 1990s with the inclusion of the category “color or race”. In 2002, it acquired a new perspective with the support of the United Nations Population Fund (UNFPA), which promoted the strengthening of national capacity to ensure social rights with a focus on gender, race and generation, in areas such as reproductive health, HIV/AIDS, violence prevention and gender equality.<sup>39</sup> To this end, it was planned to “train in the use of administrative records and improve existing systems. Improvement is understood as the inclusion of sex, age and race in all records aimed at people”<sup>40</sup>.

At the heart of these initiatives was the creation of indicators. Diversity data collection typically uses indicators, which are measurable parameters that represent specific aspects of a diversity category. When given meaning, these statistics are treated as indicators of a situation that will be the target of policy intervention. The goal is for the effectiveness of the policy to positively affect the reality of these indicators.<sup>41</sup>

Thus, as the debate on the rule of law advances and national (state or municipal) policies are structured, administrative records need to incorporate these fields within the scope of Information Systems (SIS), to provide support for official surveys that use the individual as the unit of analysis.<sup>42</sup> However, it is important to note that the information needed to monitor and evaluate the characteristics of the Brazilian population is mediated by the specificities of the Information System.

## 3. Methodology

The qualitative documentary analysis was carried out based on searches on the official websites of the Brazilian government. Priority was given to technical documents, regulations and manuals. The search gathered information on public policies and rights related to race, ethnicity and

39. UNITED NATIONS POPULATION FUND. *Proposed Projects and Programs: Assistance to the Government of Brazil (DP/ FPA/ BRA/3)*. United Nations Population Fund, 2001. Available at: [https://brazil.unfpa.org/sites/default/files/pub-pdf/country\\_programme20022006\\_0.pdf](https://brazil.unfpa.org/sites/default/files/pub-pdf/country_programme20022006_0.pdf) . Accessed on: April 29, 2024.

40. OSORIO, Rafael Guerreiro. *The IBGE Color and Race Classification System*. Brasília: Ipea, Ministry of Planning, Budget and Management, 2003. (Discussion paper, 996). P. 37.

41. OSÓRIO, Rafael Guerreiro. *The IBGE Color and Race Classification System*. Brasília: Ipea, Ministry of Planning, Budget and Management, 2003. (Text for discussion, 996).

42. OSORIO, Rafael Guerreiro. *The IBGE Color and Race Classification System*. Brasília: Ipea, Ministry of Planning, Budget and Management, 2003. (Text for discussion, 996).

population of Lesbians, Gays, Bisexuals, Transvestites and Transgenders (LGBT). The survey of decrees was conducted based on citations contained in these documents. The assessment of the conditions of social information in Health Information Systems, for the purposes of this article, prioritized only those linked to Primary Care: Mortality Information System (SIM), Live Birth Information System (SINASC), Food and Nutrition Surveillance System (SISVAN), Information System on Notifiable Diseases (SINAN) and the Outpatient Information System (SIA/SUS). The cases were assessed according to the objective of the system and its adequacy to the legal basis of the diversity categories analyzed.

## 4. Legal bases and the incorporation of diversity in Health Systems

The constitutional norms that establish the basis of legitimacy for the development of health policies have as their starting point article 196 of the Federal Constitution (1988), which ensures health as a right to be guaranteed by the State<sup>43</sup>. It should be noted that the Constitution ensures other rights and guarantees to diversity, which, in general terms, can be grouped into the axes linked to equality and non-discrimination (articles 3, 5, 14, 19, 215 and 242), territorial and cultural rights (articles 216, 231 and 232) and social rights (article 6). In the legislative field, most of the regulations are within the scope of Human Rights and Citizenship, in addition to being included in the legislation that deals with crimes related to prejudice.

### 4.1 Race/color

The mapping carried out on the legal bases identified a normative scenario composed of two laws, one decree and three ordinances. Ordinances No. 3,947/GM/MS and No. 344/MS have a direct impact on the inclusion of the variable in the SUS collection forms. Law No. 12,288, considered a fundamental legal framework in Ordinance No. 344/MS, although it addresses, among other issues, the right to health, also dialogues with legislation that deals with crimes related to prejudice, violence and intolerance. This law and Ordinance No. 992/GM/MS emerge as milestones to minimize the discriminatory framework both in the social sphere and within the scope of the Unified Health System (SUS). Below is the list of the milestones raised:

43. BRAZIL. [Constitution (1988)]. *Constitution of the Federative Republic of Brazil of 1988*. Brasília, DF: President of the Republic. Available at: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompilado.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm) . Accessed on: April 29, 2024.

- Decree No. 65,810, of December 8, 1969: International Convention on the Elimination of all Forms of Racial Discrimination.
- Ordinance No. 3,947/GM/MS, of November 25, 1998: Approves the common attributes to be adopted, mandatorily, by all systems and databases of the Ministry of Health, starting January 1, 1999.
- Ordinance No. 992/GM/MS, of May 13, 2009: National Policy for Comprehensive Health of the Black Population (PNSIPN).
- Law No. 12,288, of July 20, 2010: Statute of Racial Equality.
- Resolution No. 2/CIT, of September 2, 2014: II Operational Plan (2013-2015) of the PNSIPN within the scope of the Unified Health System (SUS).
- Ordinance No. 344/MS, of February 1, 2017: mandatory completion of the race/color question in health information system forms.
- Law No. 14,553 of 2023, which amends Law No. 12,288/2010: mandatory inclusion of fields for ethnic-racial identification in various documents. The legislation covers employment admission and dismissal forms, work accident forms, National Employment System (SINE) registration instruments, and documents for registration in the General Social Security Regime. The inclusion also applies to the Annual Social Information Report (RAIS) and IBGE survey questionnaires.

Since 1995, SINASC has used the “RACACOR” field for registration. However, reflecting the impact of Ordinance No. 992/GM/MS/2009 and Law No. 12,288/2010, there was a change in the notification method. As of 2011, in addition to collecting information on the newborn’s race/color, information on the mother was also collected.<sup>44</sup> This change allowed the mapping of access to maternal and child health policies and was a strategy to identify racial discrimination. Until then, SINASC's emphasis was on the preparation of vital statistics<sup>45 46</sup>.

44. BRAZIL. Ministry of Health. *Consolidation of the Live Birth Information System*. General Coordination of Epidemiological Information and Analysis. 2011.

45. BRAZIL. Ministry of Health. National Health Foundation. *Procedures manual for the live birth information system*. Brasilia: Ministry of Health, 2001. 32 p.

46. BRAZIL. Ministry of Health. *Consolidation of the Live Birth Information System*. General Coordination of Epidemiological Information and Analysis. 2011.

In SIM and SINASC, where the introduction of filling in the race/color question is older, the completeness of the information is greater<sup>47</sup>. Part of this characteristic comes from the legal matrix that supported the creation of the systems. Both began collecting data in the same year and are derived from the rules that regulate public records (Law 6,015, of December 31, 1973) and civil records, specifically the notary rules, respectively.<sup>48</sup>.

## 4.2 Ethnicity

Since the 2000 census, the IBGE has been surveying the race, color and ethnicity of the Brazilian population<sup>49</sup>. According to the criteria defined by the institute, the population can be classified as white, black, yellow, brown or indigenous. Those who identify as such are considered indigenous, whether through connection to indigenous lands or through ties to traditions.<sup>50</sup>(Brazil, 2017). Thus, the concept of “indigenous” developed by the IBGE is linked to indigenous groups. Since then, this classification criterion has been used, especially since ordinances n° 3.947/GM/MS/1998 and n° 344/MS/2017.

It was through Decree No. 6,040, of February 7, 2007, that the National Policy for the Sustainable Development of Traditional Peoples and Communities was established, expanding the notion of ethnicity. The category of traditional peoples and communities (PCTs) includes quilombola communities, indigenous peoples, gypsies, terreiro communities, rubber tappers, artisanal fishermen, among others. This is a formal legal recognition that is part of the land regulation framework.<sup>51</sup>.

Traditional peoples and communities have their legal recognition marked by their relations with the territory. Since the Federal Constitution of 1988 (CF/88), the Brazilian State has treated PCTs as social organizations that occupy and use territories<sup>52</sup>.

47. COELHO, R. ; REMÉDIOS, J. ; NOBRE, V. ; MREJEN, M. The race/color question in DataSUS: evolution and determinants of completeness. *Technical Note No. 30*.IEPS: Sao Paulo, 2023.

48. BRAZIL. Ministry of Health. Health Surveillance Secretariat. Department of Health Situation Analysis. *Legislation Relating to Mortality Information Systems (SIM) and Live Births Information Systems (SINASC)*.Brasilia: Ministry of Health, 2004.

49. BRAZIL. Ministry of Health.*Implementation guide for the Race/Color/Ethnicity issue*.Ministry of Health, University of Brasilia. Brasilia: Ministry of Health, 2018. 38 p.: ill.

50. BRAZIL. Ministry of Social Development.*Social work with indigenous families in basic social protection*.Brasília, DF: MDS, National Secretariat of Social Assistance, 2017.

51. BRAZIL. Ministry of Citizenship.*PCT Newsletter*. [Informative]. National Secretariat of Social Assistance, 2017. Available at: [https://www.mds.gov.br/webarquivos/arquivo/assistencia\\_social/consulta\\_publica/Informativo%20PCT.pdf](https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf) . Accessed on: February 14, 2024.

52. BRAZIL. Ministry of Social Development.*Social work with indigenous families in basic social protection*.Brasília, DF: MDS, National Secretariat of Social Assistance, 2017.

In this sense, care for PCTs is characterized by the notion of collective, which goes beyond the notion of family or individual, and is governed by Primary Health Care services oriented by territory, whether by Special Indigenous Health Districts (DSEI) or by Remaining Quilombola Communities (CRQ)<sup>53</sup>. Health care includes specialized care, health care for women and children, and food and nutritional monitoring, among others. Thus, there is “socio-assistance surveillance with socio-territorial diagnosis”<sup>54</sup>.

The legal parameters that guide the collection of data from the PCTs, initiated by the census, are incorporated into the framework of actions of the Ministry of Social Development and Fight against Hunger (MDS), according to Decree No. 6,040/2007<sup>55</sup> <sup>56</sup>. Thus, within the scope of social protection, duly registered indigenous and quilombola families were included in the records of the Single Registry for Social Programs<sup>57</sup>. Based on these considerations, the regulatory bases for collecting data on ethnicity are related to:

- Article 194 of the 1988 Federal Constitution, social security.
- Law No. 8,742, of December 7, 1993, Organic Law of Social Assistance (LOAS)
- Law No. 9,459, of May 13, 1997, which adds the clause on Racial Injury to article 140 of the Penal Code.
- Law No. 9,836, of September 23, 1999, on the Indigenous Health Care Subsystem.
- Decree No. 4887, of November 20, 2003, which treats quilombola communities as “ethnic-racial groups.
- Legislative Decree No. 143, of June 20, 2002, which approves Convention 169 of the International Labor Organization, which deals with Indigenous and Tribal Peoples.

53. BRAZIL. Ministry of Social Development. *Social work with indigenous families in basic social protection*. Brasília, DF: MDS, National Secretariat of Social Assistance, 2017.

54. BRAZIL. Ministry of Citizenship. *PCT Newsletter*. [Informative]. National Secretariat of Social Assistance, 2017. Available at: [https://www.mds.gov.br/webarquivos/arquivo/assistencia\\_social/consulta\\_publica/Informativo%20PCT.pdf](https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf) . Accessed on: February 14, 2024. P.15.

55. BRAZIL. Ministry of Social Development. *Social work with indigenous families in basic social protection*. Brasília, DF: MDS, National Secretariat of Social Assistance, 2017.

56. BRAZIL. Ministry of Health. Secretariat of Health Care. Department of Primary Care. General Coordination of Food and Nutrition Policy. *Operational manual for use of the Food and Nutrition Surveillance System. SISVAN Version 3.0. Standards and Technical Manuals*. Brasília: Ministry of Health, 2017.

57. BRAZIL. Ministry of Citizenship. *PCT Newsletter*. [Informative]. National Secretariat of Social Assistance, 2017. Available at: [https://www.mds.gov.br/webarquivos/arquivo/assistencia\\_social/consulta\\_publica/Informativo%20PCT.pdf](https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf) . Accessed on: February 14, 2024. P.15.

- Ordinance No. 254/GM/MS, of January 31, 2002, on the National Policy for Healthcare for Indigenous Peoples.
- Ordinance No. 98, of November 26, 2007, which deals with the General Registry of Remnant Quilombo Communities
- Decree No. 6,040, of February 7, 2007, which established the National Policy for Sustainable Development of Traditional Peoples and Communities.
- Decree No. 6,261/2007 (revoked by Decree No. 11,447, of March 21, 2023). Aquilomba Brasil Program and its Management Committee.
- Ordinance No. 992/GM/MS, of May 13, 2009: National Policy for Comprehensive Health of the Black Population (PNSIPN).
- Decree No. 6,872, of June 4, 2009, on the National Plan for the Promotion of Racial Equality (PLANAPIR), which in axis 3, on Health, deals with expanding access to black, indigenous and gypsy populations, and within the scope of family health, to quilombola communities.
- Decree No. 10,088 of November 5, 2009 (and Decree 5,051/2004), which complies with the legislative decree of ILO Convention 169 and the legal principle of ethnic self-determination.
- Ordinance No. 177, of June 16, 2011, which defines differentiated care for some population groups for inclusion in the Single Registry.
- Ordinance No. 2,866, of December 2, 2011, on the National Policy for Comprehensive Health of Rural and Forest Populations (PNSIP-CF)
- Ordinance GM/MS No. 3,396, of December 11, 2020
- Decree No. 12,128, of August 1, 2024, officially institutes the National Policy Plan for Gypsy Peoples.

The mapping carried out on the legal bases identified a normative scenario oriented towards the recognition of rights, demarcation of territories and administrative management of these territories. Health actions are referenced by the National Policy for Comprehensive Health of Rural and Forest Populations (PNSIPCF) and the National Policy for Comprehensive Health of the Black Population (PNSIPN). These policies highlight the health specificities of these populations, including vulnerabilities of access, violence and territorial disputes, mental health issues and use of psychotropic drugs, access to food and

sexually transmitted diseases, among others. The PNSIPCF, in particular, emphasizes aspects of citizenship, food and nutritional security, and sustainable development<sup>58</sup>.

The health assessment of these groups tends to be characterized by geographic space, by categories of gender, age, race/ethnicity and other markers of specific populations. In the health systems (SIS), ethnicity can be collected from two fields: race/color and people and traditional community. Among the systems linked to Primary Care, the Mortality Information System (SIM), the Live Birth Information System (SINASC) and the Information System on Notifiable Diseases (SINAN) use the race/color field to collect information on ethnicity. In some cases, the street field, associated with the address (street, avenue, etc.), can be used to record the name of the traditional community.<sup>59</sup> Due to its connection with the nutritional surveillance program and the actions of the Bolsa Família Program, the Food and Nutrition Surveillance System (SISVAN) has the field of traditional people and communities<sup>60</sup>.

## Lesbian, Gay, Bisexual, Transvestite and Transgender (LGBT)

The health issues of lesbians, gays, bisexuals, transvestites and transsexuals (LGBT) are strongly related to issues of violence, the process of transsexualization and the fight against HIV/AIDS and sexually transmitted diseases (STDs). In fact, it was through the fight against the HIV/AIDS epidemic that the health issues of this population gained prominence in the Brazilian scenario.<sup>61</sup> The regulatory framework governing the collection of information on this group is relatively recent, although it was preceded by debates in the field of Human Rights since the 1980s.<sup>62</sup>, as seen below:

58. IEPS; UMANE; VEREDAS INSTITUTE. *Technical Report No. 1/2023. Health of Indigenous and Quilombola Peoples*. London: Oxford University Press, 2019.

59. BRAZIL. Ministry of Health. Health Surveillance Secretariat. *Notifiable Diseases Information System. Notification Form*. Brasília: Ministry of Health, 2006.

60. BRAZIL. Ministry of Health. Secretariat of Health Care. Department of Primary Care. General Coordination of Food and Nutrition Policy. *Operational manual for use of the Food and Nutrition Surveillance System. SISVAN Version 3.0. Standards and Technical Manuals*. Brasília: Ministry of Health, 2017.

61. BRAZIL. Ministry of Health. Secretariat of Strategic and Participatory Management. Department of Support for Participatory Management. *National Comprehensive Health Policy for Lesbians, Gays, Bisexuals, Transvestites and Transsexuals*. Ministry of Health, Secretariat of Strategic and Participatory Management, Department of Support for Participatory Management. Brasília, DF: Ministry of Health, 1st ed., 2013.

62. BRAZIL. Ministry of Health. Secretariat of Strategic and Participatory Management. Department of Support for Participatory Management. *National Comprehensive Health Policy for Lesbians, Gays, Bisexuals, Transvestites and Transsexuals*. Ministry of Health, Secretariat of Strategic and Participatory Management, Department of Support for Participatory Management. Brasília, DF: Ministry of Health, 1st ed., 2013.

- Law No. 7,716, of January 5, 1989, crimes resulting from prejudice.
- Ordinance No. 2,227, of October 14, 2004, provides for the creation of the Technical Committee for the formulation of a proposal for the national health policy for the gay, lesbian, transgender and bisexual population – GLTB.
- MS/GM Ordinance No. 104, of January 25, 2011, universalizes the reporting of domestic, sexual and other violence.
- Ordinance No. 2,836, of December 1, 2011, National Policy for Comprehensive Health for Lesbians, Gays, Bisexuals, Transvestites and Transsexuals (National LGBT Comprehensive Health Policy).
- MS/GM Ordinance No. 1,271, of June 6, 2014, includes cases of sexual violence and attempted suicide in the list of diseases and conditions subject to compulsory notification.
- GM/MS Consolidation Ordinance No. 02, of September 28, 2017, which consolidates the National LGBT Comprehensive Health Policy among the national health policies of the Unified Health System.
- CIT Resolution No. 26, of September 28, 2017, II operational plan (2017-2019) of the National LGBT Comprehensive Health Policy within the scope of the Unified Health System.
- Bill No. 1082 of 2023 (in progress), which proposes to amend Law No. 8,184 of May 10, 1991, and to collect mandatory data on the LGBTQIA+ population (lesbians, gays, bisexuals, transsexuals, queer, intersex, asexuals and others) through censuses and other periodic surveys by the Brazilian Institute of Geography and Statistics (IBGE).
- Ordinance No. 762, of December 7, 2023, establishes the National Network of Evidence in Human Rights, within the scope of the Ministry of Human Rights and Citizenship.

The process of collecting and incorporating information about the LGBT population into Health Information Systems (SIS) begins with the Notifiable Diseases Information System (SINAN), through the violence surveillance module, starting in 2015.<sup>63</sup> The structure of the form of this module is capable of recording sexual orientation (heterosexual, homosexual (gay/lesbian), bisexual), gender identity (transvestite, transsexual woman, man-

63. LEAL, CHS ; SCALCO, MLA ; NUNES, RPD ; CONSORTII, ER ; KITAGAWA, BY Violence surveillance: considerations on information related to violence perpetrated against the LGBT population in the city of São Paulo. *Bis*, São Paulo, v. 2, n. 19, p. 55-61, Dec. 2018. Available at: <https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n2-diversidade-55-61.pdf> . Accessed on: April 19, 2024.

transgender person), as well as the motivation for the violence (sexism, homophobia/lesbophobia/biphobia/transphobia, racism, religious intolerance, xenophobia, generational conflict, homelessness, disability)<sup>64</sup>.

The other SINAN modules, including the one that monitors HIV/AIDS cases, do not have specific fields for gender identity and sexual orientation. For these cases, other variables are used: in HIV/AIDS monitoring, for example, data analysis is based on the field that captures the probable mode of sexual transmission (men who have sex with men (MSM) and women who have sex with women (WSW)).<sup>65</sup> For systems that do not capture this information, the gender variable remains (male, female, ignored).

## Final considerations

This brief analysis of national standards governing the inclusion of social categories that represent diversity in health information systems reveals that the relevant legislation was constructed and drafted as these categories gained social recognition. However, despite being ensured by public policy programs, statistical invisibility still persists for some of these categories.

The lack of infrastructure and information management, in terms of creating a standard, has proven to be a limiting factor in expanding the inclusion of information fields capable of representing these categories. It is observed that administrative records constitute a relevant source of data on the country's diversity, in addition to the census.

Furthermore, the recognition of these categories, whether in the context of stigmatizing diseases or violence, as in the case of the LGBTQIA+ population, or in the territorial context, as for traditional peoples and communities (PCTs), influences the way in which they are included in information systems and which systems will be considered.

The strategic path for Digital Health, as for all government digital businesses, is being outlined by a framework that assesses institutional maturity in the use of data. Considerations on how

64. LEAL, CHS ; SCALCO, MLA ; NUNES, RPD ; CONSORTII, ER ; KITAGAWA, BY Violence surveillance: considerations on information related to violence perpetrated against the LGBT population in the city of São Paulo. *Bis*, São Paulo, v. 2, n. 19, p. 55-61, Dec. 2018. Available at: <https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n2-diversidade-55-61.pdf> . Accessed on: April 19, 2024. P.57.

65. CANAVESE, D. et al. For the urgent and definitive inclusion of gender identity and sexual orientation fields in the SUS health information systems: what can we learn from the monkeypox outbreak?. *Science & Public Health*, v. 27, no. 11, p. 4191-4194, nov. 2022.

population is incorporated into official surveys, although they are old, they have always been on the agenda of the national data policy adopted by the government. This is because the aspects of the population included in a survey reflect a time, its context and the ideals of the constituents of society.

What needs to be addressed is the impact of the quality of the information that represents these categories on the future uses of these data. This perspective emphasizes both the data life cycle and the notion of the long tail of data. The data life cycle considers the evolution of access and sharing, while the long tail emphasizes the frequency of use and consumption of these data.

If, in a way, social policies become data and information policies, determining how, when and why collection should occur, the challenge lies in creating a moderating strategy that is incorporated into data processing, especially between the collection and use of this information. The mismatch between the suitability of the public entity for the capture, collection and, consequently, the adequate treatment of this information and the advancement of rights legislation can be compensated for by data governance strategies.

While information is collected at the individual level, diversity data analysis aims to understand a collective context. Furthermore, the collection and use of data has a direct and long-term impact on the legal and social rights of this population. There is a need to reconsider and reimagine the structure of this collection to meaningfully address concerns related to the use (and enjoyment) of this data and other technologies.

In this sense, international organizations advocate that public authorities adopt data governance models that are differentiated by social group and their specificities. Such models can be improved to meet the rights of these communities, using normative strategies and data principles focused on social justice. This is an area that has received little discussion in Brazil, given the country's limited experience in shaping a data culture. However, it is considered extremely relevant, addressing, among other aspects, the qualification, codification and directing the use of this data. This strategy can also support the (persistent) gap that relates the need to adjust the collection instrument to capture relevant information and the capacity to incorporate this instrument into information systems, by creating data processing and codification strategies.

## References

ADMINISTRATIVE DATA RESEARCH UK. *Administrative data is an invaluable resource for public good. Let's use it. Annual Report 2018–19.* 2019.

ARRUTI, José Maurício. Ethnicity. In: SANSONE, L.; ALVES FURTADO, C. (org.). *Critical dictionary of the social sciences of Portuguese-speaking countries.* Salvador: EDUFBA, 2014. p. 199-2013.

BALESTRA, C.; FLEISCHER, L. *Diversity statistics in the OECD: how do OECD countries collect data on ethnic, racial and indigenous identities?* OECD Statistics Working Papers, No. 2018/09, Paris: OECD Publishing, 2018. Available at: <https://doi.org/10.1787/89bae654-en> . Accessed on: April 21, 2023.

BOTOKO CLAEYSEN, Catherine et al. *Diversity Data Collection: Exploratory Mapping & Reflection: Una Europa Diversity Council Action Group Data Collection Final Report 2022.* Una Europa, 2022. Available at: <https://paris1.hal.science/hal-03930967/> . Accessed on: March 8, 2024.

BRAZIL. [Constitution (1988)]. *Constitution of the Federative Republic of Brazil of 1988.* Brasília, DF: President of the Republic. Available at: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituacaocompilado.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituacaocompilado.htm) . Accessed on: April 29, 2024.

BRAZIL. Ministry of Citizenship. *PCT Newsletter.* [Informative]. National Secretariat of Social Assistance, 2017. Available at: [https://www.mds.gov.br/webarquivos/arquivo/assistencia\\_social/consulta\\_publica/Informativo%20PCT.pdf](https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf) . Accessed on: February 14, 2024.

BRAZIL. Ministry of Citizenship. *PCT Newsletter.* [Informative]. National Secretariat of Social Assistance, 2017. Available at: [https://www.mds.gov.br/webarquivos/arquivo/assistencia\\_social/consulta\\_publica/Informativo%20PCT.pdf](https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf) . Accessed on: February 14, 2024. P.15.

BRAZIL. Ministry of Health. *The Brazilian experience in health information systems.* Brasília: Ministry of Health Publishing House, 2009. (Series B. Basic Health Texts, v. 1 – Production and dissemination of health information in Brazil).

BRAZIL. Ministry of Health. *Consolidation of the Live Birth Information System.* General Coordination of Epidemiological Information and Analysis. 2011.

BRAZIL. Ministry of Health. National Health Foundation. *Procedures manual for the live birth information system.* Brasilia: Ministry of Health, 2001. 32 p.

BRAZIL. Ministry of Health. *Implementation guide for the Race/Color/Ethnicity issue.* Ministry of Health, University of Brasilia. Brasilia: Ministry of Health, 2018. 38 p.: ill.

BRAZIL. Ministry of Health. *Ordinance No. 2,073 of August 31, 2011.* Regulates the use of interoperability and health information standards for health information systems within the Unified Health System, at the Municipal, District, State and Federal levels, and for private systems and the supplementary health sector. Official Gazette of the Union: section 1, Brasília, DF, p.63, September 1, 2011.

BRAZIL. Ministry of Health. *Ordinance No. 589 of May 20, 2015.* Institutes the National Policy on Health Information and Informatics (PNIIS). Official Gazette of the Union: issue 96, section 1, Brasília, DF, p. 72, May 22, 2015.

BRAZIL. Ministry of Health. Secretariat of Health Care. Department of Primary Care. General Coordination of Food and Nutrition Policy. *Operational manual for use of the Food and Nutrition Surveillance System. SISVAN Version 3.0. Standards and Technical Manuals*. Brasilia: Ministry of Health, 2017.

BRAZIL. Ministry of Health. Secretariat of Health Care. Department of Primary Care. General Coordination of Food and Nutrition Policy. *Operational manual for use of the Food and Nutrition Surveillance System. SISVAN Version 3.0. Standards and Technical Manuals*. Brasilia: Ministry of Health, 2017.

BRAZIL. Ministry of Health. Secretariat of Health Care. *Technical Note No. 18/2014*. Review of the National Health Promotion Policy. Brasília, 2014. Available at: <https://www.conass.org.br/biblioteca/wp-content/uploads/2014/01/NT-18-2014-Politica-de-Promo%CC%A7a%CC%83o-da-Sau%CC%81de.pdf> . Accessed on: April 29, 2024.

BRAZIL. Ministry of Health. Secretariat of Strategic and Participatory Management. Department of Support for Participatory Management. *National Comprehensive Health Policy for Lesbians, Gays, Bisexuals, Transvestites and Transsexuals*. Ministry of Health, Secretariat of Strategic and Participatory Management, Department of Support for Participatory Management. Brasília, DF: Ministry of Health, 1st ed., 2013.

BRAZIL. Ministry of Health. Secretariat of Strategic and Participatory Management. Department of Support for Participatory Management. *National Comprehensive Health Policy for Lesbians, Gays, Bisexuals, Transvestites and Transsexuals*. Ministry of Health, Secretariat of Strategic and Participatory Management, Department of Support for Participatory Management. Brasília, DF: Ministry of Health, 1st ed., 2013.

BRAZIL. Ministry of Health. Secretariat of Health and Environmental Surveillance. Department of Epidemiological Analysis and Surveillance of Noncommunicable Diseases. *Surveillance Data: profiles of databases produced by Health Surveillance in Brazil*. Brasilia: Ministry of Health, 2023. 127 p.: ill.

BRAZIL. Ministry of Health. Secretariat of Health Surveillance. Department of Strategic Coordination of Health Surveillance. *Health Surveillance Guide* [[electronic resource] / Ministry of Health, Health Surveillance Secretariat. Department of Strategic Coordination of Health Surveillance. -5th ed. rev. and update. Brasília: Ministry of Health, 2022. 1,126 p.

BRAZIL. Ministry of Health. Health Surveillance Secretariat. Department of Health Situation Analysis. *Legislation Relating to Mortality Information Systems (SIM) and Live Births Information Systems (SINASC)*. Brasilia: Ministry of Health, 2004.

BRAZIL. Ministry of Health. Health Surveillance Secretariat. *Technical Note No. 34/2023: updates and recommendations for the surveillance of congenital anomalies in Brazil*. Brasília, DF, 2023. Available at: <http://plataforma.saude.gov.br/anomalias-congenitas/nota-tecnica-34-2023.pdf> . Accessed on: March 8, 2024.

BRAZIL. Ministry of Health. Health Surveillance Secretariat. *Notifiable Diseases Information System. Notification Form*. Brasilia: Ministry of Health, 2006.

BRAZIL. Ministry of Health. Executive Secretariat. SUS Information Technology Department. *National Policy on Health Information and Informatics: Proposal Version 2.0* (Includes deliberations of the 12th National Health Conference). 2004. Available at: [http://bvsmms.saude.gov.br/bvs/publicacoes/PoliticaInformacaoSaude29\\_03\\_2004.pdf](http://bvsmms.saude.gov.br/bvs/publicacoes/PoliticaInformacaoSaude29_03_2004.pdf) . Accessed on: August 1, 2024.

BRAZIL. Ministry of Health. *Health care information systems: historical contexts, advances and perspectives in the SUS*. Brasília, DF: Graphic City and Publishing LTDA, Oct. 2015.

BRAZIL. Ministry of Social Development. *Social work with indigenous families in basic social protection*. Brasília, DF: MDS, National Secretariat of Social Assistance, 2017.

CANAVESE, D. et al. For the urgent and definitive inclusion of gender identity and sexual orientation fields in the SUS health information systems: what can we learn from the monkeypox outbreak?. *Science & Public Health*, v. 27, no. 11, p. 4191–4194, nov. 2022.

COELHO NETO, GC ; CHIORO, A. After all, how many national Health Information Systems are there in Brazil? *Public Health Notebooks*, v. 37, n. 7, p. e00182119, 2021. Available at: <https://www.scielo.br/j/csp/a/RzNmVjHqmLhPHZp6gfcD6H/?format=pdf&lang=pt> . Accessed on: April 29, 2024.

COELHO, R. ; REMÉDIOS, J. ; NOBRE, V. ; MREJEN, M. The race/color question in DataSUS: evolution and determinants of completeness. *Technical Note No. 30*. IEPS: Sao Paulo, 2023.

COELI, Cláudia Medina. Population data science. *Epidemiology and health services*: journal of the Brazilian Unified Health System, v. 31, n. 3, e2022119, 19 Dec. 2022. doi:10.1590/S2237-96222022000300001.

COSTA, Fabiana Claudia Viana. *Designation and enunciative reference of the 2000 Demographic Census. 2004*. Dissertation (Master's in Linguistics)–UNICAMP, Institute of Language Studies, State University of Campinas, Campinas, São Paulo, 2004.

BROWN, Jane. *Brazil shows its face: images of the Brazilian population in the demographic censuses from 1872 to 2000*. Rio de Janeiro: National School of Statistical Sciences, 2003. 75 p. ISSN 1677-7093; n. 6.

EC-EUROPEAN COMMISSION, Directorate-General for Justice and Consumers, FARKAS, L. *Analysis and comparative review of equality data collection practices in the European Union*. EC: Data collection in the field of ethnicity, Publications Office, 2017.

FERREIRA, FPM Administrative records as a source of statistical data. *Public Informatics*, year 10, n. 1, p. 81-93, 2008.

UNITED NATIONS POPULATION FUND. *Proposed Projects and Programs: Assistance to the Government of Brazil (DP/FPA/BRA/3)*. United Nations Population Fund, 2001. Available at: [https://brazil.unfpa.org/sites/default/files/pub-pdf/country\\_programme20022006\\_0.pdf](https://brazil.unfpa.org/sites/default/files/pub-pdf/country_programme20022006_0.pdf) . Accessed on: April 29, 2024.

IEPS; UMANE; VEREDAS INSTITUTE. *Technical Report No. 1/2023. Health of Indigenous and Quilombola Peoples*. London: Oxford University Press, 2019.

LEAL, CHS; SCALCO, M.L.A.; NUNES, RPD; CONSORTII, ER;

KITAGAWA, BY Violence surveillance: considerations on information related to violence perpetrated against the LGBT population in the city of São Paulo. *Bis*, São Paulo, v. 2, n. 19, p. 55-61, Dec. 2018. Available at: <https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n-2-diversidade-55-61.pdf> . Accessed on: April 19, 2024.

LOVEMAN, M. The politics of a transformed data landscape: ethnoracial statistics in Brazil in a regional comparative perspective. *Sociologies*, v. 23, no. 56, p. 110–153, Jan. 2021.

MELLO, Janine. State production of evidence and use of administrative records in public policies. In: KOGA, Natália Massaco (Org.) et al. *Public policies and the use of evidence in Brazil: concepts, methods, contexts and practices*. Brasília: IPEA, 2022. p. 897-914.

MIGUEL, Nadya Maria Deps. *The Brazilian Profile constructed by IBGE: a discursive memory of the Demographic Censuses from 1940 to 2010*. Thesis (Postgraduate Program in Social Memory) – Federal University of the State of Rio de Janeiro, Rio de Janeiro, 2012.

OLIVEIRA, DC Representation of the LGBTQIA+ population in epidemiological research, in the context of the National Policy for Comprehensive Health of Lesbians, Gays, Bisexuals, Transvestites and Transsexuals: expanding the production of knowledge in the SUS for social justice. *Epidemiology and Health Services*, v. 31, n. 1, e2022020, 2022.

OSORIO, Rafael Guerreiro. *The IBGE Color and Race Classification System*. Brasília: Ipea, Ministry of Planning, Budget and Management, 2003. (Text for discussion, 996).

PANZARDI, R.; CALCOPIETRO, C.; IVANOVIC, EF *New-economy sector study: electronic government and governance – lessons from Argentina*. Working paper. Washington, DC: World Bank, Jul. 2002. Available at: <https://documentos.bancomundial.org/es/publication/documents-reports/documentdetail/527061468769894044/new-economy-sector-study-electronic-government-and-governance-lessons-from-argentina> . Accessed on: February 14, 2024.

ROSENSTREICH, G. et al. *Diversity Data Collection: Exploratory Mapping & Reflection*. Una Europa, 2022. Available at: <https://una-europa.imgix.net/resources/Diversity-Data-Collection-Exploratory-Mapping-Reflection.pdf> . Accessed on: February 14, 2024.

SENRA, N. de C. The issue of administrative records vis-à-vis the generation of statistics. *Brazilian Journal of Population Studies*, [S. l.], v. 13, n. 2, p. 199–205, 1996. Available at: <https://rebep.org.br/revista/article/view/437> . Accessed on: July 23, 2024.

WORLD BANK. *Managing development: the governance dimension*. Washington, DC: World Bank Group, 1991. Available at: <http://documents.worldbank.org/curated/en/884111468134710535/Managing-development-the-governance-dimension> . Accessed on: February 14, 2024.



Access our networks



[itsrio.org](https://itsrio.org)

This book was composed in Termina, FreightSans Pro and Public Sans fonts and released by the Instituto of Technology and Society, in January 2025.