DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Artificial Intelligence and Connected Society

edited by
Sérgio Branco
Chiara de Teffé

published
January/2025

ITS
UERJ UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
DIREITO UERJ
CEPED

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Artificial Intelligence and Connected Society

edited by
Sérgio Branco
Chiara de Teffé

published
January/2025

Editors:

Sérgio Branco and Chiara de Teffé

Graphic design, cover, and layout:

Leandro Collares and Mariana Bertoluci

Editorial production:

Instituto de Tecnologia
e Sociedade - ITS

Copyediting:

Chiara de Teffé and Mariana Bertoluci

International Cataloging-in-Publication Data (CIP)
(Câmara Brasileira do Livro, SP, Brazil)

Inteligência artificial e sociedade conectada [e-book] / edited by Sérgio Branco, Chiara de Teffé. -- 1st ed. -- Rio de Janeiro : ITS - Instituto de Tecnologia E Sociedade, 2025. -- (Diálogos da pós-graduação em direito digital) PDF

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

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

24-243711 UDC-34:004.8

Subject classification index:

1. Artificial intelligence and law 34:004.8

Aline Graziele Benitez - Librarian - CRB-1/3129

How to cite:

BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Eds.). Inteligência artificial e sociedade conectada. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2025. 368p.

INSTITUTO DE TECNOLOGIA E SOCIEDADE:

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

The work Inteligência Artificial e Sociedade Conectada is protected by the following license:

Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International

---

You are free to:

Share — copy and redistribute the material in any medium or format. The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — 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.

NonCommercial — You may not use the material for commercial purposes.

NoDerivatives — 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

LIST OF AUTHORS

Bárbara Gomes D’Ascenção

Carolina Freitas Gomide de Araujo

Cláudio Mendes da Silva

Daniel Santiago Diniz

Elmano Rodrigues Pinheiro Filho

Giovana Sant’Anna

Henrique Segolin Molina

Lígia Maria de Souza Lopes Reis

Luís Henrique de Menezes Acioly

Luisa Amélia

Maíra Lima de Souza

Maria Fernanda Longato Maturana

Matheus Mantuani

Nina Ramalho Pinheiro

Rodrigo Santana dos Santos

Taís Bigarella Lemos

Victor Chame Alvim

Vinicius Azevedo Coelho

FOREWORD

Against a backdrop of rapid innovation, as Artificial Intelligence and digital technologies reshape human and institutional relationships, the book Artificial Intelligence and Connected Society seeks to contribute to the legal, social, and technological debates of this new era.

Organized into three thematic sections, the book features analyses by specialist authors, all students in the postgraduate specialization program in Digital Law offered by ITS Rio in partnership with UERJ and CEPED. They explore the complex aspects of artificial intelligence regulation, data protection, and the development of smart cities. This book is essential reading for scholars, professionals, and anyone interested in the profound impacts of artificial intelligence on an increasingly connected society.

The first section, devoted to Artificial Intelligence, takes a broad approach to the regulatory issues surrounding AI, particularly in the Brazilian context. Questions such as identifying a regulatory authority for AI, training AI through web scraping, and the originality of AI creations highlight the importance of defining limits and responsibilities for this technology. Important themes such as racism and algorithmic discrimination are explored in detailed discussions ranging from social justice to the urgent need for regulations that promote fair and responsible AI. Finally, the book examines the emerging field of neurorights and its implications, highlighting the direct impact of AI on fundamental rights.

In the second section, Smart Cities and New Technologies, the authors analyze the implications of technology for so-called smart cities and the regulations that arise to accompany them. Issues such as necropolitics and data protection in smart cities are examined, offering a critical perspective on how these innovations affect fundamental rights. Discussions of regulatory sandboxes at the municipal level and the role of the Central Bank in regulating payment fintechs give readers a practical view of the advances and complexities that technology brings to legal certainty and public governance. An examination of blockchain technology introduces a gender perspective, encouraging reflection on inclusion in a rapidly developing field.

FOREWORD

The third section, Data Protection and Digital Security, offers a regulatory analysis aimed at strengthening cybersecurity and personal data protection against the threats found in the virtual environment. One highlight is the discussion of cybersecurity for children, which explores the need for specific policies to ensure the safety of children and adolescents online in an increasingly connected world. The section closes with an analysis of the legal bases for collecting data in healthcare, 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 combines academic rigor with an innovative perspective on the contemporary challenges posed by digital technologies. With reflections that transcend borders and disciplines, this book is a valuable resource for understanding how society can advance ethically, inclusively, and with better information in the digital age.

ITS Rio believes in the importance of sharing knowledge and making it accessible. For this reason, this and the other publications from the postgraduate program are available free of charge, openly, and under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International license (CC BY-NC-ND 4.0).

In the coming years, we hope to expand our partnerships and develop further digital education initiatives that benefit society and promote access to culture, innovation, and information.

We note that the content presented here does not necessarily reflect the institutional views of ITS Rio or its members. It represents academic reflection for which its author bears sole responsibility.

We thank everyone who contributed to this project and took an interest in it.

We invite you to explore the other ITS Rio publications. We remain available and are always open to dialogue.

Rio de Janeiro, December 02, 2024.

THE EDITORS

THE EDITORS

Chiara de Teffé

She holds a doctorate and a master's degree in Civil Law from the Universidade do Estado do Rio de Janeiro (UERJ), with distinction, commendation, and a recommendation for publication. She earned her law degree from the Universidade Federal do Rio de Janeiro (UFRJ), where she received undergraduate research scholarships from CNPq and FAPERJ. She is currently the academic coordinator of the postgraduate program in Digital Law at the Instituto de Tecnologia e Sociedade do Rio (ITS Rio), offered in partnership with UERJ, and teaches Civil Law and Digital Law at IBMEC Law School. She teaches specialized postgraduate and extension courses at CEPED-UERJ, PUC-Rio, EMERJ, and ITS Rio. She is a member of the OAB/RJ Data Protection and Privacy Committee and the Civil Law Committee of the OAB Rio de Janeiro Sectional Council (2022/2024). She is a member of EMERJ's Permanent Forum on Freedom of Expression, Fundamental Freedoms, and Democracy, and its Permanent Forum on Technological Innovation in Law. She previously served as a substitute professor of Civil Law at UFRJ. She is an associate member of the Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC) and a full member of the Rio de Janeiro Municipal Council for Personal Data Protection and Privacy. She practices law in Civil Law and Digital Law and works as a personal data protection consultant. She is the author of the books "Dados pessoais sensíveis: qualificação, tratamento e boas práticas" and "Proteção do direito à imagem na Internet: da identificação do dano à sua compensação".

Sérgio Branco

Cofounder and director of the Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). He holds a doctorate and a master's degree in Civil Law from the Universidade do Estado do Rio de Janeiro (Uerj). He is a visiting researcher at the Centre de Recherche en Droit Publique at the Universidade de Montreal. He was a Visiting Research Fellow at Sciences Po between 2023 and 2024. He holds a specialization in intellectual property from the Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio, a postgraduate qualification in documentary film from FGV, and a law degree from the Universidade do Estado do Rio de Janeiro (Uerj). He is a partner at the law firm Rennó Penteado Sampaio.

CONTENTS

SECTION 1

ARTIFICIAL INTELLIGENCE

13 **Regulating artificial intelligence**: reflections on identifying a competent authority in Brazil

ELMANO RODRIGUES PINHEIRO FILHO

35 **Artificial Intelligence and Personal Data Protection**: reflections on the appropriate legal basis for training through web scraping

MATHEUS MANTUANI

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

BÁRBARA GOMES D'ASCENÇÃO

72 **Collecting Personal Data to Train Generative Artificial Intelligence**: A Challenge for Data Protection and Privacy

RODRIGO SANTANA DOS SANTOS

94 **Classifying harm arising from AI incidents**

VINICIUS AZEVEDO COELHO

113 **Bill 2.338/2023**: a study of the copyright provisions

NINA RAMALHO PINHEIRO

133 **Algorithmic Originality**: are the outputs of generative artificial intelligence original?

TAÍS BIGARELLA LEMOS

CONTENTS

151 The challenges surrounding 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 AMÉLIA LINO

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

HENRIQUE SEGOLIN MOLINA

SECTION II

SMART CITIES AND NEW TECHNOLOGIES

212 **Smart Cities and Necropolitics**: Data protection and fundamental rights in the Digital Age

CLÁUDIO MENDES DA SILVA

230 **Implementing smart cities and regulatory sandboxes**: Challenges and opportunities under the Juiz de Fora innovation law

DANIEL SANTIAGO DINIZ

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

LUÍS HENRIQUE DE MENEZES ACIOLY

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

VICTOR CHAME ALVIM

CONTENTS

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

CAROLINA FREITAS GOMIDE DE ARAUJO

SECTION 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 better protection for children and adolescents online

LÍGIA MARIA DE SOUZA LOPES REIS

346 The legal bases for collecting information about diversity in Health and Digital Health

MAÍRA LIMA DE SOUZA

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

SECTION 1

Artificial Intelligence

artificial intelligence and connected society

AUTHORS

Bárbara Gomes D'Ascenção

Elmano Rodrigues Pinheiro Filho

Henrique Segolin Molina

Luisa Amélia

Maria Fernanda Longato Maturana

Matheus Mantuani

Nina Ramalho Pinheiro

Rodrigo Santana dos Santos

Taís Bigarella Lemos

Vinicius Azevedo Coelho

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

1

Regulating artificial intelligence: reflections on identifying a competent authority in Brazil

ELMANO RODRIGUES PINHEIRO FILHO

Contents: Introduction. 1. Regulating emerging digital technologies. 2. Regulating 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 identifying a competent authority to regulate artificial intelligence in Brazil. Final considerations. References.

Introduction

Regulation is a central theme in many contemporary public policy discussions. After the economic crisis of 2008 and the COVID-19 pandemic, few would dispute the importance of regulation for the proper functioning of modern market economies.[2] Yet the role of regulation has not always been understood, recognized, or welcomed, especially when it comes to emerging digital technologies, as was the case with the internet.

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

Contrary to this utopian view, the internet is now seen as an extension of the “real world.” As networks have spread into every area of society—political, economic, social, and cultural—discussions have come to recognize regulation as essential, both to curb undesirable behavior, such as the concentration of markets by digital platforms, and to promote positive uses, such as access to digital content that respects copyright.

The debate over regulating emerging digital technologies, as happened with the internet, has reached a new level in recent years, marking a kind of loss of innocence compared with discussions in the 1990s and 2000s. While arguments

1. He holds a degree in Electrical Engineering with an emphasis on Electronics from the Universidade Estadual Paulista (Unesp), a postgraduate qualification in Telecommunications Regulation from the Universidade de Brasília (UnB), and a Master of Science in Electrical Engineering from the Instituto Militar de Engenharia (IME). He is a postgraduate student in Digital Law at the Instituto de Tecnologia e Sociedade do Rio (ITS), in partnership with the Universidade do Estado do Rio de Janeiro (UERJ) and the Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). He has worked as a Regulation Specialist at the Agência Nacional de Telecomunicações (Anatel) since 2005.

2. LODGE, Martin; WEGRICH, Kai. O enraizamento da Regulação de Qualidade: fazer as perguntas difíceis é a resposta. In: PROENÇA, Jadir Dias; COSTA, Patrícia Vieira da; MONTAGNER, Paula (Eds.). Desafios da regulação no Brasil. Brasília: ENAP, 2009. p. 17.

against any form of regulation predominated in the earlier period, with a utopian perspective on the benefits that unchecked technological innovation could bring, a much more skeptical and pessimistic view has emerged over the past twenty years,[3] recognizing the need for a specific legal framework to minimize its possible harmful effects. Nevertheless, this regulation has been developed from an adaptive perspective, grounded in experience and practice, so that it can be effective and relevant, as had already been envisaged for regulating the internet.[4]

The purpose of this paper is to explore one of the most significant emerging digital technologies: artificial intelligence. It does not, however, seek to address the subject exhaustively. Given its complexity, a detailed analysis of every aspect involved would go beyond the limits set for this paper. The aim is to examine specific aspects of artificial intelligence regulation.

The general objective of this paper is to assess different models of artificial intelligence regulation currently being implemented. More specifically, it seeks to understand the distinctive features of digital technology regulation and the possible impacts of its implementation; examine the different regulatory approaches and structures for artificial intelligence in the European Union, the United States, and the United Kingdom; assess the proposed regulation of artificial intelligence in Brazil; and investigate how Bill No. 2.338 of 2023 addresses the identification of a competent authority to regulate artificial intelligence.

This subject is relevant because emerging digital technologies transform personal and property relationships, creating and improving products, services, and activities, procedures, and practices across various economic sectors and many aspects of society, while also creating new risks and amplifying existing ones. The use of artificial intelligence, for example, to produce or manipulate content intended to disseminate facts that are manifestly false or taken out of context can potentially undermine the balance and integrity of electoral processes, thus justifying some form of regulation. The analysis will use a literature review methodology.

3. BIANQUINI, Heloisa. Regulação ex ante, regulação ex post e regulação responsiva: notas exploratórias sobre o processo sancionador da Autoridade Nacional de Proteção de Dados. In: CAMPOS, Ricardo (Ed.). O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil. 1st ed. São Paulo: Editora Contracorrente, 2023. pp. 266-267.

4. LESSIG, Lawrence. The Law of the Horse: What Cyber Law Might Teach. Harvard Law Review, Harvard, v. 113, pp. 501-546, Dec. 1999. Available at: https://cyber.harvard.edu/works/lessig/finalhls.pdf. Accessed: Oct. 1, 2024.

Accordingly, this article is divided into four chapters. Chapter 1 presents considerations on regulatory theory and the challenges of regulating emerging digital technologies, such as artificial intelligence. Chapter 2, divided into two sections, examines the evolution of artificial intelligence regulation worldwide, presenting some approaches already adopted and the debate on artificial intelligence regulation in Brazil. Chapter 3 reflects on identifying a competent authority to regulate artificial intelligence in the country, presenting the advantages and disadvantages of adopting different models under the coordination of different entities. The paper closes with final considerations, highlighting its main findings and offering suggestions for future research.

1. Regulating emerging digital technologies

Digital technologies are revolutionizing almost every sector of the economy, introducing innovative products and services, enabling new business models, and transforming how countries promote and benefit from socioeconomic development. Digital technologies 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, this transformation must be accompanied by appropriate public policies and a regulatory environment that promote fair competition, protect consumers, and encourage responsible innovation.[5]

The digitization of societies and economies is generating unprecedented amounts of data, driven by rapidly growing 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 encourage this interaction. At the same time, more devices are becoming "smart," connecting to the internet to exchange information. The explosive growth of data has led to new technologies that filter and analyze large datasets, broadly described as artificial intelligence and big data.[6]

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

6. Ibid., p. 142.

These technological innovations are challenging regulators to review their strategies for promoting fair competition and protecting consumers. Beyond technical challenges, these technologies raise legal, ethical, and macroeconomic questions. Central banks, consumer protection agencies, competition commissions, and Information and Communication Technology (ICT) regulators are working to assess the impact of these changes in their respective areas of responsibility. This may require redesigning the functions of various regulators.[7]

For regulators overseeing the ICT sector, who are directly involved with emerging digital technologies, the Digital Regulation Handbook, published by the ITU and the World Bank, identifies three main institutional models: sector-specific regulators, multisector regulators, and converged regulators. According to the study, regulators with an exclusive focus were traditionally common in telecommunications regulation. Today, however, these regulators are less common than converged or multisector regulators.

It can therefore be said that the digital age has profoundly changed the roles of regulators and public policymakers. Although regulators' traditional areas of responsibility and institutional structures may remain relevant in the digital environment, regulation needs to become more flexible and adaptable. Regulators' mandates may also need to be adjusted to encompass new digital realities.[8]

However, these new areas do not always fit neatly within existing regulatory structures, and many countries have been discussing whether their traditional regulators have the authority needed to address emerging digital technologies. Although these discussions are at an early stage, the analysis generally involves assessing whether a new regulator devoted exclusively to digital matters is needed, whether the mandate of an existing regulator should be expanded, or whether the most appropriate model would be an ICT regulator working with other government authorities responsible for areas such as consumer protection, privacy, and cybersecurity.[9]

7. Ibid., p. 142.

8. SCHOLZE, Simone Henriqueta Cossetin; VIEIRA, Vania Lucia Ribeiro; AGUIAR, Alexandre Kehrig Veronese. *Estudo sobre modelo regulatório pró-inovação*. 2024. p. 41.

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

2. Regulating artificial intelligence

To discuss the regulation of artificial intelligence, it is essential to clarify what is meant by artificial intelligence (AI). Definitions vary according to the field of knowledge used to explain it and take into account its transdisciplinary nature and the complexity of its systems, algorithms, and applications.[10] Given the rapid pace of technological advancement, the concept of artificial intelligence has also been continually updated and adjusted to reflect the latest changes.

In this context, while recognizing that the concept is subject to revision, the Organization for Economic Co-operation and Development (OECD) defines artificial intelligence as a machine-based system that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.[11]

As defined, artificial intelligence is an emerging digital technology with 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 people and society and may threaten these essential rights and freedoms. One such risk is the spread of bias and discrimination, through which AI may make discriminatory decisions. Other risks commonly associated with AI use include privacy violations; cybersecurity; malicious uses, such as fraud and unlawful acts; obtaining information that could pose risks to people's safety; disinformation and information manipulation; and harm or losses caused by unintended consequences.[12]

These technology-related risks have led to growing demand for the legal regulation of artificial intelligence. There are various approaches to this regulation, including creating AI-specific laws,

10. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. In: CAMPOS, Ricardo (Ed.). O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil. 1st ed. São Paulo: Editora Contracorrente, 2023. pp. 756-757.

11. ORGANIZATION FOR ECONOMIC CO-OPERATION 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: July 26, 2024.

12. BRASIL. Tribunal de Contas da União. Acórdão nº 616/2024. Plenary. Reporting Minister: Aroldo Cedraz. Session of 03/04/2024. Brasília, TCU, 2024. p. 6. Available at: https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233. Accessed: July 22, 2024.

adopting legislation that promotes innovation, or even deciding not to regulate on the grounds that existing regulations are already sufficient.[13]

Given the dynamic and rapidly evolving nature of this field, 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. One of the main challenges is therefore to strike a balance between protecting individual and collective rights and enabling innovation and market development.[14] In this environment, the regulatory approaches being used can be grouped into several types,[15] of which three stand out: principles-based, risk-based, and rights-based regulation.

Principles-based regulation steers the development and use of artificial intelligence (AI) systems by establishing general premises and ethical guidelines, without having 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 processes that respect human rights.[16]

Risk-based regulation, in turn, focuses on identifying and managing the risks associated with developing and using artificial intelligence systems. This approach seeks to adapt regulatory obligations or requirements to the level of risk posed by different types of AI systems.[17] Unlike principles-based regulation, which is more flexible and guided by general values, risk-based regulation adopts a more structured and specific method. It classifies AI systems by risk level and defines strict governance standards based on the severity of the risks identified. This approach seeks to ensure that control and regulatory measures are proportionate to the risk posed by each AI application.[18]

13. Ibid., pp. 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: Oct. 1, 2024.

16. Ibid., p. 21.

17. Ibid., p. 35.

18. BRASIL. Tribunal de Contas da União. Acórdão nº 616/2024. Plenary. Reporting Minister: Aroldo Cedraz. Session of 03/04/2024. Brasília, TCU, 2024, p. 8. Available at: https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233. Accessed: July 22, 2024.

Finally, rights-based regulation emphasizes the protection of human and fundamental rights in the context of artificial intelligence systems. This approach defines in advance a specific set of rights and obligations that must be respected when developing and using AI, prioritizing the safeguarding of users' rights. Although this approach offers a clear set of rules and protections, it may face significant challenges, particularly because its detailed and comprehensive nature 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 may pose greater challenges for innovation and technological advancement as it seeks to balance the protection of individual rights with the need for flexibility in technological development.[19]

From an internationalist perspective, AI policy and regulatory approaches can also be organized into three forms of legal intervention: multilateral and regional dialogues (particularly through international organizations such as the United Nations and the European Union); national strategies (adopting government policies to stimulate artificial intelligence domestically); and transnational regulatory standards (such as principles, codes of conduct, guidelines, and recommendations from nonstate actors).[20]

To analyze these regulatory approaches in greater detail, the next section will explore regulatory initiatives in the European Union (EU), the United States, and the United Kingdom, and then examine the case of Brazil.

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

Various countries are currently developing regulatory frameworks to integrate artificial intelligence into their legal systems. Globally, there is a common trend in government and jurisdictional approaches aimed not only at harnessing the benefits of AI systems for society, industry, and the public sector, but also at balancing

19. Ibid., p. 8.

20. POLIDO, Fabrício Bertini Pasquot. Novas perspectivas para regulação da inteligência artificial: diálogos entre as políticas domésticas e os processos legais transnacionais. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Eds.). Inteligência artificial e direito: ética, regulação e responsabilidade. 2nd ed., revised, updated, and expanded. São Paulo: Thomson Reuters Brasil, 2020. p. 180.

those advantages with the ethical and legal concerns associated with their implementation.[21]

Drawing on its experience with personal data protection, which led to the General Data Protection Regulation (GDPR), a regulatory model in that field, the European Union has made a sustained effort to develop a comprehensive AI framework that ensures safe and ethical technology. In 2018, the European Commission created a dedicated group to address AI, marking the start of regulatory work. A proposal for AI legislation was published in 2021. Following extensive discussions, the European Parliament adopted its negotiating position in June 2023, and a final agreement was reached in December of the same year. It became known as the Artificial Intelligence Act (EU AI Act).[22]

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 issues such as data governance, transparency, and security, but also includes an experimental regulatory environment (a regulatory sandbox[23]). This strategy seeks to ensure that regulation is adaptable and balanced, encouraging innovation while protecting users' rights and safety.[24]

To implement the EU AI Act, each EU Member State must designate or create a national authority responsible for assessing and monitoring compliance with the legislation. The proposal also provides for the creation of the European Artificial Intelligence Board, a committee intended to advise and assist national authorities in applying the rules. However, recent amendments suggest a need for a centralized agency with its own legal personality, funding, and staff to coordinate and harmonize action among Member States and prevent market fragmentation. This proposal seeks to ensure more uniform and effective regulation, aligning

21. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. In: CAMPOS, Ricardo (Ed.). O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil. 1st ed. São Paulo: Editora Contracorrente, 2023. p. 762.

22. BRASIL. Tribunal de Contas da União. Acórdão nº 616/2024. Plenary. Reporting Minister: Aroldo Cedraz. Session of 03/04/2024. Brasília, TCU, 2024, p. 8. Available at: https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233. Accessed: July 22, 2024.

23. A sandbox allows more flexible experimentation with new products and services while maintaining regulatory oversight. This strategy seeks to ensure that regulation is adaptable and balanced, encouraging innovation while protecting users' rights and safety.

24. Ibid., p. 8.

national decisions and promoting a trustworthy, cohesive AI ecosystem throughout the European Union.[25]

AI regulation in the United States, in turn, is at an early stage, reflecting an approach that is still developing to address this technology's rapid evolution. In October 2022, the country released the Blueprint for an 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 constitute formal legislation.[26] This document serves as a guide to principles for the U.S. government, focusing on avoiding regulatory overload and maintaining U.S. leadership in AI.[27] More recently, in October 2023, President Joe Biden issued an executive order[28] establishing new standards for safety and security, addressing concerns such as privacy and equity, and encouraging innovation and research in the sector.[29]

In the United States, the recent regulatory framework adopts a sectoral approach characterized by coregulation, through the actions of federal regulatory agencies and state and local governments. In this framework, federal bodies are responsible for issuing principles-based guidelines and leave implementation to the private sector. The Federal Trade Commission (FTC), for example, has published guidelines highlighting the importance of AI systems being transparent, explainable, fair, and accountable. The Department of Defense (DoD) has adopted ethical AI principles applicable to combat and noncombat functions, focusing on responsibility, equity, traceability, reliability, and governability. The Food and Drug Administration (FDA) has also introduced an action plan for AI software as a medical device, seeking to assess and monitor such software throughout its lifecycle.[30]

25. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. In: CAMPOS, Ricardo (Ed.). O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil. 1st ed. São Paulo: Editora Contracorrente, 2023. p. 764.

26. MELO, Ana Karolina Acris; SOUZA, Géssica Cardoso; VASCO, Amanda Corrêa; REIS, Bruno Salomon. Regulação da Inteligência Artificial: benchmarking de países selecionados. Brasília: Escola Nacional de Administração Pública, 2022. p. 18. Available at: https://repositorio.enap.gov.br/handle/1/7419. Accessed: Oct. 1, 2024.

27. The text does not introduce a new U.S. law or regulatory policy. It is a statement of principles based on five fundamental premises for protecting the public in the age of artificial intelligence: 1. Automated systems must be safe and effective; 2. Users must be protected against algorithmic discrimination, ensuring equitable use; 3. People must have control over the use of their data, preventing abusive practices; 4. Users must understand how and why an AI system made a particular decision; 5. People must have the option to refuse AI decisions and request human assessment in the event of an error or challenge.

28. Executive Order, comparable to a presidential decree in Brazil.

29. NAZARENO, Claudio. Regulação da inteligência artificial: experiências internacionais e desafios para o Brasil. Brasília: Câmara dos Deputados, Consultoria Legislativa, 2024. p. 15. Available at: https://bd.camara.leg.br/bd/handle/bdcamara/41741. Accessed: Oct. 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, v. 48, pp. 3-4.

In addition to guidelines and executive orders, various legislative proposals addressing artificial intelligence have been approved in the United States. These include the Algorithmic Accountability Act and the Consumer Online Privacy Rights Act, which seek to create specific regulations for automated decisions and online privacy. The Good AI Act of 2022 proposes creating an “Artificial Intelligence Hygiene Working Group,” while the Advancing American AI Act seeks to regulate AI use by government agencies. To date, however, there has been no significant progress in adopting these proposals, and the country has no comprehensive federal AI legislation.[31]

In the United Kingdom, the government published the technical document A pro-innovation approach to AI regulation in 2023, reflecting a distinct strategy for regulating artificial intelligence. Through a flexible, iterative approach,[32] the United Kingdom seeks to balance the promotion of innovation with management of the risks associated with the technology. Rather than establishing rigid, immediate regulation, the British model is designed to evolve over time, allowing ongoing adjustments as studies progress and the sector matures. This strategy is guided by principles and premises that adapt to the specific needs of different areas of the economy, favoring regulation of AI use rather than the technology itself.[33]

The aim is therefore to achieve regulation that is predominantly sectoral and adjusted to rapid cycles of technological innovation and development. In this case, the regulatory authority’s central function is not to regulate every aspect of AI directly, but to manage the process through monitoring, evaluation, and feedback. The authority is also responsible for supporting implementation of the regulatory principles, managing cross-sectoral risks, promoting innovation, and ensuring interoperability with international regulatory models.[34]

Alongside its flexible regulatory approach, the U.K. government has also published an algorithmic transparency standard, accompanied by a template and guidelines to support public-sector adoption. This initiative reflects the United Kingdom’s commitment to establishing clear

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

33. BRASIL. Tribunal de Contas da União. Acórdão nº 616/2024. Plenary. Reporting Minister: Aroldo Cedraz. Session of 03/04/2024. Brasília, TCU, 2024, p. 9. Available at: https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233. Accessed: July 22, 2024.

34. Ibid., p. 9.

and responsible practices in the use of algorithm-based systems, seeking to increase transparency and accountability in the public sector.[35]

Alongside the United Kingdom, various countries are adopting a sectoral approach to artificial intelligence regulation.36 37, These countries seek to integrate AI regulation into existing legal systems, ensuring that the principles of responsibility and reliability are effectively upheld within their authorities' specific areas of responsibility.[38]

2.2 Proposals for state regulation of AI in Brazil

The development of artificial intelligence in Brazil has been marked by significant strategic and legislative efforts, reflecting this technology's growing importance to national development. The Brazilian Artificial Intelligence Strategy (EBIA), established by MCTI Ordinance No. 4.617/2021 and updated by Ordinance No. 4.979/2021, is an important initial milestone.[39] Developed on the basis of OECD guidelines, EBIA seeks to promote inclusive growth, transparency, and safety in AI implementation in the country.[40] However, its execution has faced challenges, such as the lack of a detailed timetable and clearly defined responsibilities, which have been criticized by analysts and experts in the field.[41]

EBIA's objectives include promoting investment in research and innovation, training specialized professionals, and facilitating cooperation between the public and private sectors. Despite its fundamental role, the strategy has faced criticism for lacking a detailed plan and a dedicated AI regulator. Implementation has been slow, exacerbated by the change of government in 2023, and a review of the strategy

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, v. 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: Oct. 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: July 31, 2024.

38. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. In: CAMPOS, Ricardo (Ed.). O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil. 1st ed. São Paulo: Editora Contracorrente, 2023, pp. 766-767.

39. Information on advances in the technologies that enable AI, allowing analysis of its adoption and main impacts on society, is available from the Observatório Brasileiro de Inteligência Artificial at: https://obia.nic.br/s/home.

40. BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Estratégia Brasileira de Inteligência Artificial – EBIA. Brasília, MCTIC, 2021, p. 17. Available at: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_diagramacao_4-979_2021.pdf. Accessed: July 26, 2024.

41. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. In: CAMPOS, Ricardo (Ed.). O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil. 1st ed. São Paulo: Editora Contracorrente, 2023. pp. 759-760.

may incorporate new thematic areas and topics, such as cybersecurity and a more robust approach to public safety.[42]

In the National Congress, the debate on AI regulation has advanced through various bills. Bill No. 21 of 2020, approved by the Chamber of Deputies and currently before the Senate, established the initial framework for AI regulation but was criticized for its generic nature and lack of depth. It sought to create basic guidelines and principles for AI use, but did not sufficiently address matters such as privacy, ethics, and the creation of an authority.[43]

This bill was combined with others for joint consideration. To produce 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 preliminary bill to regulate artificial intelligence. Bill No. 2.338 of 2023 was developed in this context, building on the Committee's conclusions and seeking to reconcile, in legislation, the protection of fundamental rights and freedoms, recognition of the value of work and human dignity, and promotion of the technological innovation represented by artificial intelligence.[44]

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. In addressing AI oversight, the bill required the Executive Branch to designate an authority to ensure compliance with the established rules, without specifying whether this would be an existing body within the federal public administration or a new body to be created later.

The substitute to Bill No. 2.338/2023, presented by Senator Eduardo Gomes in June 2024, reflects recent discussions on artificial intelligence, highlighting the need for multisectoral governance and emphasizing transparency, accountability, and the protection of

42. BRASIL. Tribunal de Contas da União. Acórdão nº 616/2024. Plenary. Reporting Minister: Aroldo Cedraz. Session of 03/04/2024. Brasília, TCU, 2024, p. 7. Available at: https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233. Accessed: July 22, 2024.

43. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. In: CAMPOS, Ricardo (Ed.). O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil. 1st ed. São Paulo: Editora Contracorrente, 2023. p. 761.

44. BRASIL. Senado Federal. Projeto de Lei nº 2338, de 3 de maio de 2023. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2023. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Accessed: July 22, 2024.

human rights. The text provides for the creation of a public database of high-risk AI and the civil liability of AI actors, as well as incident reporting and compliance oversight mechanisms. These aspects represent an advance over earlier proposals, seeking to balance the protection of rights with the promotion of innovation. Regarding the competent authority, the substitute to Bill No. 2.338/2023 provides for an inspection and supervision system that includes:

- creating the National System for Artificial Intelligence Regulation and Governance (SIA), which recognizes the regulatory mandates of sectoral authorities;
- designating the National Data Protection Authority (ANPD) as the competent authority to coordinate SIA, with the additional mission of reducing regulatory asymmetry across the various intensive uses of AI systems in unregulated sectors.

3. Reflections on identifying a competent authority to regulate artificial intelligence in Brazil

Regulatory authorities are intended to regulate, organize, control, and oversee specific matters, and may vary in structure, approach, objectives, and scope. They may be established within direct or indirect public administration, or operate as independent entities or private organizations with responsibilities in the public interest.[45] In considering a competent authority to regulate artificial intelligence in Brazil, the issue can essentially be assessed from two perspectives: defining the institutional structure to be used and selecting the body that will serve as that model's central authority.

As discussed in earlier sections, proposals for a competent authority to regulate emerging digital technologies, such as AI, have followed three different models: sector-specific regulators, multisector regulators, and converged regulators.

The AI-specific regulator model, used in Spain, for example, through the creation of the Agencia Española de Supervisión

45. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. In: CAMPOS, Ricardo (Ed.). O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil. 1st ed. São Paulo: Editora Contracorrente, 2023. p. 770.

de la Inteligencia Artificial (AESIA), offers the advantage of designing an authority with the characteristics needed to address the ethical and human rights challenges raised by AI development, deployment, and use. Some argue that, given the complexity of the subject, a regulatory authority would need to bring together various areas of expertise and multidisciplinary knowledge, including legal and technical knowledge, as well as broad regulatory and rulemaking powers.[46] On the other hand, creating a body with such extensive powers and characteristics may require substantial public investment. Furthermore, there is still insufficient information about the effectiveness of this model elsewhere in the world.

The multisector regulator model, used, for example, in Jamaica (the Office of Utilities Regulation, which oversees telecommunications, energy, water, and transport), offers the advantage of using an existing institutional structure to regulate a new sector, with administrative synergies and economies of scale in process improvements. In Brazil, however, no bodies with these characteristics are equipped to regulate AI, since existing bodies, such as the Administrative Council for Economic Defense (CADE), address very specific aspects of regulation (in this case, competition protection).

Creating or merging existing authorities into a converged regulator covering related ICT areas (such as telecommunications and data protection) offers the same advantages as the previous model, with the added benefit of greater specialization. This makes the authority better able to respond swiftly and coherently to emerging AI challenges.[47] China, with the Cyberspace Administration of China,[48] is an example of this approach. In Brazil, such an approach is particularly sensitive because it requires interventions by the Legislative Branch in the Executive Branch.[49]

46. DATA PRIVACY BRASIL. Data Privacy Brasil, 2023. IA no Brasil: quem será responsável pela regulamentação?. Available at: https://www.dataprivacybr.org/documentos/ia-no-brasil-quem-sera-responsavel-pela-regulamentacao/?idProject=2331. Accessed: Oct. 2, 2024

47. BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 16/2023/CGTP/ANPD. Brasília, ANPD, 2023. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Accessed: July 30, 2024.

48. 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: Oct. 2, 2024.

49. One example of controversy was the enactment of the General Personal Data Protection Law (LGPD), when provisions proposed by the Legislative Branch concerning the structure of the National Data Protection Authority (ANPD) were vetoed by the President of the Republic on the grounds of alleged unconstitutionality in the legislative process, for violating Article 61, §1, II, "e," read together with Article 37, XIX of the Constitution. Further information on the reserved power to initiate legislation is available in: REZENDE, R. M. de. A Insustentável Incerteza no Dever-Ser: reserva de iniciativa de leis, jurisprudência oscilante e a criação de fundos orçamentários. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/Senado, April/2017 (Discussion Paper No. 231). Available at: http://senado.leg.br/estudos. Accessed: Oct. 3, 2024.

Assessing the advantages and disadvantages of these three models, and considering the Brazilian legal system and its context, as well as the transdisciplinary nature and complexity of AI systems, a hybrid approach appears most suitable for AI regulation in Brazil. It would use a converged authority to coordinate a regulatory system in association with existing sector-specific regulators, as is expected in France with the National Commission for Information Technology and Civil Liberties (CNIL). This is justified because sectoral authorities, with their experience and expertise, are better placed to address issues concerning the development and application of AI systems in fields such as healthcare, transport, and natural resources.[50] This alternative is consistent with the substitute to Bill No. 2.338/2023 presented by Senator Eduardo Gomes and currently under discussion in the National Congress.

From this perspective, the choice of central regulator naturally falls to one of the two main agencies involved in 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 forms part of the indirect federal public administration, operates as a special-status autonomous agency, and is linked to the Ministry of Communications. It is administratively independent and financially autonomous. Its objective is to promote the development of the country's telecommunications, providing a modern, efficient telecommunications infrastructure capable of offering society adequate, diverse, and fairly priced services throughout the national territory.

Headquartered in Brasília, Anatel conducts inspections and maintains closer contact with society through offices in every Brazilian state capital. According to information from March 2024 [51], its workforce totals 1,343 (one thousand three hundred and forty-three) civil servants, of whom 96.87% are members of its own staff and 2.68% are seconded from other bodies in

50. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. In: CAMPOS, Ricardo (Ed.). O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil. 1st ed. São Paulo: Editora Contracorrente, 2023. p. 772.

51. BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Boletim da Administração Direta, Autárquica e Fundacional. Brasília, MGI, 2024, p. 165. Available at: https://www.gov.br/gestao/pt-br/central-de-conteudo/publicacoes/boletins/boletins-da-administracao-direta. Accessed: July 30, 2024.

the public administration, while 0.45% have no permanent civil service affiliation and occupy positions subject to discretionary appointment and dismissal.

ANPD, in turn, 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). It began effective operation with the appointment of its first Director-President on November 5, 2020. Like Anatel, ANPD is a special-status autonomous agency linked to the Ministry of Justice and Public Security, and consequently has technical and decision-making autonomy and its own assets. ANPD is the central body for interpreting the General Data Protection Law and is responsible for establishing rules and guidelines for its implementation, seeking to uphold every Brazilian's right to have their personal data properly protected.

Headquartered in Brasília, but without decentralized offices, ANPD has no permanent staff of its own. To assemble its workforce, it relied on the secondment of 120 (one hundred and twenty) civil servants from other bodies. Including cleaning staff, secretaries, receptionists, and interns, the agency has a total of 152 (one hundred and fifty-two) people, only 10 (ten) of whom work on inspections or security incident handling, according to information from December 2023 [52].

In light of the above, taking Anatel's current telecommunications responsibilities as a reference, the agency is understood to have experience in activities similar to those required of a competent AI authority, such as accreditation, certification, and inspection.[53] Despite an apparent lack of synergy between the sectors, the development of AI solutions and systems is based on an immense, constantly flowing volume of data, accessible only through a robust, stable, extensive, and resilient connectivity infrastructure comprising multiple access and data transport networks.[54] In addition, if Bill No. 2.768 of 2022

52. CÂMARA DOS DEPUTADOS. Agência Câmara de Notícias, 2023. Presidente da ANPD pede concurso para agência; divisão de fiscalização tem apenas 5 funcionários. Available at: https://www.camara.leg.br/noticias/1014383-presidente-da-anpd-pede-concurso-para-agencia-divisao-de-fiscalizacao-tem-apenas-5-funcionarios. Accessed: July 31, 2024.

53. BRASIL. Agência Nacional de Telecomunicações. Informe nº 27/2024/ARI. Brasília, Anatel, 2024. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqbJNRZm5SUvRZmQf9kFzb6NVVMeEFdPgHerLaOe9k3Jw_0wiL8oZeTeLc2rSt0jscq85OhSwCRK5T4BsfXOKEQg. Accessed: July 30, 2024.

54. BRASIL. Agência Nacional de Telecomunicações. IA – Inteligência Artificial: Visão Institucional de Futuro. Brasília, Anatel, 2024. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYiHvsTCI8r6V0Oltjrypit3yX4N4bkPXcoJgxuzJCUPSMamOo4UK2mN71rPTGc_Cr76yKk1yu0Ggxy4v3MR80F. Accessed: July 30, 2024.

is approved in its current form, the agency's remit in emerging digital technologies would expand. Using this agency as the central body for AI regulation therefore appears appropriate, considering its established structure, regional presence, and workforce.

On the other hand, ANPD is already recognized as a leading entity in personal data protection and safeguarding citizens' privacy. AI, with its ability to process and analyze large volumes of data, is directly aligned with ANPD's responsibilities,55 56,,57 a fact acknowledged in the substitute to Bill No. 2.338/2023 [58]. This intersection between AI and data protection centers AI governance on technical and operational issues, with an ongoing emphasis on protecting fundamental rights and personal data security. It also allows the development of a technical workforce specializing in both areas, optimizing the use of public resources and avoiding regulatory fragmentation and overlapping mandates among different bodies.[59] However, because the agency is recent and still being established, and has neither permanent staff of its own nor decentralized operations, changes to its responsibilities could affect its structure and budgets, compromising its results.

Final considerations

This study has made it possible to understand the distinctive features of digital technology regulation and the possible impacts of its implementation, as well as the different regulatory approaches and structures for artificial intelligence.

The research has also provided a better understanding of the development of artificial intelligence in Brazil, which reflects an ongoing effort to align

55. BRASIL. Autoridade Nacional de Proteção de Dados. Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial. Brasília, ANPD, 2023. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/analisepreliminar-do-pl-2338_2023-formatado-ascom.pdf. Accessed: Oct. 3, 2024.

56. BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 16/2023/CGTP/ANPD. Brasília, ANPD, 2023. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Accessed: July 30, 2024.

57. BRASIL. Autoridade Nacional de Proteção de Dados. PL 2338 – SUBSTITUTIVO – COMISSÃO ESPECIAL CONTRIBUIÇÕES DA ANPD – MAIO - 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. Accessed: Oct. 3, 2024.

58. BRASIL. Senado Federal. Projeto de Lei nº 2338, de 3 de maio de 2023. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2023. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Accessed: July 22, 2024.

59. BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica 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. Accessed: July 30, 2024.

the country with international best practices, promoting responsible and innovative technological development. Although EBIA and bills such as Bill No. 2.338/2023 represent significant advances, effective implementation and the creation of dedicated regulatory structures will be essential to ensure that Brazil fully harnesses AI's potential. This must be done while protecting citizens' rights and promoting a safe, ethical environment for innovation.

Nevertheless, despite the advanced proposals, Brazil faces challenges in effectively implementing these strategies and regulations. The question of creating a specialized regulator or using the existing regulatory structure remains open. A dedicated authority could play a crucial role in applying and enforcing AI laws, as well as in defining best practices and audits.

Regardless of the regulatory system chosen, and in light of the public administration model established by the 1988 Federal Constitution, the authority must be established as a special-status autonomous agency, with technical and decision-making autonomy, as well as its own assets and staff. Experience with implementing regulatory agencies in Brazil indicates that the AI regulatory authority should incorporate practices such as public consultations and hearings, interaction with stakeholders, and collaborative, evidence-based mechanisms into its decision-making process. The authority must also have an advisory body whose principal function is to ensure the active participation of diverse groups and sectors of society in AI-related decisions, both in formulating and implementing public policies and in the work of the central authority.

In light of the above, future research should assess EBIA's effectiveness in practice, analyzing how it has been applied and its impacts to date, as well as regulatory policies in other jurisdictions, to identify success and failure factors and their implications for artificial intelligence regulation in Brazil.

As noted at the outset, this study has confirmed the complexity of the issue of artificial intelligence in our time. It has also highlighted the urgency and inevitability of addressing the subject, and the need to define its regulation so that Brazilian society can meet the challenges that AI presents.

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, v. 48, p. 105767, 2023. Available at: https://doi.org/10.1016/j.clsr.2022.105767. Accessed: 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, v. 47, p. 105761, 2022. Available at: https://doi.org/10.1016/j.clsr.2022.105761. Accessed: July 24, 2024.

BRASIL. Agência Nacional de Telecomunicações. Informe nº 27/2024/ARI . Brasília, Anatel, 2024. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqbJNRZm5SUvRZmQf9kFzb6NVVMeEFdPgHerLaOe9k3Jw_0wiL8oZeTeLc2rSt0jscq85OhSwCRK5T4BsfXOKEQg. Accessed: July 30, 2024.

BRASIL. Agência Nacional de Telecomunicações. IA – Inteligência Artificial: Visão Institucional de Futuro . Brasília, Anatel, 2024. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYiHvsTCI8r6V0Oltjrypit3yX4N4bkPXcoJgxuzJCUPSMamOo4UK2mN71rPTGc-Cr76yKk1yu0Ggxy4v3MR80F. Accessed: July 30, 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial . Brasília, ANPD, 2023. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/analisepreliminar-do-pl-2338_2023-formatado-ascom.pdf. Accessed: Oct. 3, 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 16/2023/CGTP/ANPD . Brasília, ANPD, 2023. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Accessed: July 30, 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. PL 2338 – SUBSTITUTIVO – COMISSÃO ESPECIAL CONTRIBUIÇÕES DA ANPD – MAIO – 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. Accessed: Oct. 3, 2024.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Estratégia Brasileira de Inteligência Artificial – EBIA . Brasília, MCTIC, 2021. Available at: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_diagramacao_4-979_2021.pdf. Accessed: July 26, 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Boletim da Administração Direta, Autárquica e Fundacional . Brasília, MGI, 2024. Available at: https://www.gov.br/gestao/pt-br/central-de-conteudo/publicacoes/boletins/boletins-da-administracao-direta. Accessed: July 30, 2024.

BRASIL. Senado Federal. Projeto de Lei nº 2338, de 3 de maio de 2023. Dispõe sobre o uso da Inteligência Artificial . Brasília: Senado Federal, 2023. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Accessed: July 22, 2024.

BRASIL. Tribunal de Contas da União. Acórdão nº 616/2024 . Plenary. Reporting Minister: Aroldo Cedraz. Session of 03/04/2024. Brasília, TCU, 2024. Available at: https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233. Accessed: July 22, 2024.

CÂMARA DOS DEPUTADOS. Agência Câmara de Notícias, 2023. Presidente da ANPD pede concurso para agência; divisão de fiscalização tem apenas 5 funcionários . Available at: https://www.camara.leg.br/noticias/1014383-presidente-da-anpd-pede-concurso-para-agencia-divisao-de-fiscalizacao-tem-apenas-5-funcionarios. Accessed: July 31, 2024.

CAMPOS, Ricardo (Ed.). O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil . 1st ed. São Paulo: Editora Contracorrente, 2023. 778 p. ISBN 978-65-5396-146-3.

DATA PRIVACY BRASIL. Data Privacy Brasil, 2023. IA no Brasil: quem será responsável pela regulamentação? . Available at: https://www.dataprivacybr.org/documentos/ia-no-brasil-quem-sera-responsavel-pela-regulamentacao/?idProject=2331. Accessed: Oct. 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: July 31, 2024.

FRAZÃO, Ana; MULHOLLAND, Caitlin (Eds.). Inteligência artificial e direito: ética, regulação e responsabilidade . 2nd ed., revised, updated, and expanded. São Paulo: Thomson Reuters Brasil, 2020. 736 p. ISBN 978-65-5614-221-0.

GIL, Antonio Carlos. Como elaborar projetos de pesquisa . 4th ed. São Paulo: Atlas, 2008. 176 p. ISBN 85-224-3169-8.

HARTMANN, Ivar A. (Ed.). Policy Paper: Regulação de Inteligência Artificial no Brasil . Rio de Janeiro: FGV Direito Rio, 2020. 39 p. Available at: https://direitorio.fgv.br/conhecimento/policy-paper-regulacao-de-inteligencia-artificial-no-brasil. Accessed: Oct. 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: Oct. 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: July 24, 2024.

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

MELO, Ana Karolina Acris; SOUZA, Géssica Cardoso; VASCO, Amanda Corrêa; REIS, Bruno Salomon. Regulação da Inteligência Artificial: benchmarking de países selecionados . Brasília: Escola Nacional de Administração Pública, 2022. 35 p. Available at: https://repositorio.enap.gov.br/handle/1/7419. Accessed: Oct. 1, 2024.

NAZARENO, Claudio. Regulação da inteligência artificial: experiências internacionais e desafios para o Brasil . Brasília: Câmara dos Deputados, Consultoria Legislativa, 2024. 32 p. Available at: https://bd.camara.leg.br/bd/handle/bdcamara/41741. Accessed: Oct. 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: Oct. 1, 2024.

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

PROENÇA, Jadir Dias; COSTA, Patrícia Vieira da; MONTAGNER, Paula (Eds.). Desafios da regulação no Brasil. Brasília: ENAP, 2009. 342 p. ISBN 978-85-256-0062-2.

RÁDI, 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: 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: July 24, 2024.

REZENDE, R. M. de. A Insustentável Incerteza no Dever-Ser: reserva de iniciativa de leis, jurisprudência oscilante e a criação de fundos orçamentários . Brasília: Núcleo de Estudos e Pesquisas/ CONLEG/Senado, April/2017 (Discussion Paper No. 231. Available at: http://www.senado.leg.br/estudos. Accessed: Oct. 3, 2024.

ROQUETE, Felipe Leitão Valadares. Inteligência artificial, valores e incerteza: um problema insolúvel para a regulação? . Revista Internet & Sociedade, 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-insoluvel-para-a-regulacao.pdf. Accessed: Oct. 1, 2024.

SCHOLZE, Simone Henriqueta Cossetin; VIEIRA, Vania Lucia Ribeiro; AGUIAR, Alexandre Kehrig Veronese. Estudo sobre modelo regulatório pró-inovação . 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: Oct. 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: July 31, 2024.

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

WEBER, Rolf. Artificial Intelligence: A Theoretical Analysis of Regulatory Models. In : BELLI, Luca; GASPAR, Walter B. (Eds.). The Quest for AI Sovereignty, Transparency and Accountability: Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition . Rio de Janeiro: FGV Direito 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: July 31, 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

2

Artificial Intelligence and Personal Data Protection: reflections on the appropriate legal basis for training through web scraping

MATHEUS MANTUANI

Contents: Introduction. 1. Scraping Online Information in the Age of Big Data. 2. Reconciling Data Protection with Web Scraping. 3. In Search of the Legal Ground Applicable to AI Training. Final Considerations. References.

Introduction

In 1956, ten scientists met at Dartmouth College in New Hampshire, United States, to conduct a study on artificial intelligence ("AI"). It was based on the hypothesis that aspects of learning and other features of the human mind could, in principle, be described precisely enough for a machine to simulate them.[2]

Almost seventy years after this research field began, AI systems[3] can be seen to have developed historically in accordance with this ideal of using information probabilistically to reach increasingly complex results.[4] [5], This is because computing took as its premise that these systems were machines that manipulated numbers, so that everything could be encoded mathematically[6] through algorithms—operations that would provide a path for machines to process data and automate decisions.[7]

1. Lawyer. Postgraduate student in Digital Law at UERJ. Holds a law degree from UERJ. He has worked in technology and intellectual property at Rennó Penteado Sampaio Advogados since 2021. He served as Technical Editor and Coordinator of the Revista da Faculdade de Direito da UERJ. He interned at the Tribunal de Justiça do Estado do Rio de Janeiro and the Defensoria Pública do Estado do Rio de Janeiro. He was a director of the Centro Acadêmico Luiz Carpenter and a student representative on the Departmental Council, the Department of State Law, and the Department of Legal Theory and Foundations at UERJ Law School. He worked as a researcher and scholarship-supported teaching assistant at UERJ. He has authored articles published in academic journals and book chapters.

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

3. The precise concept of an AI system remains contested, but this research adopts the definition in the Artificial Intelligence Regulation recently approved in the European Union: "a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers from the input it receives how to generate outputs 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 Harmonised Rules on Artificial Intelligence. European Union: European Parliament, 2024, Article 3, paragraph 1.

4. BOSTROM, Nick. Superinteligência: caminhos, perigos e estratégias para um novo mundo. Translation: Aurélio Monteiro, Clemente Penna, Fabiana Monteiro, and Patrícia Geremias. Rio de Janeiro: Darkside, 2018.

5. BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol. Revista Direito e Práxis. Rio de Janeiro, 2024. Forthcoming.

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

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

Among the types of information that could be used to train and develop AI systems, personal data[8] available on the Internet[9] have attracted particular attention in a Big Data context. The term describes the "fuel" that makes machines work,[10] the raw material needed for systems to process information.[11] As Gustavo Tepedino emphasizes, "every day, a vast amount of data is extracted on an incalculable scale by economic actors,"[12] a situation that allows machines to become more "intelligent"—in the sense that they learn and improve their systems based on the personal data collected.[13]

One technique commonly used in these contexts is data scraping—automated extraction intended to collect large amounts of information and organize them into a database[14] for subsequent analysis and use.[15] However, scraping information from the Internet (web scraping) has been criticized from a personal data protection perspective,[16] since specific legislation in this area tends to restrict the collection and subsequent processing[17]

8. Under Article 5, I, of the General Personal Data Protection Law (Federal Law No. 13.709/2018), personal data may be defined as information relating to an identified or identifiable natural person. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Congresso Nacional, 2018.

9. Article 5, I, of the Brazilian Internet Civil Rights Framework ("MCI") defines the Internet as the system consisting of the set of logical protocols, structured on a worldwide scale for public and unrestricted use, intended to enable data communication between terminals through different networks. Idem. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Congresso Nacional, 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 work. Just as oil powered machines and factories in the Industrial Age, Big Data powers the relevant machines 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. United States, California, v. 51, no. 615, pp. 1.149-1.210, Sept., 2017, p. 1.154.

11. ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder. Translation: George Schlesinger. São Paulo: Intrínseca, 2019.

12. TEPEDINO, Gustavo. As tecnologias e a renovação do Direito Civil. 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. Under Article 5, IV, of the General Personal Data Protection Law, a database is a structured set of personal data established in one or more locations, in electronic or physical form. BRASIL. Lei n.º 13.709, de 14 de agosto de 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. United States, Washington, DC., Aug., 2023.

16. Recently, the Brazilian National Data Protection Authority ("ANPD") ordered the precautionary suspension of personal data processing to train the AI of Meta Platforms, Inc., considering, on a preliminary assessment of plausibility, that the company's "broad, general, and indiscriminate collection of all information made available and shared by users on its platforms" was unlawful. BRASIL. Voto n.º 11/2024/DIR-MW/CD. Brasília: Autoridade Nacional de Proteção de Dados, 2024, p. 11.

17. Under Brazilian law, specifically Article 5, X, of the General Personal Data Protection Law, the technical term processing encompasses every operation performed on personal data, including collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of information, modification, communication, transfer, dissemination, or extraction. Idem. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum.

of those data available online,[18] as can be seen in activities aimed at training AI systems.

Accordingly, the central aim of this research is to identify the extent to which Brazil's General Personal Data Protection Law (Federal Law No. 13.709/2018, "LGPD") limits web scraping for AI system training, given the need to ground the collection of online information in one of the situations provided for by law—the so-called legal bases. Through bibliographic research and direct review of specialist literature, the article's chapters present the rise of Internet scraping in the Big Data context, its clash with personal data protection law, and the challenges of identifying a legal ground that permits AI training through online scraping. The final considerations examine the substantial role of Brazil's National Data Protection Authority ("ANPD"),[19] as the interpreter of the LGPD, in balancing the protection of data subjects' fundamental interests and rights with support for the country's technological development, while giving equal consideration to the principle of freedom for Internet-based business models.

1. Scraping Online Information in the Age of Big Data

Web scraping commonly facilitates AI-based analytical processes through code[20] and key steps that include, for example, inserting information and the URL ("Uniform Resource Locator")—the term for the "specific indication" of an Internet page[21]—into the scraping script, so that the data and content requested by the programmer can be extracted, generally through spreadsheets or text files.[22]

This type of data mining is a prerequisite for the business model of various technology companies. Collecting information available online now provides the structure needed

18. One example of a restriction on web scraping is Article 7, §7, of the General Personal Data Protection Law. Under this provision, subsequent processing of personal data that are public or have been made manifestly public by the data subject may be carried out for new purposes only if the legitimate and specific purposes of the new processing and the preservation of the data subject's rights are observed, along with the foundations and principles set out in that Law. Ibid.

19. Under Article 5, XIX, of the LGPD, ANPD is the public administration body responsible for upholding, implementing, and monitoring compliance with the Law throughout the national territory. Ibid.

20. The Python programming language is one example of a tool that facilitates 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. *Marco Civil da Internet: construção e aplicação*. Juiz de Fora: Editar, 2016, p. 125.

22. TALIAFERRO, Jocelyn; HEDADJI, Fatima; DULING, Emma. Web Scraping as a Data Collection Strategy: the perils and pitfalls. Social Sciences & Humanities Open. Netherlands, Amsertdã. Forthcoming.

to create and add value through scraping: the practice has been used, for example, to monitor competitors' prices and to integrate and compare product prices, contributing to litigation in this area and challenges to these operations.[23] There are even reports of Internet data scraping being used for spam, cyber scams, fraud, denial-of-service attacks, sales of facial images to public security agencies, and manipulation of elections.[24]

At the same time, large-scale scraping of Internet information has also become essential to training certain AI models, such as generative artificial intelligence[25] or general-purpose systems.[26] This involves not only web scraping of personal data, but also the content of books,[27] news, and journalistic articles—a situation that raises additional discussions and barriers concerning copyright and related rights.[28] Scraping therefore becomes a "convenient," albeit criticized, method of obtaining raw material to develop AI systems.[29]

Creating intellectual property barriers to training these models can pose a significant challenge for system developers.[30] After all, the business model that has prevailed in web scraping involves feeding AI substantial amounts of information, facilitated by recent technological advances, so that models establish and form their decision patterns based on

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. United States, Kansas, v. 70, no. 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. United States, Michigan, v. 120, no. 5, pp. 913-945, Mar., 2022.

25. Article 4, IV, of the latest version of Brazilian Bill No. 2.338 of 2023 defines generative AI as an AI model specifically intended to generate or significantly modify, with varying degrees of autonomy, text, images, audio, video, or software code. BRASIL. Projeto de Lei n.º 2.338, de 2023. Dispõe sobre o desenvolvimento, fomento, uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília: Congresso Nacional, 2024.

26. The European Artificial Intelligence Regulation defines general-purpose systems as AI models, including those trained on large amounts of data using self-supervision at scale, that display significant generality and can competently perform a wide range of distinct tasks, regardless of how they are placed on the market, and can be integrated into a variety of systems or applications, except models used as prototypes before being placed on the market. EU. Artificial Intelligence Act, locus citatum, Article 3, paragraph 63.

27. O GLOBO. Escritores Processam OpenAI por Uso de Obras para Treinar ChatGPT sem Autorização. O Globo, Rio de Janeiro, July 20, 2023.

28. GRYNBAUM, Michael; MAC, Ryan. The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work. The New York Times. United States, New York, Dec. 27, 2023.

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

30. DELACROIX, Sylvie. Sustainable Data Rivers? Critical AI. United States, North Carolina, 2024. Forthcoming.

the data accessed, which is why it is said that “any algorithm is only as good as the data on which it is based.”[31]

Beyond copyright concerns, however, AI systems are often trained using personal data collected on a large scale from the Internet.[32] This opens a complementary debate and analysis, with specific restrictions on scraping in Brazil, since the LGPD guarantees every natural person control over their personal data and the fundamental rights to freedom, intimacy, and privacy.[33]

2. Reconciling Data Protection with Web Scraping

Personal data protection has been described for years as a fundamental right,[34] even before its express inclusion in the Constitution.[35] This definition sought a balance with other related rights—such as privacy, information, and transparency—and an approach that would simultaneously favor the inclusion of personal data in the market without treating that information merely as legal assets owned by data subjects.[36]–[37] Personal data can certainly be converted into valuable information for economic activities, so it would be reasonable to view the advent of the LGPD as strengthening informational self-

31. DONEDA, Danilo et alia. Considerações Iniciais sobre Inteligência Artificial, Ética e Autonomia Pessoal. Pensar. Fortaleza, v. 23, no. 4, pp. 1-17, Oct./Dec., 2018, p. 5.

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

33. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum, Article 17. For a critical analysis of Article 17 of the LGPD, see FRAZÃO, Ana. Direitos Básicos dos Titulares de Dados Pessoais. Revista do Advogado, v. 39, no. 144, pp. 33-46, Nov., 2019.

34. “The qualifier fundamental indicates that these are legal situations without which human beings cannot fulfill themselves, live together, and sometimes even survive.” SILVA, José Afonso da. Curso de Direito Constitucional Positivo. São Paulo: Malheiros, 2005, p. 178.

35. BRASIL. Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília: Congresso Nacional, 2022.

36. A data subject is the natural person to whom the personal data relate, under Article 5, V, of the LGPD. Idem. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum. Regarding the term adopted by the legislation, it is important to emphasize that “the use of the term ‘titular’ [data subject], although criticized by some legal scholars (who see the reference to titularity as invoking a proprietary perspective that is wholly inappropriate in matters directly concerning the human person), still seems appropriate, given the need to identify clearly the persons to whom the law refers.” SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Tutela da Pessoa Humana na Lei Geral de Proteção de Dados Pessoais: entre a atribuição de direitos e a enunciação de remédios. Pensar. Fortaleza, v. 24, no. 3, pp. 1-22, July/Sept., 2019, p. 8.

37. DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais: elementos da formação da Lei Geral de Proteção de Dados*. São Paulo: Thomson Reuters, 2020.

determination[38] and as a counterweight to the "retail trade"[39] in data self-regulated by the processing agents themselves.[40]

Brazilian personal data protection law thus establishes a proactive environment,[41] requiring controllers[42] to "exercise greater care in carrying out their activities."[43] Internet business models involving personal data processing and AI must therefore be reconciled with the LGPD's legal provisions[44] through a creative approach that also includes the regulatory State's guarantee of freedom of enterprise for economic activities conducted online.[45]–[46] This is no trivial task, and Carlos Affonso Souza describes one of the many difficulties in balancing data protection with AI system development:

> The LGPD states that all data subjects have the right to request the rectification and deletion of their personal data held by a company. [[47]] But what happens when those personal data have already been used to train a model underpinning a generative AI system? Once the model has been trained, the company may delete the personal data stored in its systems, but the outcome of that training may appear in the way the model is used in a wide variety of applications. To date, there are no viable ways to untrain a model without incurring disproportionate costs, energy consumption, and labor.[48]

38. Informational self-determination may be described as a "right to maintain control over one's own information." RODOTÀ, Stefano. A Vida na Sociedade de Vigilância: a privacidade hoje. Translation: Danilo Doneda and Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 92.

39. BIONI, Bruno. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 48.

40. FRAZÃO, Ana. *Fundamentos da Proteção de Dados Pessoais – noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2023, pp. 21-50.

41. MORAES, Maria Celina Bodin de. LGPD: um novo regime de responsabilização civil dito proativo. Civilistica.com. Rio de Janeiro, v. 8, no. 3, pp. 1-6, Dec., 2019.

42. Under Article 5, VI, of the LGPD, a controller is the natural or legal person, governed by public or private law, responsible for decisions concerning personal data processing. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum.

43. MONTEIRO FILHO, Carlos Edison do Rêgo. Tutela dos Dados Pessoais e sua Efetividade no Ordenamento Jurídico Brasileiro: direito de acesso, reparação e prevenção de danos. Revista de Direito da Responsabilidade. Portugal, Coimbra, v. 3, pp. 298-315, Mar., 2021, p. 314.

44. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. *A Utilização Econômica de Rastreadores e Identificadores On-Line de Dados Pessoais*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2023, pp. 585-604.

45. The regulation of Internet use in Brazil notably balances principles such as personal data protection and freedom for business models promoted on the Internet. BRASIL. Lei n.º 12.965, de 23 de abril de 2014, locus citatum, Article 3, III and VIII.

46. Some legal scholars state, for example, that "there can be no presumption that a particular way or model of exploiting an area of economic activity on the Internet is prohibited." SOUZA, Carlos Affonso; LEMOS, Ronaldo. Marco Civil da Internet: construção e aplicação, locus citatum, p. 48.

47. Article 18, III and IV, of the LGPD establishes data subjects' rights to request the correction of incomplete, inaccurate, or outdated data, as well as the anonymization, blocking, or deletion of unnecessary or excessive data or data processed in breach of the legislation. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum.

48. SOUZA, Carlos Affonso. Meta x ANPD: separar espaços da IA e dos dados pessoais não será nada fácil. Universo Online, São Paulo, July 04, 2024.

In addition, one of the principles established in the LGPD that directly affects AI system training is transparency:[49] the guarantee of clear, accurate, and readily accessible information about the processing performed.[50] Accordingly, despite the economic importance of automated personal data use,[51] controllers cannot simply fail to provide data subjects with information about how these activities are carried out.[52]

However, the complexity of the associations and correlations made while feeding AI—which may even become unexpected[53]—creates another challenge: how to explain activities that are initially unknown or poorly understood by the controllers themselves.[54]–[55] This situation creates risks of further potential violations of the principles of purpose[56] and adequacy.[57] Consequently, the criticized mystery[58] surrounding these operations has opened the way for debates about algorithmic audits intended to uncover mistaken or inaccurate decisions, unlawful or abusive discrimination, and harm

49. Transparency is also enshrined in European legislation. Spain's data protection authority ("AEPD") advises that it should enable data subjects to understand the impact associated with AI solutions, requiring controllers to provide information about systems' efficiency, resources, and limitations. This also includes specifically informing data subjects whether using their data for AI training will enable the resulting models to reidentify them later. ESPANHA. Adecuación al RGPD de Tratamientos que Incorporan Inteligencia Artificial – una introducción. Spain, Madrid: Agencia Española de Protección de Datos, 2020.

50. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum, Article 6, VI.

51. It should be emphasized that "processing information and data through algorithms may provide a way to simplify economic decisions, increase efficiency, and personalize production, as well as broaden opportunities to monetize digital services through personalized content and digital marketing." DONEDA, Danilo et alia. Considerações Iniciais sobre Inteligência Artificial, Ética e Autonomia Pessoal, locus citatum, p. 4.

52. After all, without such transparency, data subjects could not exercise their rights under the LGPD against the controller, since they would not even know that their personal data were being processed. Some scholars, however, believe that relying on transparency and a model of informational self-determination in AI would be insufficient to contain harms arising from 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. United States, Massachusetts, v. 104, no. 4, pp. 1.021-1.042, May, 2024.

53. SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. *O Direito à Explicação entre a Experiência e a sua Positivação na LGPD*. IN: MENDES, Laura Schertel *et alii* (Coords.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, pp. 243-270.

54. The LGPD requires, for example, that the processing agent provide information about the specific purpose of the activity involving personal data. If consent is the applicable legal basis, it may also be withdrawn if the data subject disagrees with the new purpose. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum, Article 9, I and § 2.

55. "This complexity further highlights the limitations of current privacy rights in addressing broader implications related to data use and algorithm-based decision-making. Even experts struggle to understand why algorithms produce certain results." [Our translation]. SOLOVE, Daniel. Artificial Intelligence and Privacy. Florida Law Review. United States, Florida, v. 77, no. 1, Jan., 2025. Forthcoming.

56. "[P]rocessing for legitimate, specific, and explicit purposes communicated to the data subject, with no possibility of subsequent processing incompatible with those purposes." BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, opere citato, Article 6, I.

57. "[C]compatibility of processing with the purposes communicated to the data subject, in accordance with the processing context." Ibidem, Article 6, II.

58. PASQUALE, Frank. The Black Box Sociey: the secret algorithms that control money and information. United States, Massachusetts: Harvard University Press, 2015.

to the data subject.[59]–[60] On the other hand, defining processing purposes in advance has been described as an “old idea” that could oppose AI systems’ potential to identify new purposes, including ones beneficial to data subjects.[61]

Scraping techniques used by developers to collect information on the Internet are another component in the discussion of the boundary between AI and personal data protection. For some, the fact that data subjects’ information is publicly available online should not constitute a “loophole” allowing its collection, shared use, and other processing activities without due transparency and for purely commercial purposes.[62] Rather, the absence of specific, concise, understandable, and readily accessible information[63] about scraping prevents data subjects from exercising their right to object to the operation.[64]

Accordingly, the European Data Protection Board (“EDPB”) indicates that information scraping poses particular risks to natural persons’ fundamental rights and freedoms,[65] and the European Data Protection Supervisor (“EDPS”) argues that web scraping for AI training may fail to comply with personal data protection principles.[66]

However, potential incompatibility does not mean that scraping should be subject to a “categorical ban” that hinders AI training,

59. MITTELSTADT, Brent et alia. The Ethics of Algorithms: mapping the debate. Big Data & Society. United States, California, v. 3, no. 2, July/Dec., 2016.

60. The LGPD also provides that ANPD may conduct an audit to verify discriminatory aspects of automated personal data processing, while observing trade and industrial secrets, if the controller fails—when requested—to provide clear and adequate information about the criteria and procedures used for a particular automated decision. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum, Article 20, § 2. For a detailed understanding of the meaning of automated personal data processing, see VERONESE, Alexandre. Os Direitos de Explicação e de Oposição diante das Decisões Totalmente Automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2023, pp. 377-408.

61. HILDEBRANDT, Mireille. Esclavos de los macrodatos. ¿O no? Revista de Internet, Derecho y Política. 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. Guidance from the French data protection authority (“CNIL”). FRANÇA. 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 it fined Bisnode for failing to inform data subjects directly about its scraping practices. Arguing that individual notification would involve “disproportionate effort,” the processing agent had merely mentioned the operation in its privacy policy—which the regulator considered insufficient in that case. POLÔNIA. 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 Orientations for ensuring data protection compliance when using Generative AI systems. European Union: European Data Protection Supervisor, 2024.

although data protection's legal requirements must be applied proportionately here so that they, too, do not lose their meaning if no reconciliation between the two fields is envisaged.[67] Thus, while preventing scraping would impose considerable costs on developers, since basic search and information retrieval functions "depend" on web scraping,[68] the fundamental right to data protection must likewise be taken seriously and cannot be regarded merely as an obstacle to processing agents' economic activities.

In conclusion, data protection laws seem, ultimately, to conflict to some extent with AI operations in a Big Data framework.[69] This risks inhibiting innovation and new technological benefits for society[70] as nation-states intensify strategic competition and relax interventionism to favor AI development.[71]

Brazil, however, has chosen to mirror almost entirely Europe's more protective regulatory framework,[72–73] seeking to maintain the LGPD's full applicability to AI training through web scraping.[74] It should also be emphasized that Brazilian personal data protection law authorizes subsequent processing of personal data that are public or have been made manifestly public by the data subject only when legitimate and specific purposes for the new activity and the preservation of the data subject's rights are guaranteed, together with the foundations and principles established in the LGPD.[75]

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

68. "Banning scraping would entail a major financial and social cost, since many basic Internet and AI functions related to search and information 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-related practices." [Our translation]. Ibidem, p. 52.

69. ZARSKY, Tal. Incompatible: the GDPR in the age of Big Data. Seton Hall Law Review. United States, New Jersey, v. 47, no. 4, pp. 995-1.020, Aug., 2017.

70. Carlos Affonso Souza, Christian Perrone, and Eduardo Magrani argue that "prohibiting mechanisms that automate decisions, or even artificial intelligence, machine learning, and the like, would be tantamount to condemning humans to the use of horses after the invention of the internal combustion engine." SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. O Direito à Explicação entre a Experiência e a sua Positivação na LGPD, locus citatum, p. 246.

71. For a mapping of different AI regulatory proposals beyond European legislation, see ITS. Como Regular a Inteligência Artificial? Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2024.

72. EU. Artificial Intelligence Act, locus citatum.

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

74. Under Article 30, III, of Brazilian Bill No. 2.338 of 2023, developers of general-purpose AI systems must, before making them commercially available, process and incorporate only datasets collected and processed in compliance with legal requirements and subject to adequate data governance, particularly in accordance with the LGPD. In addition, Article 61, § 3, of the Bill determines that text and data mining involving personal data is subject to the LGPD's provisions. BRASIL. Projeto de Lei n.º 2.338, de 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 that information. EU. Artificial Intelligence Act, locus citatum, recital 10 and Article 2, paragraph 7.

75. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum, Article 7, § 7.

The path the country appears to be taking certainly prioritizes the fundamental right to personal data protection in developing systems that use such information as their raw material—although there is still no consensus on the appropriate regulatory choice to provide safeguards "against the problems that AI may bring."[76] In any event, the current situation points toward a legislative foundation centered on the human person,[77] while technology companies base certain economic practices on scraping online data, making the continuation of scraping a true "conundrum."[78]

To better delineate the scope and challenges of making Internet scraping viable, the next chapter of this research investigates how web scraping might be grounded in one of the legal bases established in the LGPD. Processing agents must select one of the bases contained in the legislation as a condition for starting any personal data operation,[79] including collection for AI system training.

3. In Search of the Legal Ground Applicable to AI Training

Selecting an authorizing legal basis is one of the "requirements" established in the LGPD to ensure the lawfulness of personal data processing.[80] In practice, controllers must assess the specific purpose and context for which they seek to use the information, so as to reconcile them with one of the legal provisions described in the legislation.[81] In Brazil, notably, there is no hierarchy among the bases, "since they are all listed horizontally" in the LGPD.[82]

However, a distinction is drawn between the bases authorizing the processing of sensitive personal data[83] (Article 11, LGPD) and non-sensitive personal data (Article

76. LEMOS, Ronaldo. O que o Brasil Quer da Inteligência Artificial? Folha de São Paulo, São Paulo, Apr. 07, 2024.

77. BRASIL. Projeto de Lei n.º 2.338, de 2023, locus citatum, Article 2, I.

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

79. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: estudo sobre as bases legais. Civilistica.com. Rio de Janeiro, v. 9, no. 1, pp. 1-38, May, 2020.

80. SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius. Considerações Iniciais sobre os Interesses Legítimos do Controlador na Lei Geral de Proteção de Dados Pessoais. Direito Público. Brasília, v. 16, no. 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. *Proteção de Dados Pessoais: a função e os limites do consentimento, locus citatum,* p. 188.

83. Under Article 5, II, of the LGPD, sensitive personal data are personal data concerning racial or ethnic origin, religious belief, political opinion, membership of a trade union or religious, philosophical, or political organization, data concerning health or sex life, and genetic or biometric data, when linked to a natural person. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum.

7, LGPD), since the former constitute a special category protected by the Law, which establishes stricter mechanisms for authorizing controllers' activities involving that information in light of its potential misuse for unlawful or abusive discrimination and other violations of human rights.[84]

One initial possible view is the argument that collecting personal data through web scraping for AI system training does not have the purpose and aim[85] of processing sensitive information or causing harm to data subjects, but merely of ensuring, within the logic of Big Data, the inputs needed to feed the systems. Along these lines, the EDPB states that the mere fact that a processing agent carries out a large-scale activity does not automatically mean that there is a purpose of inferring[86] sensitive data if such information is also collected during the operation.[87] In this same context of Internet scraping, it can be argued that a detailed analysis of every item of information processed to detect sensitive data in the scraped dataset would hardly be feasible.[88]

On the other hand, it is equally possible to argue that scraping to train AI systems must rely on a more protective basis if sensitive personal data are collected during scraping, regardless of the activity's purpose and potential harm.[89] The French data protection authority ("CNIL") emphasizes, however, that if the controller implements measures to automatically exclude the collection of

84. TEFFÉ, Chiara Spadaccini de. Dados Pessoais Sensíveis: qualificação, tratamento e boas práticas. Indaiatuba: Foco, 2022. The same author also argues that: "[a]s artificial intelligence has frequently been used for decision-making, people's lives become increasingly vulnerable to unlawful or abusive discriminatory processing, for example in situations involving assessments of the likelihood of committing crimes, healthcare, credit granting, and participation in employment selection processes." Idem. A Categoria Especial de Dados Sensíveis: fundamentos e contornos. In: SCHREIBER, Anderson; MONTEIRO FILHO, Carlos Edison do Rêgo; OLIVA; Milena Donato (Orgs.). Problemas de Direito Civil. Rio de Janeiro: Forense, 2021, pp. 97-123, p. 105.

85. For an overview of potential AI uses intended to collect or infer 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 special protection for sensitive data applies to any personal data processing that reveals sensitive personal data and may harm the data subject. BRASIL. Lei n.º 13.709, de 14 de agosto de 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 to describe closed-circuit television ("CCTV") capturing the image of a person wearing religious clothing: since the cameras are used to ensure the premises' security, without collecting biometric data or identifying people's religious beliefs, it would make no sense to require processing to rely on a more protective basis associated with 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 bears repeating, identifying a specific, more restrictive legal basis before proceeding with processing would be essential. 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 involving sensitive data intended to "ensure bias detection and correction" in relation to AI systems, subject to additional requirements to guarantee data subjects' protection. EU. Artificial Intelligence Act, locus citatum, Article 10, paragraph 5.

sensitive data through scraping, incidental and residual operations involving that information, unsupported by a more restrictive basis, would cease to be unlawful in these cases.[90]

In Brazil, among the main bases in the LGPD related to processing non-sensitive data for commercial AI system training through web scraping, only consent and legitimate interest stand out.[91] More restrictively, only specific and prominent consent could, in principle, provide a basis for online scraping of sensitive personal data for commercial AI training.[92] This is because the specific purpose of improving systems does not appear to be equivalent to performing a possible contract between the scraper and the data subject, nor to a credit analysis that a bureau might conduct for credit protection itself—other bases that the processing agent could put forward to support scraping, but which would require greater argumentative effort because they relate to specific and uncommon cases.[93]

At the same time, the legal basis of consent itself—which consists of the data subject's freely given, informed, and unambiguous expression of agreement to the processing of their personal data for a specific purpose[94]—faces challenges in the context under analysis. As noted above, data subjects may not understand the purposes of certain "opaque" operations carried out for AI training,[95]–[96] nor be able to withdraw their authorization and request the deletion of data that have already fed

90. FRANCE. IA: assurer que le traitement est licite – définir une base légale. France, Paris: Commission Nationale de l'Informatique et des Libertés, 2024.

91. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum, Article 7, I and IX.

92. Ibidem, Article 11, I.

93. For an analysis of the legal bases of contract performance and the regular exercise of contractual rights, see PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. Compliance Digital e LGPD. São Paulo: Thomson Reuters, 2021. For a specific overview of credit protection and the LGPD, see OLIVA, Milena Donato; VIÉGAS, Franciso de Assis. Tratamento de Dados para a Concessão de Crédito. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2023, pp. 547-584.

94. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum, Article 5, XII. For a detailed analysis of the legal basis of consent, see TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O Consentimento na Circulação de Dados Pessoais. Revista Brasileira de Direito Civil. Belo Horizonte, v. 25, no. 3, pp. 83-116, Nov., 2020; and BIONI, Bruno. Proteção de Dados Pessoais: a função e os limites do consentimento, 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. United States, New York, pp. 1-90, June, 2019, p. 70; and UNITED KINGDOM. Guidance on AI and Data Protection, locus citatum.

96. This concern is even more relevant when discussing consent to process sensitive data, since consent must be specific in such cases. According to the literature, "[s]pecific should be understood as consent expressed in relation to concrete purposes clearly determined by the controller before the data are processed; here too, and with greater emphasis, granularity requirements apply." TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: estudo sobre as bases legais, locus citatum, p. 34.

the systems,[97] undermining the requirements for freely given, informed, and unambiguous consent. Moreover, obtaining individual consent from every data subject seems unfeasible and would require disproportionately costly effort in the context of web scraping, which involves large-scale personal data collection.[98]

This would leave only the controller's legitimate interest as a legal basis. It does not apply to sensitive personal data processing and has been described, albeit critically, by the Dutch data protection authority ("AP") as the only appropriate basis for online scraping.[99] Legitimate interest is the "authorizing basis designed precisely to address situations in which seeking the data subject's consent could itself become an obstacle to the regular exploitation of personal data";[100] its proper use "enables and expands new business models and various commercial strategies."[101] However, this legal basis must be weighed case by case against the data subject's fundamental rights and freedoms[102] and remains subject to oversight by the National Authority, which has already presented a model test for controllers to balance processing interests against potential unwanted impacts, interpreted in accordance with the LGPD.[103] This means that processing agents' purely economic activities must serve human-centered purposes, prioritizing the human person and the protection of their personal data.[104]

In short, with regard to data processing for system training through web scraping, legitimate interest offers a flexible basis for the operation, insofar as it allows a balance between AI's commercial and social benefits and data subjects' rights and interests.[105] Nevertheless, controllers must actually adopt 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: separar espaços da IA e dos dados pessoais não será nada fácil, 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 alii. Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. ArXiv Working Paper no. 2401.07348. United States, New York, Mar., 2024.

99. NETHERLANDS. Handreiking Scraping door Particulieren en Private Organisaties. Netherlands, The Hague: Autoriteit Persoonsgegevens, 2024.

100. SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius. Considerações Iniciais sobre os Interesses Legítimos do Controlador na Lei Geral de Proteção de Dados Pessoais. Direito Público. Brasília, v. 16, no. 90, pp. 109-131, Dec., 2019, p. 110.

101. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Tratamento de Dados Pessoais na LGPD: estudo sobre as bases legais, locus citatum,* p. 19.

102. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum, Articles 7, IX, and 10.

103. BRASIL. Hipóteses Legais de Tratamento de Dados Pessoais – legítimo interesse. Brasília: Autoridade Nacional de Proteção de Dados, 2024.

104. BUCAR, Daniel; VIOLA, Mario. Tratamento de Dados Pessoais por "Legítimo Interesse do Controlador": primeiras questões e apontamentos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. 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.

for robust security and risk mitigation[106]—such as pseudonymization, criteria for collecting only information necessary for training,[107] and mechanisms for objecting to the activity ("opt-out")[108]—

as well as provide transparent and continually updated information about processing.[109] Without this, that legal basis would likewise be inappropriate and inconsistent with the LGPD, ANPD guidance,[110] and best practices in privacy and personal data protection.

Final Considerations

This article sought to identify the most appropriate legal basis for training AI systems with personal data through web scraping. Starting with an analysis of information scraping in the Big Data era, it highlighted how the LGPD established a markedly human-centered framework, under which controllers' economic activities came to be considered in relation to the various requirements and obligations in the governing legislation. In this complex situation, ANPD is responsible for making final determinations on the interpretation of the LGPD while balancing online scraping practices with personal data protection and positioning itself as the competent authority to coordinate the National Artificial Intelligence Regulation and Governance System. This is challenging work that will require particular attention from the Authority, which already includes web scraping and AI in its map of priority topics and regulatory agenda.

Finally, selecting a suitable legal basis for a processing activity does not, by itself, ensure that the operation complies with the LGPD. Controllers must therefore continue implementing good practices to safeguard data subjects' rights and the principles

106. ESPANHA. *Adecuación al RGPD de Tratamientos que Incorporan Inteligencia Artificial – una introducción, locus citatum.*

107. FRANCE. IA: assurer que le traitement est licite – définir une base légale, locus citatum. Pseudonymization is processing through which data can no longer be associated, directly or indirectly, with an individual except through additional information kept separately by the controller in a controlled and secure environment. Moreover, the necessity principle (Article 6, III, LGPD) deserves particular emphasis in processing based on legitimate interest. BRASIL. Lei n.º 13.709, de 14 de agosto de 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: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. Italy, Rome: Garante per la Protezione dei Dati Personali, 2023. The LGPD also requires controllers to adopt measures to ensure transparency in data processing based on legitimate interest. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum, Article 10, § 2.

110. The Authority also recommends demonstrating data subjects' legitimate expectations regarding processing, providing mechanisms for exercising rights, observing the necessity principle, conducting a three-stage balancing test, and paying greater attention to processing children's and adolescents' data. BRASIL. Hipóteses Legais de Tratamento de Dados Pessoais – legítimo interesse, locus citatum.

and foundations established in the Law. Only through cooperation between regulated actors and ANPD will it be possible to ensure freedom for business models promoted on the Internet, in a creative balance with privacy and personal data protection in Brazil, moving toward the development, promotion, and 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. United States, Washington, DC., Aug., 2023.

AMARIKWA, Melany. Internet Openness at Risk: generative AI's impact on data scraping. Richmond Journal of Law & Technology. United States, 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. United States, California, v. 51, no. 615, pp. 1,149-1.210, Sept., 2017.

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

BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol. Revista Direito e Práxis. Rio de Janeiro, 2024. Forthcoming.

BIONI, Bruno. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

BOSTROM, Nick. Superinteligência: caminhos, perigos e estratégias para um novo mundo. Translation: Aurélio Monteiro, Clemente Penna, Fabiana Monteiro, and Patrícia Geremias. Rio de Janeiro: Darkside, 2018.

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

BRASIL. Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília: Congresso Nacional, 2022.

BRASIL. Hipóteses Legais de Tratamento de Dados Pessoais – legítimo interesse. Brasília: Autoridade Nacional de Proteção de Dados, 2024.

BRASIL. *Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Brasília: Congresso Nacional, 2014.

BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília: Congresso Nacional, 2018.

BRASIL. Projeto de Lei n.º 2.338, de 2023. Dispõe sobre o desenvolvimento, fomento, uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília: Congresso Nacional, 2024.

BRASIL. *Voto n.º 11/2024/DIR-MW/CD*. Brasília: Autoridade Nacional de Proteção de Dados, 2024.

BUCAR, Daniel; VIOLA, Mario. Tratamento de Dados Pessoais por "Legítimo Interesse do Controlador": primeiras questões e apontamentos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2023, pp. 453-472.

DELACROIX, Sylvie. Sustainable Data Rivers? Critical AI. United States, North Carolina, 2024. Forthcoming.

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters, 2020.

DONEDA, Danilo; MENDES, Laura Schertel; SOUZA, Carlos Affonso Pereira de; ANDRADE, Norberto. Considerações Iniciais sobre Inteligência Artificial, Ética e Autonomia Pessoal. Pensar. Fortaleza, v. 23, no. 4, pp. 1-17, Oct./Dec., 2018.

ESPANHA. Adecuación al RGPD de Tratamientos que Incorporan Inteligencia Artificial – una introducción. Spain, Madrid: Agencia Española de Protección de Datos, 2020.

FRANCE. IA: assurer que le traitement est licite – définir une base légale. 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.

FRAZÃO, Ana. Direitos Básicos dos Titulares de Dados Pessoais. Revista do Advogado, v. 39, no. 144, pp. 33-46, Nov., 2019.

FRAZÃO, Ana. Fundamentos da Proteção de Dados Pessoais – noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2023, pp. 21-50.

GOODYEAR, Michael. Circumscribing the Spider: Trademark Law and the edge of data scraping. Kansas Law Review. United States, Kansas, v. 70, no. 2, pp. 295-328, Dec., 2021.

GRYNBAUM, Michael; MAC, Ryan. The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work. The New York Times. United States, New York, Dec. 27, 2023.

HILDEBRANDT, Mireille. Esclavos de los macrodatos. ¿O no? Revista de Internet, Derecho y Política. Spain, Barcelona, v. 17, pp. 7-44, Nov., 2013.

NETHERLANDS. Handreiking Scraping door Particulieren en Private Organisaties. Netherlands, The Hague: Autoriteit Persoonsgegevens, 2024.

ITALY. ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. Italy, Rome: Garante per la Protezione dei Dati Personali, 2023.

ITS. *Como Regular a Inteligência Artificial?* Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2024.

LEMOS, Ronaldo. O que o Brasil Quer da Inteligência Artificial? Folha de São Paulo, São Paulo, Apr. 07, 2024.

MCCARTHY, John; MINSKY, Marvin; ROCHESTER, Nathaniel; SHANNON, Claude. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. United States, 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. United States, 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. United States, California, v. 3, no. 2, July/Dec., 2016.

MONTEIRO FILHO, Carlos Edison do Rêgo. Tutela dos Dados Pessoais e sua Efetividade no Ordenamento Jurídico Brasileiro: direito de acesso, reparação e prevenção de danos. Revista de Direito da Responsabilidade. Portugal, Coimbra, v. 3, pp. 298-315, Mar., 2021.

MORAES, Maria Celina Bodin de. LGPD: um novo regime de responsabilização civil dito proativo. Civilistica.com. Rio de Janeiro, v. 8, no. 3, pp. 1-6, Dec., 2019.

NEWELL, Allen. Intelectual Issues in the History of Artificial Intelligence. In: MACHLUP, Fritz; MANSFIELD, Una (Eds.). The Study of Information: interdisciplinary messages. United States, 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. United States, New York, Mar., 2024.

O GLOBO. Escritores Processam OpenAI por Uso de Obras para Treinar ChatGPT sem Autorização. O Globo, Rio de Janeiro, July 20, 2023.

OLIVA, Milena Donato; VIÉGAS, Franciso de Assis. Tratamento de Dados para a Concessão de Crédito. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Prote-

ção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2023, pp. 547-584.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. Compliance Digital e LGPD. São Paulo: Thomson Reuters, 2021.

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

PASQUALE, Frank. The Black Box Sociey: the secret algorithms that control money and information. United States, 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. A Vida na Sociedade de Vigilância: a privacidade hoje. Translation: Danilo Doneda and Luciana Doneda. Rio de Janeiro: Renovar, 2008.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. São Paulo: Malheiros, 2005.

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

SOLOVE, Daniel. Artificial Intelligence and Privacy. Florida Law Review. United States, Florida, v. 77, no. 1, Jan., 2025. Forthcoming.

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

SOLOVE, Daniel; HARTZOG, Woodrow. Kafka in the Age of AI and the Futility of Privacy as Control. Boston University Law Review. United States, Massachusetts, v. 104, no. 4, pp. 1.021-1.042, May, 2024.

SOUZA, Carlos Affonso. Meta x ANPD: separar espaços da IA e dos dados pessoais não será nada fácil. Universo Online, São Paulo, July 04, 2024.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. Juiz de Fora: Editar, 2016.

SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. *O Direito à Explicação entre a Experiência e a sua Positivação na LGPD*. IN: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo; RODRIGUES JR., Otavio; BIONI, Bruno (Coords.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, pp. 243-270.

SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius. Considerações Iniciais sobre os Interesses Legítimos do Controlador na Lei Geral de Proteção de Dados Pessoais. Direito Público. Brasília, v. 16, no. 90, pp. 109-131, Dec., 2019.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Tutela da Pessoa Humana na Lei Geral de Proteção de Dados Pessoais: entre a atribuição de direitos e a enunciação de remédios. Pensar. Fortaleza, v. 24, no. 3, pp. 1-22, July/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 perils and pitfalls. Social Sciences & Humanities Open. Netherlands, Amsertdã. Forthcoming.

TEFFÉ, Chiara Spadaccini de. A Categoria Especial de Dados Sensíveis: fundamentos e contornos. In: SCHREIBER, Anderson; MONTEIRO FILHO, Carlos Edison do Rêgo; OLIVA; Milena Donato (Orgs.). Problemas de Direito Civil. Rio de Janeiro: Forense, 2021, pp. 97-123.

TEFFÉ, Chiara Spadaccini de. *Dados Pessoais Sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Foco, 2022.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: estudo sobre as bases legais. Civilistica.com. Rio de Janeiro, v. 9, no. 1, pp. 1-38, May, 2020.

TEPEDINO, Gustavo. As tecnologias e a renovação do Direito Civil. OAB/RJ, Rio de Janeiro, June 12, 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O Consentimento na Circulação de Dados Pessoais. Revista Brasileira de Direito Civil. Belo Horizonte, v. 25, no. 3, pp. 83-116, Nov., 2020.

TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A Utilização Econômica de Rastreadores e Identificadores On-Line de Dados Pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2023, pp. 585-604.

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

EU. Generative AI and the EUDPR. First EDPS Orientations 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, Alexandre. Os Direitos de Explicação e de Oposição diante das Decisões Totalmente Automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2023, pp. 377-408.

ZARSKY, Tal. Incompatible: the GDPR in the age of Big Data. Seton Hall Law Review. United States, New Jersey, v. 47, no. 4, pp. 995-1.020, Aug., 2017.

ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder. Translation: George Schlesinger. São Paulo: Intrínseca, 2019.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

3

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

BARBARA GOMES D'ASCENÇAO

Contents: Introduction. 1. Data Capitalism and Inequalities. 2. Algorithmic Racism in Public Security and the Labor Market. 3. Data Colonialism and Culture; 4. Transparency, Algorithmic Ethics, and Public Policy. Final considerations. References.

Introduction

Artificial intelligence (AI) has become a constant and transformative presence across modern society, from virtual assistants to complex decision-making systems in critical areas such as healthcare, public security, and the labor market. Notable examples include AI for medical diagnosis and predictive surveillance systems used by police forces in various cities. Although AI offers numerous advantages, it also brings significant challenges, particularly regarding social justice and equity. One of the most pressing problems is algorithmic racism, whereby algorithms reflect and reinforce racial inequalities in society. As Noble[2] emphasizes, "algorithms have the power to perpetuate historical and structural biases under the appearance of technical neutrality."

Racism is a social construct that permeates various spheres of life, and technology, developed by social actors, is not immune to these influences. Despite its neutral appearance, technology can perpetuate dominant and hegemonic logics. The central question this article addresses is: how do algorithms used in different social spheres contribute to reinforcing structural racism? This question is crucial because, according to Silva,[3] "AI systems are not mere technical tools but reproductions of the values and prejudices of their societies of origin."

The study's relevance lies in the need for a critical, ethical, and political understanding of AI systems. The decisions these systems make directly affect millions of lives, particularly those of people belonging to minority groups. Understanding and mitigating algorithmic racism is crucial to promoting a fairer and more equitable society. As Zuboff[4]

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

2. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021. p. 34.

3. SILVA, Tarcízio da. *Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais*. São Paulo: Edições Sesc SP, 2022. p. 45.

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

argues, “surveillance capitalism deepens inequalities by monetizing personal data, frequently reinforcing existing prejudices.”

1. Data Capitalism and Inequalities

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

Personal data are collected across various digital platforms, including social networks, search engines, and online services. These data are used to create detailed user profiles, enabling companies and governments to make decisions based on personal information. The problem is that these data often carry historical and structural prejudices. For example, location data may reflect racial and socioeconomic segregation in cities, perpetuating existing inequalities.[7]

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

The data used to train AI systems frequently carry historical prejudices. When applied in areas such as public security, healthcare, and the labor market, these systems can perpetuate and even amplify racial inequalities. O’Neil[8] states that “algorithms are not impartial; they reflect their creators’ priorities and prejudices and the data that feed them.” For example, a study by Noble[9] revealed that Google searches for traditionally African American names returned advertisements related to criminal records more frequently than searches for

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. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021. p. 43.

8. O’NEIL, Cathy. *Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia*. Santo André: Editora Rua do Sabão, 2020. p. 56.

9. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021.

traditionally white names, demonstrating how historical prejudices are embedded in the data that feed these systems.

Moreover, using data for decision-making can lead to discriminatory practices. A study conducted by Pasquale[10] demonstrated that credit algorithms tend to deny loans to individuals from racial minorities at a disproportionate rate. Trained on historical credit data, these algorithms reflect past prejudices and discrimination, perpetuating these communities' financial exclusion. A lack of transparency about how data are collected, processed, and used also exacerbates the problem, making biases harder to identify and correct.

Surveillance capitalism, as described by Zuboff,[11] not only exploits personal data for profit but also helps construct a social system in which inequality is institutionalized through technology. This economic model prioritizes profit maximization over equity and justice, creating a vicious cycle in which marginalized people continue to be disadvantaged. A lack of regulation and opaque data collection and use practices make it difficult for individuals to understand and challenge algorithms' decisions.

To better understand how data capitalism perpetuates inequalities, it is important to analyze the intersection of technology, society, and the economy. The prevailing capitalist model uses technology not only as a tool for efficiency but also as a mechanism of social and economic control. The "datafication" of social practices turns aspects of everyday life into commodities that are then used to predict and influence consumption behavior, reinforcing patterns of discrimination and exclusion. Zuboff[12] argues that this model creates a new form of power in which those who control data can shape social reality in ways that perpetuate inequality.

Gomes's[13] critical analysis of data colonialism shows that data control and manipulation are modern forms of colonialism in which power and exploitation no longer operate through territorial control but through control of data. Gomes argues that "data colonialism perpetuates the exploitation and marginalization of already vulnerable populations by

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, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023. p. 25.

consolidating the power of major technology corporations at the same time." This critical perspective complements Zuboff's[14] analysis by highlighting how historical and colonial power structures are reproduced and reinforced in the digital environment.

Gomes[15] also emphasizes that data extraction practices often take place without individuals' explicit consent, reinforcing the power asymmetry between data collectors and data subjects. This results in a form of colonization in which data are extracted and used in ways that primarily benefit technology corporations and governments at the expense of the most vulnerable populations.

2. Algorithmic Racism in Public Security and the Labor Market

In Sergipe, during a match in the Sergipano Football Championship, a facial recognition system caused an innocent person to be detained because of a false positive, causing embarrassment and fear for the citizen who was wrongly detained.[16] This incident shows how technology can reinforce existing prejudices, becoming a tool of oppression rather than justice. Facial recognition systems, widely used by security forces, demonstrate how the uncritical application of AI can result in discriminatory practices that exacerbate the marginalization of vulnerable groups.

Public security systems frequently use algorithms that associate Blackness and poverty with criminality, resulting in increased incarceration rates and violence against minorities. According to Silva,[17] "algorithmic surveillance systems perpetuate the criminalization of Black bodies, reinforcing structural racism through automated practices." Developed on the basis of historical policing data, these algorithms often incorporate and amplify prejudices, 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, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023. p. 23.

16. G1. 'Medo, frustrado e constrangido', diz homem detido por engano em estádio após erro do sistema de reconhecimento facial. Fantástico, 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: Oct. 18, 2024.

17. SILVA, Tarcízio da. *Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais*. São Paulo: Edições Sesc SP, 2022. p. 102.

Studies show that facial recognition systems are more likely to make errors when identifying individuals of certain ethnicities. The study Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects compared 189 algorithms from 99 different developers and found that most algorithms showed variations in accuracy based on demographic factors, producing a higher false-positive rate for Asian and African American faces than for Caucasian faces—as much as 10 to 100 times higher, depending on the algorithm.[18] 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[19] emphasize that “facial recognition algorithms frequently fail to correctly identify darker-skinned people, exacerbating discriminatory surveillance practices.”

The application of algorithms in the labor market also reveals profound inequalities. Algorithms used by companies to select candidates often disadvantage racial minorities. Noble[20] observes that these algorithms may reflect programmers’ prejudices and the historical data used to train them. The University of Washington study Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination showed that AI systems used for résumé screening tend to reject African American-sounding names, even when all other qualifications are equal.[21] 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 in AI development teams can exacerbate these problems. AI developers frequently do not represent the diversity of the population their technologies will affect, which may lead to a feedback loop in which prejudices are inadvertently encoded in algorithms. Benjamin[22] argues that “including

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: Oct. 18, 2024.

19. BEZERRA, Arthur Coelho; COSTA, Camila Mattos da. Pele negra algoritmos brancos: informação e racismo nas redes sociotécnicas. Liinc em Revista, v. 18, no. 2, 2022. p. 89.

20. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora 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. Accessed: Oct. 18, 2024.

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

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

The interaction between algorithmic racism and public security and employment practices reveals how technologies, when not properly supervised and regulated, can reinforce unequal power structures. Technology, which should serve as a tool for justice and equity, often ends up perpetuating the very inequalities it promised to resolve. A lack of diversity and biases in data and development teams are crucial factors contributing to this perpetuation.

Gomes[23] offers an in-depth analysis of the implications of algorithmic racism in the context of cybercrime and public security. Gomes[24] highlights specific cases in which predictive surveillance systems have led to disproportionate police interventions in predominantly Black neighborhoods, exacerbating distrust and conflict between these communities and security forces.

Also discussed is how a lack of transparency and difficulty accessing the criteria used by surveillance algorithms create an environment in which abuses can occur without adequate oversight. This point is crucial to understanding how technology can be used for either good or ill, depending on how it is implemented and regulated.

3. Data Colonialism and Culture

The concept of data colonialism, as discussed by Zuboff,[25] refers to technology corporations and governments controlling and exploiting marginalized populations' data without those populations' consent or adequate benefit. This process perpetuates inequalities and further marginalizes already vulnerable groups, creating a new type of colonialism in the digital environment.

Couldry and Mejias[26] define data colonialism as "a new phase of capitalism in which data extraction is the principal form of capital

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

24. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023

25. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. 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.

accumulation." They argue that this practice reflects and amplifies global inequalities, with technology companies from developed countries extracting users' data in developing countries for their own economic benefit. This dynamic creates a relationship of dependence and exploitation in which developing countries' populations are reduced to mere data suppliers.

Moreover, Thatcher, O'Sullivan, and Mahmoudi[27] emphasize that data colonialism involves the "production of knowledge from extracted data, which are frequently used to control and govern populations in non-transparent ways." They argue that knowledge production from extracted data often ignores the social and cultural contexts from which those data are taken, resulting in policies and practices that perpetuate marginalization and exclusion.

A clear example of data colonialism 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 millions of Facebook users' data were used without consent to influence the 2016 US presidential election, highlights how data can be exploited for political and economic ends.[28] This case illustrates the implications of data colonialism, in which data extraction is used to manipulate democratic processes, reinforcing elites' power over the masses.

The cultural implications of data colonialism are profound. Gomes[29] discusses how data appropriation and exploitation can lead to a loss of cultural control and the erosion of communities' autonomy. The author emphasizes that "collecting and using data without adequate community involvement may distort and decontextualize cultural practices, contributing to the alienation and devaluation of those 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 millions of Facebook users' data. Cambridge Analytica used an application called thisisyourdigitallife, which collected personal data under the pretext of a personality test for academic purposes. However, these data were shared with Cambridge Analytica and used to create detailed psychological profiles intended to influence 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 sanctions 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, July 24, 2019. Available at: https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer. Accessed: Oct. 15, 2024.

29. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023. p. 23.

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

Furthermore, data colonialism significantly affects communities' self-determination. When reduced to sources of data, communities lose the ability to define their own narratives and destinies. As Couldry and Mejias[30] state, "data colonialism undermines populations' ability 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 marginalized populations' rights and ensure an equitable distribution of the data economy's benefits. This participatory approach is fundamental to mitigating data colonialism's negative effects and promoting social justice in the digital environment.

Couldry and Mejias[31] advocate creating data sovereignty policies under which communities control their own data and can decide how those data are used. They argue that "data sovereignty is a critical response to data colonialism, enabling communities to regain control of their digital resources."

Implementing robust regulations that protect privacy and guarantee informed consent is another crucial step. Brazil's General Personal Data Protection Law (LGPD) and the European Union's General Data Protection Regulation (GDPR) are examples of legislation intended to protect individuals' rights regarding their personal data. These laws establish standards for collecting, storing, and using data, promoting transparency and accountability.

It is therefore important to promote critical digital literacy that enables populations to understand and question power dynamics in the digital environment. Gomes[32] 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 for empowering individuals and communities to exercise control over their data and resist data colonialism practices.

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, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023. p. 34.

4. Transparency, Algorithmic Ethics, and Public Policy

The opacity of algorithms and the lack of transparency in the decisions these systems make raise significant ethical questions. Pasquale[33] 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[34] suggests that understanding the cultural and historical context in which algorithms are developed is necessary to mitigate their discriminatory effects. Noble[35] also emphasizes that "resistance to algorithmic racism must involve both a critique of technologies and the transformation of the social systems that produce them."

To mitigate these problems, governments and institutions must develop public policies regulating AI use to ensure that these systems are auditable and accountable. Yeshimabeit and Traub[36] propose that "AI regulation must include mechanisms for transparency and accountability to prevent the perpetuation of racial inequalities." Silva[37] argues that human rights impact assessments must be a prerequisite for adopting algorithmic systems, emphasizing that "transparency and accountability are essential to ensuring equity in algorithmic processes."

Regular audits to identify and correct biases are one proposed solution. O'Neil[38] suggests that "independent audits are necessary to ensure that algorithms are not reinforcing prejudices and inequalities." Auditing must become a standard practice in algorithm development and implementation processes, enabling biases to be detected and corrected before they cause significant harm.

Furthermore, it is crucial to create algorithms trained on diverse and representative data. Benjamin[39] emphasizes that "including 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. *Enculturaging Algorithms*. In: *Proceedings of the International Conference: Artificial Intelligence & Regulation*. LUISS Rome, 2019. p. 94.

35. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora 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, Tarcízio da. *Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais*. São Paulo: Edições Sesc SP, 2022. p. 137.

38. O'NEIL, Cathy. Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia. 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.

voices in algorithm development is crucial to creating fairer and more equitable systems." In addition, Pasquale[40] argues that "the data used to train algorithms must be carefully selected to avoid reproducing historical biases." Data diversity and the inclusion of varied perspectives are essential to developing algorithms that serve all of society fairly.

Raising awareness of AI's risks and impacts on society is another essential step. Capurro[41] emphasizes the importance of digital literacy that includes a critical understanding of algorithms and their social implications. Noble[42] argues that "education about AI's impacts must be an integral part of academic curricula to prepare future generations to address these technologies' ethical and social issues." Education is a powerful tool for empowering individuals to question and better understand algorithms' influence on their daily lives. This educational process not only develops critical thinkers but also enables them to use technology for their own benefit and the social good.

Gomes[43] suggests that implementing effective public policies must include the active participation of communities affected by algorithms. It is crucial to develop policies that include marginalized communities' voices, ensuring that their concerns and needs are considered in AI system development and implementation. This participatory approach is fundamental to creating policies that not only mitigate algorithms' negative effects but also promote justice and equity.

In this way, AI can be used to promote social justice by developing technologies that help reduce inequalities and empower marginalized communities. Noble[44] suggests that "AI technologies must be designed from a social justice perspective, considering the needs and experiences of historically

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

42. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021. p. 135.

43. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023. p. 28.

44. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021. p. 149.

marginalized groups." Capurro [45] stresses the need for an ethical and responsible approach to 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 affect marginalized groups. A study presented at the NeurIPS conference in 2023, entitled Reevaluating COMPAS: Base Rate Tracking and Racial Bias, analyzed the shortcomings of COMPAS, showing significant deviations and raising concerns about the presence of racial biases in the system. [46]

To mitigate these problems, algorithmic systems must be transparent and auditable. This means that organizations using these systems must be able to explain how the algorithms work and what data are used to train and operate these models. Diakopoulos [47] 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, ethical algorithm development is essential. This includes implementing practices that ensure diversity in training data and development teams. Binns [48] 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 must be aware of the social and ethical impacts of their creations and take proactive measures to mitigate the risks.

A concrete example of AI regulation is the European Union's General Data Protection Regulation (GDPR) [49]. The GDPR establishes strict guidelines on how personal data must be collected, stored, and used, ensuring that individuals have control over their data. One of the GDPR's provisions, under Article 22, requires that

45. CAPURRO, Rafael. *Enculturaging 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 COMPAS: Base Rate Tracking and Racial Bias. NeurIPS, 2023. Available at: NeurIPS Conference. Accessed: October 13, 2024.

47. DIAKOPOULOS, Nicholas. Accountability in algorithmic decision making. Communications of the ACM, v. 59, no. 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: October 20, 2024.

49. 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: October 11, 2024.

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

Another example is Brazil's General Data Protection Law (LGPD) [50], which seeks to protect Brazilian citizens' privacy rights and regulate the collection, storage, and use of personal data. The LGPD establishes several legal bases for processing data, explicit consent being one of them, but also includes grounds such as the performance of contracts, compliance with legal obligations, and the controller's legitimate interest, among others. In addition, the law requires organizations to implement measures to ensure the security and privacy of the personal data they process.

In addition to regulations, self-regulation 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 ethical AI development that include principles of transparency and accountability. This coalition works to promote AI practices that respect human rights and advance social justice. [51]

Implementing independent audits is also a recommended practice to ensure the transparency and fairness of algorithms. O'Neil [52] suggests that "independent audits are necessary to ensure that algorithms are not reinforcing prejudice and inequalities." These audits should be conducted by independent entities that can objectively assess the fairness and effectiveness of algorithmic systems.

Final Considerations

It can be seen that, although algorithms and AI systems have the potential to benefit society, addressing and mitigating the racial biases embedded in these systems is crucial. Promoting algorithmic ethics is essential to ensure that technology advances equitably and fairly. Recognizing algorithmic biases and being transparent about them 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 (Internet Civil Rights Framework). Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed: October 11, 2024.

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

52. O'NEIL, Cathy. Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia. Santo André: Editora Rua do Sabão, 2020. p. 143.

steps toward building a fairer society [53]. The fight against algorithmic racism is not merely a technical issue, but a battle for equity and justice in an increasingly digitalized world.

Accordingly, 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 of AI's impacts are fundamental steps toward creating a technological environment that serves everyone fairly. Experts in the field argue that combating algorithmic racism is part of a broader struggle 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 algorithms' influence on their lives. Education must prepare future generations to address the ethical and social issues raised by these technologies, promoting a more aware and equitable society. There is consensus that education about AI's impacts 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 must be designed from a social justice perspective, considering the needs and experiences of historically marginalized groups. In this way, it is possible to mitigate the negative effects of algorithmic racism and promote a fairer and more 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. Accessed: October 18, 2024.

BEZERRA, Arthur Coelho; COSTA, Camila Mattos da. Pele negra algoritmos brancos: informação e racismo nas redes sociotécnicas. Liinc em Revista, v. 18, no. 2, 2022.

53. SILVA, Tarcízio da. *Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais*. São Paulo: Edições Sesc SP, 2022.

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: 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 (Internet Civil Rights Framework). Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed: 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: October 13, 2024.

DIAKOPOULOS, Nicholas. Accountability in algorithmic decision making. Communications of the ACM, v. 59, no. 2, 2016.

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

G1. 'Medo, frustrado e constrangido', diz homem detido por engano em estádio após erro do sistema de reconhecimento facial. Fantástico, April 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: October 18, 2024.

GOMES, Bárbara. Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações. Undergraduate thesis. 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: October 18, 2024.

NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021.

O'NEIL, Cathy. *Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia*. Santo André: Editora Rua do Sabão, 2020.

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

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

SILVA, Tarcízio da. *Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais*. São Paulo: Edições Sesc SP, 2022.

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, no. 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: October 11, 2024.

VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society, v. 12, no. 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 Training Generative Artificial Intelligence: A Challenge for Data Protection and Privacy

RODRIGO SANTANA DOS SANTOS

Contents: Introduction. 1. Key Concepts. 1.1 Machine Learning in the Context of Generative AI. 1.2 Extracting Data from the Internet (Data Scraping). 1.3 Privacy, Data Protection, and AI in Brazil. 2. International Best Practices on AI, Privacy, and Data Governance. 2.1 Organisation for Economic Co-operation and Development. 2.2 European Union Guidelines for Trustworthy AI. 3. Analysis of Case Studies. 3.1 Extracting data from the internet through data scraping. 3.2 Meta's collection of data 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, activity, or right with the promotion of a regulated environment that fosters new technologies and business models for the country's socioeconomic development. In the digital environment, assessing models that seek this balance is highly relevant, given the dynamism of technological development and the need for trust in commercial, economic, and social relationships in that environment.

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

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

One of the main challenges is ensuring data protection and privacy during generative AI training, given the need for excessive data collection, including personal data. The opportunities offered by advances in this AI segment are undeniable, for example in improving scientific and creative writing, [2] education and learning, [3] accessibility and

1. Currently General Coordinator of Standardization at the National Data Protection Authority (ANPD). A career civil servant specializing in regulation in the technological field, working on the regulation of telecommunications services and personal data protection. Holds a master's degree in Electrical Engineering from UNB and a postgraduate qualification in Digital Law from ITS Rio/UERJ. A member of Study Group 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: August 02, 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: July 27, 2024.

inclusion, reducing economic and social inequality, [4] as well as in health and medicine. [5]

Accordingly, this article seeks to identify the main problems and challenges involved in the excessive collection of personal data to train AIs, considering techniques for extracting data from the internet, such as data scraping, and the observed trend among so-called Big Tech companies to change their privacy policies to collect massive amounts of users' personal data in order to train generative AIs.

The article is divided into a theoretical section, covering key concepts, which presents technical and legal concepts, and international best practices on AI, privacy, and data governance; and a section with case studies on extracting data from the internet through data scraping and on Meta's collection of data for AI training, identifying possible regulatory solutions.

1. Key Concepts

1.1 Machine Learning in the Context of Generative AI

Machine learning is a subfield of AI focused on developing algorithms that enable machines to learn from data and make predictions or decisions without being explicitly programmed for each specific task. [6] It can also be defined as a computational method that uses experience to improve performance or make more accurate predictions. [7]

Among the various types of machine learning, deep learning is a subfield that focuses on algorithms inspired by brain architecture, that is, a deep neural network, and these 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,

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: 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: August 01, 2024.

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

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

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

In this regard, a deep learning model needs a large volume of data to effectively train the various parameters that make up the neural network and, of course, obtain more precise and accurate results. [8]

1.2 Extracting Data from the Internet (Data Scraping)

Extracting data from the Internet, also known as scraping, can be understood as the automated practice of extracting large amounts of data published on internet websites. This extraction is performed using software that sends requests to web pages, collects and analyzes their content, and extracts specific information of interest. Extraction enables data to be collected quickly and inexpensively, often without the consent or knowledge of the data owners or the individuals to whom the data belong. [9]

The general term “data scraping” refers to any time “a computer program extracts data from output generated by another program.” More specifically, scraping is the “retrieval of content posted on the World Wide Web using a program other than a web browser or an application programming interface (API).” Extraction “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.” [9]

Scraping data from the internet is a method that makes it possible to obtain an enormous amount of data at relatively low cost. This scenario is ideal for meeting the demands of AI machine learning methods, such as deep learning, which require large amounts of data.

One of the most notorious cases of scraping for AI was carried out by Clearview AI, a startup that scraped more than three billion images to develop a facial recognition system. [9]

Another case was recently presented by Human Rights Watch, an international, nongovernmental, nonprofit human rights organization, which analyzed 0.0001% of the LAION-5B database, containing 5.85 billion images and captions 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: August 02, 2024.

to train AI. [10] This investigation found photographs of children from 10 Brazilian states. [11]

Many data scraping cases have gone to court, for example the case involving hiQ Labs and LinkedIn in the United States. [12] hiQ is a small data analytics company that used automated bots to collect information from public LinkedIn profiles. LinkedIn used legal means to prevent this collection; however, hiQ Labs filed a lawsuit against LinkedIn, seeking an injunction against this restriction, which was granted. LinkedIn appealed, and the district court's preliminary injunction was upheld, preventing LinkedIn from denying hiQ Labs access to LinkedIn members' public profiles. However, following another appeal in a different court, hiQ was found to have violated LinkedIn's terms of use, and a settlement was reached. [12]

There are several cases in US courts involving platform companies whose users' information is scraped. In this veritable data scraping war, various companies claim that such conduct conflicts with privacy and personal data protection laws, but in fact, in some cases they are seeking to protect data they believe to be theirs, or protecting their website and their own commercial interests. Ultimately, user privacy and security end up being invoked when they align with corporate interests. [12]

On the other hand, a new data scraping market is emerging. [12] For example, Open AI made deals with the Associated Press and Axel Springer, the parent company of Político and Business Insider, to obtain data, including personal data. [13]

1.3 Privacy, Data Protection, and AI in Brazil

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

10. HUMAN RIGHTS WATCH. Brasil: Fotos de crianças são usadas indevidamente para alimentar IA. 2024. Available at: https://www.hrw.org/pt/news/2024/06/10/brazil-childrens-personal-photos-misused-power-ai-tools. Accessed: August 02, 2024.

11. EUROPEAN UNION. Artificial Intelligence Act. 2024. Available at: https://artificialintelligenceact.eu/ai-act-explorer/. Accessed: August 03, 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: August 02, 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: August 02, 2024. Citing BARRADI, Thomas, OpenAI Offering Media Outlets as Little as $1M to Use News Articles for AI Models, New York Post. 2024.

In this regard, the law's application established a regulatory framework for processing personal data, regardless of the medium, physical or digital, or the technology used, such as blockchain or AI.

It should also be noted that Article 3 of the LGPD provides that the law applies if: i) the processing operation is carried out within the national territory; ii) the processing activity is intended to offer or supply goods or services or to process data of individuals located within the national territory; or iii) the personal data being processed were collected within the national territory.

Thus, it can be concluded that the LGPD applies whenever personal data are processed, even through AI, under Article 3 of the law.

Accordingly, the principles, rights, and safeguards provided for in the law must be observed, with the principles of purpose, necessity, nondiscrimination, transparency, and accountability particularly relevant in the AI context.

All processing of personal data must be based on one of the legal grounds provided for in Articles 7 and 11 of the LGPD, with no hierarchy among them. It should be noted that the legislation places greater restrictions on the sensitive personal data specified in the law and on processing that reveals these types of data; the legal ground of legitimate interest cannot be applied.

Another AI-related provision of the LGPD appears in Article 20. This article establishes the right to a review of decisions made solely on the basis of automated processing when they affect the data subject's interests. Paragraph 1 provides for the right to information about the criteria and procedures used for the decision, also known as the right to an explanation.

The article directly concerns AI systems, but some points require regulation or interpretation by the ANPD. These include the parameters for considering a "decision made solely on the basis of automated processing." In this case, it would be useful to define the level of human intervention that could occur for the processing to be considered automated. Another point would be the criteria for determining when an interest is actually being affected.

In this regard, beyond Article 20 of the LGPD, one issue has raised concerns among authorities and academia: the relationship between excessive collection of personal data to train AI systems and privacy.

Regarding this collection of personal data, there are legal aspects that must be observed, such as compliance with the aforementioned principles, legal grounds for processing, and obligations provided for in the LGPD.

Also noteworthy is the likely limitation of data subjects' rights provided for in the LGPD, such as access, correction, anonymization, blocking, deletion, and explanation, which will be discussed in greater detail below. In addition, informational self-determination is a fundamental pillar of the LGPD for data subjects' actions.

Furthermore, a data protection and privacy policy is a best-practice instrument provided for in Article 50 of the LGPD. This article states that controllers and processors, within their respective responsibilities for processing personal data, individually or through associations, may formulate best-practice and governance rules that establish organizational conditions, operating arrangements, procedures, including complaints and petitions from data subjects, security standards, technical standards, specific obligations for the various parties involved in processing, educational activities, internal oversight and risk-mitigation mechanisms, and other aspects related to personal data processing.

Paragraph 2 further provides that the controller or processor demonstrate a commitment to adopting internal policies that ensure compliance with standards and best practices relating to personal data protection, and establish appropriate policies and safeguards based on a process of systematically assessing privacy impacts and risks.

In this regard, the policy can be considered an internal governance instrument containing guidelines and measures concerning data processing, from collection to deletion. This set of rules is addressed to employees or public and private entities that interact with the controller or processor.

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

Accordingly, considering the best-practice and governance rules provided for in Article 50 of the LGPD, the controller must adopt internal processes and policies that ensure comprehensive

compliance with standards and best practices relating to personal data protection. For example, the United Kingdom's data protection authority (Information Commissioner's Office – ICO) published guidance on how to provide privacy information to data subjects. [14]

2. Best Practices on AI, Privacy, and Data Governance

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

2.1 Organisation for Economic Co-operation and Development

The Organisation for Economic Co-operation and Development (OECD) [15] published a document analyzing the intersection between privacy and artificial intelligence, especially generative AI, which requires enormous volumes of data for learning [16]. This analysis was based on the guiding principles included in the OECD Privacy Guidelines of 1980, updated in 2013, and the OECD Recommendation on AI of 2019 (called the "OECD Recommendation on AI"), updated in 2024.

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

The document identifies potential similarities and differences between AI and privacy principles.

Principle 1.1: Inclusive growth, sustainable development, and well-being. The document identifies positive social benefits, such as improvements in health and efforts to combat climate change, and economic benefits, such as reducing the costs of producing 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-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/. Accessed: August 03, 2024.

15. Organisation for Economic Co-operation and Development (OECD). An 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. Accessed: August 04, 2024.

greater system accuracy can conflict with privacy and data protection rights, as larger amounts of data are needed for training. The document notes that data protection authorities and courts have dealt with these conflicts for many years, applying constitutional mechanisms to resolve conflicts between competing rights and interests in specific cases, for example by applying the “balancing test” to identify proportionality between privacy and AI systems.

Principle 1.2: Respect for the rule of law, human rights, and democratic values, including fairness 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 safeguards, amplifies these risks because of the massive scale and scope of the application of such systems and their input training data during the training phase.

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

Regarding explainability and interpretability, the document notes that they feature in policy discussions in both the AI and privacy communities. The complexity and often “black box” nature of machine-learning-derived AI systems, particularly generative AI models, make these issues increasingly urgent.

Principle 1.4: Robustness, security, and safety. This principle addresses security and safety measures relating to data processing that must be adopted.

It states 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.” [17] The document notes that robust machine learning models traditionally need large, representative datasets for training. This can conflict with the data minimization principle [18]. However, certain safeguards, such as Privacy Enhancing Technologies (PETs), can help narrow the gap between developing secure AI models and protecting individuals’ privacy rights.

Principle 1.5: Accountability. The document states that both the privacy and AI communities have developed approaches to accountability and risk management. It highlights OECD work on AI classification [19] and accountability, [20] which provides 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 published guidelines for considering AI trustworthy. According to the document, trustworthy AI would comprise three elements that should be observed throughout the system’s entire lifecycle: a) it should be lawful, complying with all applicable laws and regulations; b) it should be ethical, ensuring adherence to ethical principles and values; and c) it should be robust, both technically and socially, since even with good intentions, AI systems can cause unintentional harm. [21]

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

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: November 04, 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. Accessed: August 04, 2024. Citing 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. Accessed: August 04. Citing OECD. “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. Accessed: August 04. Citing 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: August 04, 2024.

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

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

The analysis will address two cases related to collecting personal data to train generative AI and is restricted to Brazilian legislation.

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

3.1 Extracting data from the internet through data scraping

First, it should be mentioned that balancing internet data extraction with the principles, foundations, and safeguards provided for in the LGPD presents an enormous challenge.

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

The purpose principle means carrying out processing for legitimate, specific, explicit purposes communicated to the data subject, with no possibility of subsequent processing in a manner incompatible with those purposes. The necessity principle means limiting processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportionate, and not excessive 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 reconcile with the law. For example, how can the purpose of AI training be considered specific, how can this purpose be communicated to the data subject, and how can it be determined what data are necessary if general-purpose AI applications can be highly 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 runs counter to the necessity principle.

Another noteworthy issue concerns informational self-determination, a foundation of the LGPD provided for in item II of Article 2, which grants data subjects the right to control their own personal data based on the precepts of good faith and transparency.

Data subjects cannot exercise this right to control their data, given that they do not even know their data are being processed. A lack of compliance with these guidelines can lead to serious legal consequences and undermine users' trust in AI systems.

Data scraping is an activity that is difficult to bring into compliance with the transparency principle, since it is a silent activity that occurs without the data subject's knowledge.

Regarding the legal grounds for collecting data for AI training, provided for in Articles 7 and 11 of the LGPD, the most commonly used ground is legitimate interest.

The LGPD establishes stricter parameters for processing data on this basis under Article 10. For example, it may only serve as a basis for processing personal data for legitimate purposes, considered in light of concrete 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 Law.

In addition, the ANPD published a guide [22] explaining the need for a balancing test to assess whether the processing activity does not override fundamental rights and freedoms and respects the data subject's legitimate expectations. There can be no legitimate expectation in this case, since the data subject is unaware of the processing.

Regarding data subjects' rights, data subjects are hindered in 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. Being unaware of the processing being carried out and lacking clear communication channels with the controller weakens the entire legal model established.

22. ANPD. Guia Orientativo de Hipóteses Legais de Tratamento de Dados Pessoais: Legítimo Interesse. 2024. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Accessed: October 28, 2024.

Article 20 establishes the processing agent's obligation to provide, whenever requested, clear and adequate information about the criteria and procedures used for the automated decision, while respecting commercial and industrial secrets. This provision addresses the so-called right to an explanation, which relates to the best practice of explainability.

Another debated issue concerns whether data already public on the internet [23] could be processed without the data subject's consent. Article 7, paragraph 4 of the LGPD provides that the consent requirement is waived for data made manifestly public by the data subject, while safeguarding the data subject's rights and the principles provided for in the Law.

Furthermore, it should also be noted that Article 7, paragraph 3 provides that processing personal data to which access is public must consider the purpose, good faith, and public interest that justified making them available.

Therefore, even if data subjects' consent is considered unnecessary, collecting public personal data for AI training must comply with the purpose, good faith, rights, and principles provided for in the LGPD.

It should be noted that the legislator provided that obtaining consent would not be necessary; however, processing data will require using a legal ground authorizing that processing.

In this regard, data scraping for general-purpose AI systems has a high potential for noncompliance with the LGPD and does not follow best practices for developing AI systems, particularly transparency, explainability, data governance, and accountability. However, AI's role in developing new business models and technological solutions is undeniable, as already mentioned in this article. Legal, technical, and administrative safeguards, to be presented in section 3.3, are therefore needed to reduce risks to the fundamental rights to data protection and privacy.

3.2 Meta's collection of data for AI training

Recently, Meta announced a new privacy policy that raised concerns among users. Meta stated that, starting June 26, 2024, users' public posts would be used to train generative AI without needing to obtain 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: August 02, 2024.

Meta's privacy policy states that the data collected are shared with companies in the Meta corporate group, including Facebook, Messenger, Instagram, and others.

An examination of Meta's privacy policy [24] shows that the following data are collected:

- Content created, such as posts, comments, or audio;
- Content provided through our camera feature, camera roll settings, or voice-enabled features;
- Messages sent and received, including their content, subject to applicable laws;
- Metadata about content and messages, subject to applicable laws;

- The types of content, including ads, that users view or interact with, and how they do so;
- The apps and features used and the actions users take in them;
- Purchases or other transactions users make, such as through Meta's checkout experiences, including credit card information;

- Hashtags used;
- The time, frequency, and duration of their activities on Meta's products.

It also explains that it collects contact data, such as information about friends, followers, groups, accounts, Facebook pages, and other users and communities with whom users are connected or interact. The company states that it collects names and email addresses or phone numbers if uploaded or imported from a device, such as when syncing an address book.

In its privacy center, Meta describes how it processes data for AI training and states that a generative AI model can create content, such as text, images, and audio, when a person gives instructions or asks a question.

It explains that it uses models that generate text and images and need massive amounts of data to make estimates and be more effective.

24. META. Política de Privacidade da Meta. 2024. Available at: https://pt-br.facebook.com/privacy/genai. Accessed: August 04, 2024.

It also states that it processes data based on five pillars: privacy and security, fairness and inclusion, robustness and safety, transparency and control, and governance and responsibility.

It further describes processing data on the basis of legitimate interest, in the same way as it does in the European region and the United Kingdom.

In response to the possible change in Meta's privacy policy, the ANPD, through Order No. 20/2024/PR/ANPD, published in the Official Gazette on July 02, 2024, supported by Vote No. 11/2024/DIR-MW/CD from director Miriam Wimmer, issued a preventive measure ordering the immediate suspension in Brazil of Meta's new privacy policy, which authorized the use of personal data published on its platforms to train AI systems. [25]

The company's request for reconsideration was denied through Decision Order PR/ANPD No. 24/2024, considering the need to postpone analysis of the requests for suspensive effect and for full reconsideration of the decision until a technical analysis of the proposed measures and submission by Meta of a compliance plan specifying concrete deadlines for implementing the measures under Article 36 of the Oversight Regulation (Resolution CD/ANPD No. 01/2021), or documentation proving their entry into force, and submission of the balancing test for the legal ground of Legitimate Interest, within up to 10 (ten) business days.

However, after all requested documentation was submitted, Decision Order PR/ANPD No. 33/2024, based on VOTE No. 23/2024/DIR-JR/CD, decided to suspend the precautionary decision as follows: (i) approve the updated compliance plan submitted by the company, under the reasoning presented in Vote No. 23/2024/DIR-JR/CD and Technical Note No. 39/2024/FIS/CGF/ANPD; and (ii) suspend the preventive measure imposed on Meta by the Board of Directors under Decision Order PR/ANPD No. 20/2024, subject to full compliance with the compliance plan.

Regarding privacy and data protection, the suspension order was based on four important points: the legal ground; the principles of purpose, necessity, and transparency; limitations on data subjects' rights; and the use of children's and adolescents' personal data.

25. ANPD. ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta. 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: August 04, 2024.

Legal Ground

According to the director's vote underpinning the decision on the preventive measure, regarding the legal ground, legitimate interest did not appear to be the most appropriate basis for processing, considering that sensitive personal data might be processed, particularly given the possible use of images, audio, text, and videos that could reveal data subjects' political, religious, and sexual affiliations, among other aspects of personality listed in Article 5, II of the LGPD.

It further emphasized that, for this legal ground to be used appropriately, the interest must be based on concrete situations, that is, real, clear, and precise situations aimed at specific, well-defined interests, even in the near future, excluding interests considered on the basis of abstract or merely speculative situations.

In addition, the analysis concluded that it is reasonable to assume that, in principle, data subjects do not expect information posted on the social network years earlier to be used to train generative AI.

The vote also addressed purpose, which it called the generic and broad purpose of training generative AI systems. Strong indications were found that the company's processing to train AI systems is not supported by the legal ground of legitimate interest, whether because it involves processing sensitive data, violates data subjects' legitimate expectations, or fails to comply with the principles of purpose and necessity.

In light of the director's analysis that legitimate interest would not be the most appropriate legal ground for processing data to train generative AI, and considering that sensitive data are present or that processing would probably reveal sensitive data, only consent could serve as the legal basis.

However, if the legal basis of legitimate interest were used, qualifications would be necessary to bring processing into compliance with the LGPD. First, stronger data governance would be needed in data collection, including an inventory to identify the types of data processed in order to separate those not considered sensitive, a record of processing operations as provided for in Article 37, and preparation of a Data Protection Impact Assessment.

Furthermore, a balancing test would need to be prepared to assess the specific purpose of training, the need for the data, and the

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

In this regard, the vote of the director reporting on the company's request for reconsideration, based on Technical Note No. 39/2024/FIS/CGF/ANPD, stated that the company had submitted all required documentation, including the legitimate interest balancing test, which contains more detailed information on processing personal data to train a generative AI system, along with various safeguards implemented to prevent the identification of data subjects and third parties' personal data through inferences.

According to Technical Note No. 39/2024/FIS/CGF/ANPD, the company's application of safeguards ensuring the possibility of pseudonymizing users' personal data, in order to mitigate any harmful effects on data subjects arising from processing, enables the legal grounds under Article 7 of the LGPD to apply to personal data processing for training generative AI models.

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

Transparency of data processing

Regarding transparency, the analysis by the director that underpinned the preventive measure concluded that there had been a failure to disclose clear, precise, and easily accessible information about the change in the privacy policy to allow personal data to be used for AI training.

However, the vote of the director who examined the request for reconsideration stated that the company had improved the mechanisms for providing information on data processing for generative AI. In addition, the compliance plan submitted includes a series of measures, such as notifications, updates to the privacy policy, and creation of a dedicated area on the website, demonstrating significant changes to provide greater transparency in complying with the ANPD's requirements.

In this respect, it must be understood that a privacy policy is an internal regulatory document directed at employees or natural or legal persons who interact with the agent. Under the LGPD, transparency must ensure that clear, precise, and easily accessible information

about the processing being carried out and the respective processing agents is accessible to the data subject, while respecting commercial and industrial secrets.

In this regard, the privacy notice is understood to be the most appropriate transparency mechanism for informing data subjects about processing. Attention must be paid to using communication methods that can guide data subjects clearly and simply. For example, if children's and adolescents' data are involved, users' physical and motor, perceptual, sensory, intellectual, and mental characteristics must be considered, using audiovisual resources where appropriate, to provide the necessary information to parents or legal guardians in a manner suited to children's understanding.

Exercise of data subjects' rights

Regarding the exercise of data subjects' rights, the director's vote underpinning the effective measure stated that there appear to be obstacles that excessively limit the exercise of rights. It showed that, to exercise the right to object, data subjects must go through several steps, requiring them to click eight options in the Facebook app.

In this respect, unlike the scraping of personal data from the internet, the processing agent is in a position to develop solutions and channels through which data subjects can exercise the rights provided for in the LGPD.

If the agent can justify using the legal basis of legitimate interest, it would be useful to have opt-out mechanisms, given the provision for deleting data that are unnecessary, excessive, or processed in noncompliance with the LGPD, which appears to apply in this case.

The vote of the reporting director who examined the suspension of the measure stated that the company had improved its opt-out mechanisms, facilitated access to the exercise of rights for users and nonusers by reducing the number of clicks needed to access them, and adopted measures to facilitate transparency, as mentioned above, in accordance with the ANPD's requirements.

Processing children's and adolescents' data

Regarding the processing of children's and adolescents' data, the vote underpinning the preventive measure stated that the necessary safeguards do not appear to be present for processing children's and adolescents' personal data to train AI systems, particularly on the legal ground of legitimate interest.

The legal ground of legitimate interest can be used for processing children's and adolescents' data. The ANPD published a guide on the legal basis of legitimate interest [26] and reaffirmed its understanding that it may be used to process minors' data. However, according to the ANPD's analyses in this specific case, safeguards would be necessary to ensure stronger protection of these data subjects' fundamental rights when processing data for AI training, specifically on the legal ground of legitimate interest.

In this regard, the company stated in its compliance plan that personal data from accounts belonging to users under 18 would not be processed to train and develop its generative AI models, thereby averting risks to this category of data subjects for the time being. However, Meta stressed that it would continue to discuss with the ANPD, within the ongoing oversight proceedings, the legitimacy of processing this category of data subjects' personal data.

In this regard, it should be noted that, in Europe, Meta announced that it "is not training its Llama models on content generated by accounts belonging to Europeans under 18." [27]

3.3 Possible Regulatory Solutions

The article by Solove and Hartzog [28] identifies possible solutions, notably, from the perspective of data protection and privacy, banning data scraping for use in generative AI training and using consent. The article also proposes an agenda for regulators consisting of four principles covering reasonable risks and harms, benefits to society, transparency and accountability processes, and protection of data used for AI training.

It should also be noted that technical measures or safeguards can be sought to improve data collection for training AI systems, particularly on the legal ground of legitimate interest, and thereby ensure fundamental rights.

Under the LGPD, personal data are information relating to an identified or identifiable natural person. There does not appear to be a need to identify the data subject to train AI systems. It therefore seems sensible to

26. ANPD. Guia orientativo de hipóteses legais de tratamento de dados pessoais: Legítimo Interesse. 2024. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Accessed: November 03, 2024.

27. META. 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: November 04, 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: August 02, 2024.

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

Privacy-Enhancing Technologies (PETs), 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 to create synthetic data, can help resolve regulatory problems concerning the use of personal data in generative AI training. [29]

If the legal ground used is legitimate interest, the right to object (opt-out) is considered necessary so that data subjects can choose not to have their personal data processed for this purpose.

In this regard, France's data protection authority, the Comission Nationale de l'Informatique et des Libertés (CNIL), in a recent public consultation publication [30], suggested safeguards for AI training, notably anonymization or pseudonymization, the use of synthetic data, greater transparency of data processing, development of more transparent and auditable systems, and facilitation of the exercise of rights.

Final Considerations

The research revealed enormous regulatory challenges concerning data protection and privacy that must be addressed to develop ethical and responsible generative AI solutions that inspire trust and benefit society.

Data protection and privacy must not be a factor limiting innovation and new business models. However, the processing agent must observe the principles and safeguards provided for in the LGPD to create an environment of greater trust and security for developing AI systems.

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

29. PANGHANGAM. Nivarthi, K. S. How Privacy-Enhanced Technologies (Pets) are Transforming Digital Healthcare Delivery. American Scientific Research Journal for Engineering, Technology, and Sciences, 90 (1), 351–361. 2022. Available at: https://asrjetsjournal.org/index.php/American_Scientific_Journal/article/view/8268. Accessed: November 04, 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: November 04, 2024.

The use of anonymization or pseudonymization techniques, particularly Privacy-Enhancing Technologies (PET), synthetic data, processing transparency measures, and measures facilitating the exercise of rights can help ensure the fundamental rights to data protection and privacy during personal data processing for training generative AI systems.

The ANPD's actions concerning the change in Meta's Privacy Policy are aligned with international concerns debated in academia and by public authorities about excessive data collection for generative AI training.

The research can evolve to assess opportunities for regulatory solutions and their impacts on the fundamental rights to data protection and privacy, innovation, and socioeconomic development.

References

ANPD. ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta. 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: August 04, 2024.

ANPD. Guia Orientativo de Hipóteses Legais de Tratamento de Dados Pessoais: Legítimo Interesse. 2024. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Accessed: 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: 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: November 04, 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: November 04, 2024.

HUMAN RIGHTS WATCH. Brasil: Fotos de crianças são usadas indevidamente para alimentar IA. 2024. Available at: https://www.hrw.org/pt/news/2024/06/10/brazil-childrens-personal-photos-misused-power-ai-tools. Accessed: August 02, 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: August 03, 2024.

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

META. Política de Privacidade da Meta. 2024. Available at: https://pt-br.facebook.com/privacy/genai. Accessed: August 04, 2024.

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

MOHRI. M; Rostamizadeh. A; Talwalkar. A. *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. Accessed: August 04, 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: November 04, 2024.

Organisation for Economic Co-operation and Development (OECD). An intergovernmental economic organization with 38 member countries, founded in 1961 to stimulate economic progress and world trade.

PANGHANGAM. Nivarthi, K. S. How Privacy-Enhanced Technologies (Pets) are Transforming Digital Healthcare Delivery. American Scientific Research Journal for Engineering, Technology, and Sciences, 90 (1), 351–361. 2022. Available at: https://asrjetsjournal.org/index.php/American_Scientific_Journal/article/view/8268. Accessed: November 04, 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: 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: August 02, 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: August 02, 2024.

EUROPEAN UNION. Artificial Intelligence Act. 2024. Available at: https://artificialintelligenceact.eu/ai-act-explorer/. Accessed: August 03, 2024.

EUROPEAN UNION. Ethics guidelines for trustworthy AI. 2019. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Accessed: August 04, 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: August 01, 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

5

Classification of Harms Arising from AI Incidents

VINICIUS AZEVEDO COELHO

Contents: Introduction. 1. Incidents arising from artificial intelligence systems. 2. Types of harm related to AI incidents. 3. Severity levels of harm in AI incidents. Final considerations. References.

Introduction

In the network society, information and communication technologies have revolutionized how people interact and relate to one another. According to sociologist Manuel Castells, one of the leading theorists of the information age, digital transformation has profoundly changed human sociability, with impacts that transcend geographical and cultural boundaries [2].

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, fostering inclusive and sustainable growth and enabling significant scientific advances. Furthermore, its ability to integrate and analyze data from multiple sources improves decision-making and the automation of complex processes, demonstrating its broad usefulness in different systems [3].

For example, in commerce, AI contributes to task automation, personalization of customer experiences, and forecasting market trends [4]. In healthcare, it is used to diagnose diseases, develop treatments, and provide personalized care [5]. In transportation, AI features in the development of self-driving cars, improvements to public transport safety and efficiency, and traffic management [6]. In the environment, it helps monitor air and water quality, develop renewable energy, and reduce pollution [7]. In science, it accelerates research, tests

1. Postgraduate student in Digital Law at ITS/UERJ. Email: viniciusazevedocoelho@gmail.com.

2. CASTELLS, Manuel. A era da informação: economia, sociedade e cultura, v. 1 - A sociedade em rede. Translated by Roneide Venâncio Majer. 17th ed. São Paulo: Paz e Terra, 2016.

3. BALTRUŠAITIS, T.; AHUJA, C.; MORENCY, L. P. Multimodal Machine Learning: A Survey and Taxonomy. IEEE Transactions on Pattern Analysis and Machine Intelligence, v. 41, no. 2, pp. 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 forecast demand for products and services.

5. By way of 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 precisely 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 energy more efficiently.

hypotheses, discovers new medicines, and develops new technologies [8]. These are some examples of how AI can transform society. As the technology continues to develop, AI will have an even greater impact on our lives.

However, despite its transformative impacts, AI also brings a series of risks and ethical challenges. These risks can range from privacy and security issues to broader social and economic impacts and may lead to incidents causing substantial harm. Understanding and managing these adverse consequences are essential to ensure that AI's benefits are maximized while its harms are minimized.

AI incidents can be caused by various factors, including systemic vulnerabilities, human failures, and cyberattacks. These incidents can cause a range of negative consequences, such as physical and environmental harm and reputational and financial impacts. Harms can have different severity levels, from insignificant impacts to damage to property, health, and critical infrastructure, and even human deaths. In this context, assessing and classifying harms is a fundamental part of an effective response to AI incidents, with the primary aim of mitigating consequences and protecting organizations and users of artificial-intelligence-based systems.

In this context, this article's general objective is to map and identify the main concepts relating to harms arising from AI security incidents. It is therefore expected to be possible to categorize and understand incidents involving AI and their main consequences, as well as develop general frameworks indicating the types of harm arising from AI incidents and their severity levels. The two research questions that guided this study were: 1. What types of harm relate to different AI systems? and 2. What are the severity levels of harms arising from AI incidents?

This study therefore starts from the central problem of mapping and identifying the types of harm caused by security incidents in artificial intelligence systems, as well as assessing the severity levels of these harms. This problem is relevant because the increasing adoption of AI systems across various areas of society increases exposure to risks associated with

8. AI is currently already being used to analyze large scientific datasets and to create models that can predict the behavior of molecules and materials.

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

The methodology chosen to seek answers to the research questions includes a literature review, specifically concerning the conceptual and terminological foundation, using as primary sources texts published by authors specializing in cybersecurity, information technology, and artificial intelligence.

In addition, this study draws on publications by international organizations such as the Organisation for Economic Co-operation and Development (OECD), the United States National Institute of Standards and Technology (NIST), and the European Union on AI incidents and their consequences. These organizations have published documents on information security in AI that may be useful to researchers and professionals in the field. Also regarding research sources, to find practical examples of AI incidents, we used the AI Incident Database platform (https://incidentdatabase.ai), which collects, categorizes, and shares information on 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 section explores the definitions essential to its development and is devoted to definitions of AI incidents and harm. The second section addresses specific types of harm. The third and final section discusses severity levels of harms arising from AI incidents.

1. Incidents arising from artificial intelligence systems

This section introduces the fundamental concepts for understanding and developing the research. Its purpose is to present notions related to artificial intelligence and briefly address the idea of risks associated with systems using AI, before arriving at a definition of incidents arising from AI.

To establish the meaning of artificial intelligence, contributions by authors such as McCarthy, Newell and Simon, and Boden were used. For the notions of risk and harm, we drew on the theory of German sociologist Niklas Luhmann, who emphasizes the importance of assessing social impacts in his risk theory. This sociological approach was preferred over a quantitative treatment of risk typical of the exact sciences.

Defining artificial intelligence is itself challenging. Maria Regina Rigolon Korkmaz notes 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, widely debated definition of artificial intelligence emerged as a specific area of computing focused on developing computers that can imitate human intelligence in performing tasks [9].

This initial definition, proposed by John McCarthy [10], considered by many to have coined the term, describes artificial intelligence as the engineering of intelligent machines, that is, machines that exhibit characteristics associated with human intelligence. In the notorious conference proposal, McCarthy and his colleagues based their work on the idea that “every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it” [11].

A few decades later, Allen Newell and Herbert Simon [12] 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 [13].

Margaret Boden, one of today’s leading AI experts, defines AI as a way of creating systems that can think, learn, and act intelligently [14].

9. KORKMAZ, Maria Regina Rigolon. *Decisões Automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomsom Reuters Brasil, 2023, p. 95.

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

11. MCCARTHY, John. *Proposta para o 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 related 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 various aspects of AI. McCarthy's definition emphasizes creating machines that exhibit intelligent characteristics previously associated with human behavior. Newell and Simon's definition highlights creating systems that can learn and solve problems autonomously. Boden's definition emphasizes creating 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, both in relation to specific mathematical structures and in their practical uses [15].

Although different or complementary, these definitions show us the versatility of this new technology, which can be used in simple or complex systems. Understanding this multiplicity of AI systems is relevant to an adequate understanding of the risks and harms arising from each type.

This is because simple uses of artificial intelligence generally involve specific and 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 users' purchase histories and preferences to suggest items. The risks associated with these simple uses are relatively low and may include language comprehension errors or inappropriate suggestions, which usually result in minor user dissatisfaction and limited impact.

On the other hand, complex uses of artificial intelligence 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 greater, including fatal traffic accidents if an autonomous vehicle fails or incorrect medical diagnoses that can lead to inappropriate treatments. Thus, while simple systems present lower and more manageable risks,

15. KORKMAZ, Maria Regina Rigolon. *Decisões Automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomsom Reuters Brasil, 2023, p. 98.

complex applications require greater robustness, transparency, and regulation to mitigate potentially serious impacts.

To understand risk within the scope of this study, we drew on Niklas Luhmann's social perspective [16]. According to the author, risks are inherent in society's increasingly contingent modernization. For Luhmann, society's future increasingly depends on decision-making: the future turns into risk as the possibilities increase

Luhmann proposes a concept of risk that presupposes uncertainty about future harms: risk is discussed when probable harm is the consequence of an action. For Luhmann, the concept of risk is associated with the condition of making decisions. Every decision entails the possibility that something may go wrong, that is, that a risk may materialize as harm. Thus, risk is the probability that an undesirable event will occur as a result of a decision [17]. Advanced technologies such as AI make social complexity ever greater and make it harder to predict and measure consequences.

Therefore, based on Luhmann's theory, risks are an inevitable consequence of society's modernization and growing complexity. In the context of artificial intelligence, this perspective is particularly relevant because the implementation of AI systems in various spheres of modern life exemplifies this increasing complexity. Every AI application, from simple chatbots to autonomous vehicles, involves decisions that can potentially turn the future into a field of uncertainties. The ability to predict and control the consequences of these decisions becomes increasingly challenging as technology advances, expanding possibilities and consequently risks.

We have seen that Luhmann maintains that risk is inherent in the condition of making decisions, where any choice carries the probability of resulting in harm. Thus, applying this to AI, every implementation of an artificial intelligence system involves decisions about algorithms, data, and application contexts that may fail or produce undesirable outcomes. 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 significant harms to citizens' freedom and privacy materializing.

16. In the sociology of risk, Luhmann reveals his concern about the imprecision of the concept and the difficulty the hard sciences encountered in adequately analyzing the problem of risk. Their concepts were vague and based on quantitative models. Luhmann therefore proposes assessing risks as a social problem grounded in 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 amplified by the contingent nature of technological decisions, where a system failure can have catastrophic consequences.

Thus, based on the elements studied so far, we can define AI risk as the uncertain possibility of an undesirable consequence occurring as a result of a decision made by an artificial-intelligence-based system.

The materialization of risk as harm constitutes an AI incident. According to the CSET taxonomy, AI harms have four elements that, once correctly defined, allow harms caused by AI to be identified. These key components serve to distinguish harms from nonharms and AI harms from harms not caused by AI. For an AI harm to occur, there must be: (1) an entity that suffered (which may be a person, thing, or place); (2) a harmful event or problem that (3) can be directly linked to a consequence of the behavior of (4) an AI system. All four elements must be present for AI harm to occur [18].

Additionally, according to an OECD study to define an AI incident, harm is expressed as the probability that an injury will actually occur [19]. Risk is a function of both the probability of an event occurring and the severity of the resulting consequences. In this context, AI-related risks and harms must be understood and managed to ensure its reliability and safe, responsible use. According to the OECD study [20]:

> Defining harm and assessing its types, severity levels, and other relevant dimensions (for example, scope, geographic scale, quantification, etc.) is fundamental to identifying the incidents that lead or may lead to that harm and developing an effective framework to address them [21].

18. CENTRE 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: January 17, 2024.

20. Ibid., p. 8.

21. Freely translated in the source from the original: “Defining harm and assessing its types, severity levels and other relevant dimensions (e.g. 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”.

Thus, the idea of harm as a consequence of risk is central to understanding AI incidents. Having made these considerations, we now turn to defining AI incidents.

Amodei et al., in the article Concrete Problems in AI Safety, describe AI incidents as events in which an artificial intelligence system behaves in an unintended or harmful manner because of problems such as specification failures, robustness errors, scalability failures, or safety complexity [22].

Crawford and Calo, in There is a Blind Spot in AI Research, define AI incidents as events in which artificial intelligence technologies cause harm or fail to operate as expected, generally because of limitations in research and development that do not fully consider their social and ethical impacts [23].

In addition to the authors above, some organizations also offer relevant definitions of AI incidents. According to the CSET taxonomy developed for the AI Incident Database, AI incidents involve real-world failures or near failures arising from the use of artificial intelligence systems [24]. Complementing this, the AI Index Report 2024 – Stanford HAI conceptualizes 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 [25]. The OECD's proposed definition of an AI incident states [26]:

> 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 nondiscrimination [27].

22. AMODEI, D. et al. Concrete Problems in AI Safety. 2016. Available at: https://arxiv.org/abs/1606.06565. Accessed: August 6, 2024, pp. 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: August 07, 2024, pp. 311-313.

24. AI Incident Database. CSET Taxonomy AI Incident Database. Available at: https://incidentdatabase.ai/taxonomy/cset/. Accessed: August 07, 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. Accessed: August 07, 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: January 17, 2024, p. 11.

27. Freely translated in the source from 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 contributions above, for the purposes of this study, an AI incident will be considered an event or situation in which an AI system fails or behaves unexpectedly, resulting in negative consequences. This may include technical errors, malfunctions, incorrect decisions, or biases that lead to harmful outcomes for individuals, organizations, or society in general. These incidents may occur because of problems in the design, training, implementation, or operation of AI systems. The types of harm related to AI incidents will be addressed in the next section.

2. Types of harm related to AI incidents

The increasing use of AI systems worldwide leads to an increase in the number of AI systems, which, as seen in the previous section, can cause real harm to people, organizations, and the environment.

Undesirable consequences related to AI systems differ from traditional cybersecurity risks in several ways [28]. 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 alone introduces problems such as data quality and bias, which can distort AI's outputs and decisions. Data accuracy and impartiality thus become critical issues, directly affecting AI systems' effectiveness and reliability.

Furthermore, the inherent complexity of AI systems and their dependence on data for training and decision-making create additional challenges, especially regarding privacy and security. Unlike traditional software, AI systems can be opaque, making it difficult for users to understand how decisions are made and data are used. This opacity, together with complexity, broadens the range of possible incidents, which may affect a small number of individuals or have significant impacts across different 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 harm. When this risk materializes, we face actual harm. 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: January 17, 2024.

of actual harms in standards and regulations are highly context-dependent and generally focus on physical injury or damage to people's health, property, or the environment (IEC 61508-1:2010, ISO/IEC 51:2014, ISO 26262-1:2018). In some cases, such as personal data protection regulations, they may refer to injuries caused by data breaches, including physical, material, or nonmaterial damage to natural persons, such as loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage to the natural person involved.

CSET, a research center focused on emerging technologies, divides these harms into two broad categories in its AI harm framework: tangible harms and intangible harms [29].

Tangible harm is material in nature and is therefore observable, verifiable, and definite. Common examples include physical injury (including death), financial loss, and damage to private or public property. This type of harm is generally 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, generally cannot be directly observed. Although the event causing the harm may be observable and its effects and consequences may be expressed observably, the harm itself is not. Intangible harm may include, but is not limited to, mental/psychological harm, pain and suffering, harm to intangible property (for example, intellectual property theft or damage to a company's reputation), and loss of trust or belief.

The figure below, adapted and translated from CSET material, indicates the types of harm categorized as tangible and intangible.

29. 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: August 6, 2024, p. 9.

Table 1 – Tangible and intangible harms divided into categories (CSET) [30]

Tangible harm categories		Intangible harm categories
Health/Physical safety harm		Harmful content
Infrastructure harm		Differential treatment
Physical property harm		Human/Civil rights
Financial loss		Democratic norms
Environmental harm		Privacy
Other		Other

According to CSET, harms can be classified by type as follows: Tangible harms:

• Health/physical safety harm: includes death, injury, or reduced life expectancy.
• Infrastructure harm: involves the network of roads, railways, utilities, and buildings needed to maintain commerce, transportation, political structures, and normal everyday life. Infrastructure may be harmed through destruction, diminished capacity, or reduced effectiveness

• Physical property harm: refers to the destruction of a physical object.

• Financial loss: encompasses any loss of an economic nature that does not arise from injury or damage.
• Environmental harm: relates to ecological degradation resulting in pollution, habitat destruction, waste of natural resources, or industrial accidents.

Intangible harms:

• Harmful content: involves deepfakes, disinformation, cyberbullying, identity misrepresentation, 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: August 6, 2024.

• **Differential treatment**: encompasses issues of bias and fairness related to AI. However, the bias must be associated with a group having a protected characteristic. Differential treatment based on protected characteristics generally overlaps with or occurs alongside a civil rights violation.

• Violation of human rights, civil liberties, civil rights, or democratic norms: relates to violations of the protection and promotion of fundamental rights and freedoms.

• **Privacy**: harms may occur through unjustified surveillance, data breaches, or the collection and use of personal information without consent.

• Other harms: harms that do not fall within any of the other categories mentioned.

This CSET taxonomy is used as the main reference for other specific and relevant studies on the subject, such as the OECD proposal, which presents similar categories, as indicated in the table below:

Table 2 – Types of harm related to AI incidents [31]

Type of harm	Description	Example
Physical harm	Refers to bodily injuries or direct physical harm caused to a person. May involve harm to health or safety, or other negative impacts on physical health.	Failures in industrial robots causing workplace accidents.
Environmental harm	Indicates undesirable consequences for the environment, such as soil contamination, air pollution, or water pollution.	Use of AI in industrial processes resulting in pollutant leaks.
Financial harm, including property harm	Includes economic losses, financial damage, or negative impacts on personal or business finances. May involve material damage to physical property, such as buildings, vehicles, equipment, and others.	Failures in automated trading systems causing 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: January 17, 2024.

Table 2 – Types of harm related to AI incidents

Continuation

Type of harm	Description	Example
Reputational harm	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.	An AI algorithm that unfairly discriminates against customers, causing a negative perception of the institution.
Harm to the public interest	Refers to harms affecting the protection of critical infrastructure and social institutions.	AI used to manipulate public information, affecting trust in government institutions
Restrictions on civil liberties	Harms resulting in the restriction or violation of an individual's civil rights, such as discrimination and privacy violations, among others.	Facial recognition systems leading to mass surveillance and invasion of privacy.
Psychological harm	Refers to emotional, mental, or psychological harms, such as stress, trauma, and anxiety, among others.	Artificial intelligence on social media contributing to anxiety and depression.

Classifying harms arising from AI incidents is essential for understanding and effectively mitigating the risks associated with using this technology. Categorizing harms, whether as tangible or intangible, or by type, allows for a more precise and detailed analysis of incident consequences. Tangible harms, such as physical injuries, financial losses, and material damage, are more easily quantified and verified, facilitating immediate response and corrective measures. Intangible harms, on the other hand, such as psychological suffering, loss of trust, and privacy violations, although harder to quantify, are equally important and require specific approaches to be addressed appropriately.

Clear harm classification also improves the collection and analysis of AI incident data, allowing patterns and trends to be identified. This contributes to developing better security practices and policies, helping prevent similar incidents from recurring. In addition, detailed categorization of harm types facilitates communication among different stakeholders, including AI developers, end users, and researchers, promoting a shared understanding of the risks and consequences associated with AI use.

In the regulatory context, classifying harms arising from AI incidents plays an important role in formulating effective laws and policies. Regulators need an accurate understanding of the types of harm that may occur to establish appropriate security and liability standards. Thus, harm classification not only improves incident response and mitigation but also supports creating a robust regulatory framework that protects society against AI's potential risks.

3. Severity levels of harm in AI incidents

A second relevant factor to consider regarding AI harms concerns their severity. Assessing the severity of harms caused by Artificial Intelligence (AI) incidents is a fundamental aspect of risk management in this field. A stratified approach to classifying harm severity allows for a more accurate and differentiated analysis of the impacts these incidents may generate. This is essential not only for developing appropriate regulatory policies but also for implementing effective preventive and corrective measures.

Furthermore, categorization by severity level plays a critical role in prioritizing incident responses. By identifying and focusing on the most serious incidents, resources can be allocated more efficiently to protect public interests and safeguard individual safety and rights. This classification system also promotes clear communication about the risks and consequences associated with AI use, reinforcing transparency and responsibility in handling this technology.

According to the previously cited OECD study, there is as yet no widely accepted, comprehensive classification system accounting for all dimensions of harm caused by AI systems (that is, scope, scale, severity, types, impacts, etc.). An important step in this direction is the taxonomy developed by CSET, which proposes five levels of severity for harm caused by AI systems: negligible harm (negligible), minor harm (minor), moderate harm (moderate), severe harm (severe), and critical harm (critical). Based on these levels, we prepared the table below:

Table 3 – Severity levels of harm in AI incidents [32]

Severity	Description	Examples
Negligible (Negligible)	Minimal harm, easily remedied.	Rounding error in low-impact financial calculations by an AI system.
Minor (Minor)	Limited harm to property, social stability, the political system, or civil liberties.	Content moderation AI failing to detect and remove offensive posts on a social network, causing limited discomfort.
Moderate (Moderate)	Injury or near injury to humans. Significant harm to financial interests.	An AI medical diagnosis system providing an incorrect result, leading to unnecessary treatment. An error in an AI algorithm used for automated stock market trading.
Severe (Severe)	Serious injury or near death of humans. Significant disruption to financial interests at a regional or national scale. Severe harm to property or the environment.	AI failure in autonomous vehicles leading to a traffic accident with serious injuries. Failure in AI systems used to forecast and manage a city's power grids.
Critical (Critical)	Death or near death of many humans. Critical disruption to financial interests at a national or global scale.	Failure in AI systems responsible for managing critical infrastructure, such as nuclear power plants or dams. Collapse of AI-based high-frequency trading systems, causing a stock market crisis with global economic impact.

The relevance of classifying harms can be illustrated by the provisions of Article 73 of the EU AI Act. Although it does not encompass all severity levels included in the CSET taxonomy, the European regulatory framework establishes the legal obligation to report serious AI incidents to supervisory authorities. According to the EU AI Act (Article 3, point 49, b),

> (49) "serious incident" means an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following: (a) the death of a person or serious harm

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: January 17, 2024.

> to a person's health; (b) a serious and irreversible disruption of the management or operation of critical infrastructure; (c) the infringement of obligations under Union law intended to protect fundamental rights; (d) serious harm to property or the environment.

In summary, categorizing harms is crucial to ensure compliance with the AI Act's provisions, which require responses proportionate to the severity of incidents, contributing to transparency and effectiveness in risk management and responses to AI incidents. This may serve as a basis for future legislation as AI incidents become more frequent and regulations evolve to keep pace with technological advances.

Final considerations

In concluding this introductory study of incidents arising from Artificial Intelligence (AI), several reflections emerge, integrating the theoretical and practical aspects explored in the previous sections.

First, the conceptualization of AI itself, as presented by McCarthy, Newell and Simon, and Boden, establishes an essential theoretical background. These definitions, which emphasize the engineering of intelligent machines, the autonomy of cognitive systems, and systems' ability to think and act intelligently, are fundamental to understanding their operating foundations and serve as a starting point for reflecting on the risks and harms associated with these systems. Luhmann's approach to risk, which considers the complexities and uncertainties associated with decisions, offers a critical lens for assessing AI's risks and harms in a social context.

This study highlighted how AI, despite its transformative potential in sectors as varied as healthcare, transportation, and the environment, carries inherent risks and consequences. These consequences, varying in probability and impact, can significantly affect individuals, groups, environments, and societies. The analysis of AI-related harm types in the second section revealed a range of potential consequences, from physical and environmental harms to financial, reputational, and psychological impacts.

Defining harm severity levels, as proposed by the CSET taxonomy, illustrates the need for a well-founded and adaptable regulatory framework. Establishing a precise classification of harms

by severity level not only helps accurately assess impacts but also guides the formulation of appropriate and prioritized responses to AI incidents.

In summary, this study reveals the complexity and dynamism of the challenges presented by AI. While the technology offers unprecedented opportunities for advances and innovation, it also requires careful reflection on the risks and responsibilities associated with its use.

Looking toward possibilities for future work, we intend to continue exploring this subject, with a particular focus on assessing AI incidents. Deepening our understanding of how best to manage risks and mitigate harms will be fundamental to ensuring safe and responsible AI use aligned with ethical and social values. Thus, studying the risks and harms associated with AI remains not only relevant but essential as we advance into the era of digital transformation.

References

AI Incident Database. CSET Taxonomy AI Incident Database. Available at: https://incidentdatabase.ai/taxonomy/cset/. Accessed: August 07, 2024.

AMODEI, D. et al. Concrete Problems in AI Safety. 2016. Available at: https://arxiv.org/abs/1606.06565. Accessed: August 6, 2024.

BALTRUŠAITIS, T.; AHUJA, C.; MORENCY, L. P. Multimodal Machine Learning: A Survey and Taxonomy. IEEE Transactions on Pattern Analysis and Machine Intelligence, v. 41, no. 2, pp. 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. Accessed: 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: August 07, 2024.

CASTELLS, Manuel. A era da informação: economia, sociedade e cultura, v. 1 – A sociedade em rede. Translated by Roneide Venâncio Majer. 17th ed. São Paulo: Paz e Terra, 2016.

CENTRE FOR SECURITY AND EMERGING TECHNOLOGY (CSET). Understanding AI Harms: An Overview. Available at: https://cset.georgetown.edu/article/understanding-ai-harms-an-overview/. Accessed: August 06, 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: August 6, 2024.

KORKMAZ, Maria Regina Rigolon. *Decisões Automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomsom Reuters Brasil, 2023.

LUHMANN, Niklas. *Risk: A Sociological Theory*. New York: Routledge, 1993.

MCCARTHY, John. *Proposta para o 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: 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: 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: August 07, 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. Accessed: August 07, 2024.

EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of August 9, 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://eur-lex.europa.eu/eli/reg/2024/1689. Accessed: October 06, 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

6

Bill 2.338/2023: A Study of Its Copyright Provisions

NINA RAMALHO PINHEIRO

Contents: Introduction. 1. The Copyright Law (Law No. 9.610/1998) and key concepts: protected works, moral and economic rights, and limitations. 2. Copyright and related rights in light of the 4th substitute text of Bill 2.338/23 and the proposed amendments. 2.1. Rights of rights holders and copyright limitations. 2.2. Remuneration. 2.3. Transparency and the regulatory sandbox. 2.4. Personality rights and use of images. Final considerations. References.

Introduction

Advances in the development and use of artificial intelligence (AI) systems are evident globally, and the rapid incorporation of this technology into a wide range of fields brings regulatory challenges involving issues such as competitiveness, the risk of economic concentration, and impacts on employment/work.

The need to establish clear rules for developing and applying the technology safely, responsibly, and sustainably, while respecting fundamental rights, gives rise to different regulatory models (e.g., general/sectoral, principles-based, vertical/horizontal) based on the strategies of each national policy.

In Brazil, although there were earlier initiatives [2], the debates on the subject took more definite shape with Bill 21/2020, authored by representative Eduardo Bismarck, culminating in 2022 in the formation of the Federal Senate's Commission of Legal Experts to prepare a draft substitute text to inform the regulation of artificial intelligence in the country [3].

The Commission's work (CJUSBIA) marks significant progress in structuring legal guidelines for AI in Brazil. Following public hearings and consultations with more than fifty experts from different sectors (government, business, civil society, and academia), a proposed substitute text was presented and became Bill No. 2338/2023 [4].

1. Bachelor of Laws from the Pontifícia Universidade Católica de São Paulo (PUC/SP). Holds a postgraduate qualification in Civil Procedure from FGV Direito SP (FGV LAW). A postgraduate student in Digital Law at the Instituto de Tecnologia e Sociedade (ITS Rio), in partnership with the Universidade do Estado do Rio de Janeiro (UERJ) and the Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). An attorney in Strategic Litigation, focusing on issues involving Digital Law, Technology, and Data Protection. Contact: nina.rpinheiro@gmail.com.

2. For example: Bills 5051/20219 and 5691/2019, which establish general principles for AI use.

3. Following consideration 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: July 15, 2024.

Bill No. 2338/2023 can be interpreted as progress because it reflects a long process of multistakeholder discussion and sought to reconcile a risk-based regulatory approach [5] with the protection of fundamental rights, without ignoring the promotion of innovation and agents' accountability.

Despite this progress, numerous points have continued to be refined and debated through Technical Notes [6] issued by organizations representing society and contributions at public hearings. As a result, by November 2024, 150 proposed amendments and four substitute texts had been presented in the Federal Senate.

Among the issues generating the greatest disagreement and uncertainty is copyright protection in the development and use of artificial intelligence systems, especially generative AI. To date, the subject has been addressed by nineteen amendments [7], of which two were accepted [8], one was partially accepted [9], one was withdrawn by its author [10], and fifteen were rejected [11].

From this perspective, the main objective of this study is to analyze these amendments, their stated justifications, the arguments for their approval or rejection, and changes to the wording of the related articles in Bill 2.338/23, in order to identify the main points of discussion for improving regulation concerning copyright protection.

To this end, the primary research material consists of amendments addressing copyright, compared with the articles of "Section IV – Copyright and related rights" of the 4th substitute text of Bill 2.338/23, dated November 28, 2024. The secondary material consists of guidance applicable to the subject, specific legislation, foreign regulatory experience, supporting literature, and technical notes issued by competent organizations. From the primary material, we sought to extract the broad themes addressed, here called "points," which will be analyzed individually based on the identified research questions and possible solutions, considering the secondary material analyzed.

5. LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET (LAPIN). Projeto de Lei nº 2338/2023 - Nota Técnica. August 2023. Available at: https://direitosnarede.org.br/2023/08/23/coalizao-direitos-na-rede-divulga-nota-tecnica-sobre-o-pl-2338-2023-que-busca-regular-a-ia/. Accessed: 13/07/2024.

6. For example: IDEC, ANDP, Coalizão Direitos na Rede.

7. Amendments No. 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 No. 6, 20, 36, 40, 55, 56, 61, 72, 102, 103, 109, 110, 112, 118, 119, 128.

To present the study, we chose to address, in the first chapter, essential definitions for understanding its scope by mapping the Copyright Law (Law No. 9.619/98, or “LDA”), such as protected work, moral and economic rights, and related rights. This chapter also presents basic artificial intelligence concepts, introducing the definition of model training and data and text mining. In the second chapter, the four points selected through analysis of the primary research material—namely (i) rights of rights holders and copyright limitations, (ii) remuneration, (iii) transparency and the regulatory sandbox, and (iv) personality rights and use of images—are addressed based on the wording of the articles in the Bill’s 4th substitute text and the related amendments submitted. The study concludes with an assessment of advances and uncertainties surrounding the subject and future prospects for addressing the challenges identified.

1. The Copyright Law (Law No. 9.610/1998) and key concepts: protected works, moral and economic rights, and limitations

Before analyzing the provisions of Bill 2.338/23 that seek to establish a framework for copyright in artificial intelligence, it is important to briefly discuss the specific legislation applicable to the subject, in order to provide essential definitions for understanding the points addressed in the Bill.

In Brazil, copyright and related rights protection is established in the Copyright Law (Law No. 9.619/98). To understand the object of copyright protection, Article 7 of the LDA [12] indicates that creations of the mind expressed through any medium or support are protected, regardless of whether they relate to literature, the arts, or science. From the legal provision, it is clear that concepts, styles, or ideas are not protected, but only the external expression of these elements.

12. Article 7. Protected intellectual works are creations of the mind expressed through any medium or fixed in any tangible or intangible support, known or invented in the future, such as: I - texts of literary, artistic, or scientific works; II - lectures, speeches, sermons, and other works of the same nature; III - dramatic and dramatic-musical works; IV - choreographic and pantomimic works whose stage performance is fixed in writing or in any other manner; V - musical compositions, with or without lyrics; VI - audiovisual works, with or without sound, including cinematographic works; VII - photographic works and works 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, drafts, and visual works concerning geography, engineering, topography, architecture, landscaping, scenography, and science; XI - adaptations, translations, and other transformations of original works presented as a new intellectual creation; XII - computer programs; XIII - collections or compilations, anthologies, encyclopedias, dictionaries, databases, and other works that, through the 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 copyright legislation and makes other provisions.) Available at: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Accessed: July 3, 2024.

Although the legislation is not explicit and opposing views exist, the prevailing legal scholarship also supports originality as a requirement for a work to receive legal protection. As Sérgio Branco [13] cautions, this originality should not be confused with “absolute novelty,” but understood as the element capable of distinguishing a particular work from others through the author’s intellectual and creative effort.

Beyond these points, protection of a work must also observe the protection term established by law, currently limited to 70 years from January 1 of the year following milestones such as death (works in general), publication (anonymous, pseudonymous, or posthumously published works), and disclosure (collective, audiovisual, and photographic works), after which the work enters the public domain.

Although Article 7 of the LDA lists types of protected works, given their mutability due to external factors such as cultural issues and technological development, specialist legal scholarship maintains that the list is illustrative. Thus, a work will receive copyright protection if the essential requirements presented here are met.

Beyond the object of protection, the LDA establishes that protected works need an author responsible for holding creative control over the work [14]. Under Article 11 of the LDA, the author is the “natural person who creates a literary, artistic, or scientific work.”

As Luca Schirru [15] raises, 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 Guilherme Carboni [16] aptly observes, stems from the Romantic conception reflected in the Berne Convention (1886). On the assumption that works were a true extension of their creator’s personality, this justified granting exclusive rights over works to the author as a natural person.

13. BRANCO, Sérgio. Direitos autorais na Internet e o uso de obras alheias. Rio de Janeiro: Lumen Juris, 2007. Available at: https://repositorio.fgv.br/items/9d286b3c-c77e-46f2-ad95-1bc48debd48c. Accessed: July 13, 2024.

14. CANTALI, Fernanda Borghetti. Inteligência artificial e direito de autor: tecnologia disruptiva exigindo reconfiguração de categorias jurídicas. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência. Porto Alegre. v. 4. pp. 1–21. July/December 2018. Available at: https://www.indexlaw.org/index.php/revistadipic/article/view/4667/pdf. Accessed: July 20, 2024.

15. SCHIRRU, Luca. Direito autoral e inteligência artificial: autoria e titularidade nos produtos da IA. Thesis (Doctorate in Public Policy, Strategies, and Development) - Instituto de Economia, Universidade Federal do 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. Accessed: July 13, 2024.

16. CARBONI, Guilherme. Direito Autoral, Diversidade das Expressões Culturais e Pluralidade de Autorias. In: Direito da Propriedade Intelectual, Vol II: estudos em homenagem ao Pe. Jorge Hammes (edited by Luiz Gonzaga Silva Adolfo and Marcos Wachowicz). Curitiba: Juruá. 2014.

To understand the exclusivity of the rights granted to authors, it is essential to define the nature of these rights. Although this is not an undisputed understanding, the LDA adopted the dualist theory, which provides for two distinct categories of rights over a work: moral rights and economic rights.

Moral rights, addressed in Articles 24, 25, 26, and 27 of the LDA, would result from the projection of the author's personality into the work [17] because of the indissoluble bond [18] between them. In this context, they reflect the author's relationship with the work itself and encompass the right to attribution of authorship [19], control over circulation [20], and modification of the work [21].

Although conceptualizing authors' moral rights as personality rights [22] is questionable, since they are not innate to individuals and arise only upon the creation of a protected work, under Article 27 of the LDA these rights are also inalienable, unwaivable, not subject to limitation periods, and immune from attachment.

Economic rights, in turn, which may be traded and transferred for payment or free of charge, partially or in full, concern forms of economically exploiting the work through the author's or rights holder's [23] powers to use, enjoy, and dispose of it before it enters the public domain.

As Eliane Abrão [24] argues, these rights can also be considered exclusive, since under Article 28 of the LDA, the forms of using a work listed in Article 29—including reproduction, publication, adaptation, translation, distribution, and inclusion in a database—depend on the author's/rights holder's prior express approval.

In addition to copyright, Articles 89 to 96 of the LDA establish related rights to ensure artists' participation and remuneration in future uses of a work in which they participated. This includes the rights of

17. SOUZA, Allan Rocha de. Direitos morais do autor. Civilistica.com. Rio de Janeiro, year 2, no. 1, January–March/2013. Available at: https://civilistica.emnuvens.com.br/redc/article/view/73/53. Accessed: July 27, 2024.

18. STAUT JÚNIOR, Sérgio Said. *Direitos Autorais: entre as relações sociais e as relações jurídicas*. Moinho do Verbo. Curitiba. 2006.

19. The right to claim authorship of a work and have one's name or pseudonym credited (Article 24, I and II, LDA).

20. The right to keep a work unpublished and to withdraw it from circulation (Article 24, III and VI, LDA).

21. Aiming to ensure the work's integrity in relation to third parties, while granting the author the possibility of modifying it even after it has been put into circulation (Article 24, IV and V, LDA).

22. BRANCO, Sérgio. PARANAGUÁ, Pedro. Direitos Autorais. 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: July 13, 2024.

23. Given the possibility of transferring rights, the rights holder will not always be the author of the work and may assume original ownership through legal transactions, death, or a legal provision.

24. ABRÃO, Eliane. *Direitos de autor e direitos conexos*. São Paulo: Ed. do Brasil, 2002.

performing artists, phonogram producers, and broadcasting companies regarding the interpretation, performance, or dissemination of a work.

As 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 performances/broadcasts; making them available to the public for access at any time and place; and any other form of using their interpretations or performances.

Although they protect the author of a work, including as a way to encourage diversity and the creative economy, the rights and protection granted by the LDA are not absolute. They are qualified by the public interest and the promotion of other fundamental rights (e.g., culture, accessibility, education) under Articles 46, 47, and 48 of the law.

These provisions establish situations in which use of a protected work is permitted without the author's/rights holder's prior authorization, without this constituting a violation of the law or third parties' rights. For example, brief passages from a literary work may be quoted in an academic book for criticism or study; educational institutions may reproduce portions of works exclusively for teaching activities; news or informative articles may be reproduced in the press; and paraphrases and parodies are permitted if they are not actual reproductions of the original work and do not discredit it, among other examples.

In the context of copyright protection applied to the use, development, and training of artificial intelligence systems, interpreting these limitations and whether their list is exhaustive proves relevant.

Although not unanimous [25], a broad interpretation of legal limitations in light of the Federal Constitution has gained strength as a way to reflect technological evolution, encompass new forms of creation, and overcome the apparent obsolescence of current legislation [26].

To understand the provisions addressed in "Section IV – Copyright and related rights" of the 4th substitute text of Bill 2.338/23, it is also relevant to understand concepts such as an artificial intelligence system, an AI developer and agent, and the process of text and data mining.

25. Authors such as Carlos Alberto Bittar and Plínio Cabral advocate a restrictive interpretation of the limitations.

26. SCHIRRU, Luca. Direito autoral e inteligência artificial: autoria e titularidade nos produtos da IA. Thesis (Doctorate in Public Policy, Strategies, and Development) - Instituto de Economia, Universidade Federal do 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. Accessed: July 13, 2024.

In the draft regulation, an AI system is defined [27] as a machine-based system with varying degrees of autonomy, capable of inferring from a set of data and information and generating outputs such as predictions, recommendations, or decisions.

To perform their functions, most artificial intelligence systems consist of algorithms capable of learning from a database (machine learning) [28], sometimes processing these data in a manner similar to neural networks (deep learning) [29].

Regardless of how a system operates and learns, the success and accuracy of predictions, recommendations, and decisions depend on a large volume of input data used to train algorithms, identify meaningful patterns, and improve system performance.

In this context, text and data mining (TDM [30]), an automated technique for extracting large volumes of data directly or through other tools to identify patterns and correlations [31], becomes relevant. Information extracted from immense amounts of data [32] provides insights for use in research, development, or application in artificial intelligence systems.

From a copyright perspective, although some defend the legality of text and data mining even without an express legal provision, because it involves a nonexpressive use through which factual elements and patterns [33]—not protected by copyright—are extracted

27. Article 4 [...] I – artificial intelligence system: a machine-based system that, with varying degrees of autonomy and for explicit or implicit objectives, infers from a set of data or information it receives how to generate outputs, particularly predictions, content, recommendations, or decisions 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: November 29, 2024.)

28. In the original: “Machine Learning: algorithms that analyze data, learn from them, 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, December 5, 2019, freely translated in the source). Available at: https://www.ibm.com/blog/ai-machine-learning-and-deep-learning-whats-the-difference/. Accessed: July 13, 2024.

29. In the original: “Deep Learning: neural network algorithms that learn on their own about the relevant features of data. Able to adapt through repeated training to discover hidden patterns and insights” (CERON, Rodrigo. AI, machine learning and deep learning: What’s the difference? IBM, December 5, 2019, freely translated in the source). Available at: https://www.ibm.com/blog/ai-machine-learning-and-deep-learning-whats-the-difference/. Accessed: July 13, 2024.

30. Text and Data Mining.

31. Article 4 [...] XIII - text and data mining: a highly automated process of extracting and analyzing large amounts of data, carried out directly on primary data or indirectly through another tool, from which patterns and correlations are extracted to generate information relevant to researching, developing, or using 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: November 29, 2024)

32. ROCHA, Maria Victória. Prospeção de texto e dados (text and data mining) na diretiva relativa aos direitos de autor e direitos conexos no mercado único digital. RRDDIS – Revista Rede de Direito Digital, Intelectual & Sociedade, Curitiba, v. 2, no. 4, pp. 99-164, 2022, p. 103. Available at: https://revista.ioda.org.br/index.php/rrddis/article/view/76/45. Accessed: July 16, 2024.

33. SOUZA, Allan Rocha de. SCHIRRU, Luca. Alvarenga. MIGUEL BARROS. Mineração de textos e dados na pesquisa em saúde: reflexões sobre direitos autorais. Cadernos de Saúde Pública 2024. Available at: https://cadernos.ensp.fiocruz.br/ojs/index.php/csp/article/view/8597/19335. Accessed: July 27, 2024.

– considering that databases (Article 7, XII, XIII, paragraph 2, LDA) and protected works are accessed, an express legal provision on the applicable limitation is important to ensure legal certainty.

In this context, reflecting international legislative experiences such as copyright reforms in Japan [34], Singapore [35], and Israel [36], Brazil's Bill 2.338/23 recognizes the inadequacy of the limitations in Article 46 of the LDA. Even with a broad interpretation, these limitations refer only to reproducing works for specific purposes and do not encompass other forms of use necessary for TDM. The Bill therefore proposes a specific limitation for this activity, seeking to balance and make the exclusivity of the copyright system more flexible in the public interest.

To comply with the obligations in Bill 2.338/23, it is important to understand to whom the law applies. Under Article 4, VIII of the 4th substitute text of Bill 2.338/23, artificial intelligence agents, which may be natural persons or legal entities under public or private law, are developers (Article 4, V) [37], distributors (Article 4, VI) [38], and deployers (Article 4, VII) [39] operating in the value chain and internal governance of artificial intelligence systems.

Despite current legislation, the dynamism of AI technology development exposes gaps that raise questions about the application and adequacy of existing mechanisms for copyright protection. Recognizing these gaps, Bill 2.338/23 and its proposed amendments seek to build regulation that considers the new reality and balances public and private interests. To examine the compatibility of the regulatory suggestions for protecting authors without making technological progress unviable, the next chapter will analyze the proposed legislative update from the perspectives of rights holders' rights, copyright limitations, remuneration arrangements, the duty of transparency and the regulatory sandbox, and personality rights and use of images.

34. In Japan, copyright law was adjusted to allow data mining for research purposes, including AI development, without needing to obtain rights holders' prior consent.

35. In Singapore, the Copyright Act 2021 includes a data mining exception allowing protected works to be used for computational analysis, including AI development, without rights holders' prior authorization.

36. Israel permits the use of data for AI under conditions ensuring privacy and security but does not impose severe restrictions on using protected data for AI training.

37. Responsible for developing the artificial intelligence system (from creation, training, and implementation to improvement), directly or by commission, with a view to placing it on the market or using it in a service they provide, under their own name or brand, for payment or free of charge.

38. Responsible for making the AI system available and distributing it for a third party to operate, for payment or free of charge.

39. Responsible for employing or using the artificial intelligence system in their name or for their benefit, including for configuration, maintenance, or support through providing data for the AI system's operation and monitoring.

2. Copyright and related rights in light of the 4th substitute text of Bill 2.338/23 and the proposed amendments

Although guidelines for aligning copyright with data access for machine training and artificial intelligence system development have been a concern since the CJUSBIA's final report, which became the initial text of Bill No. 2.338/2023, relevant advances have already been made following analysis of numerous proposed amendments on the subject. Accordingly, this study will present the main copyright-related "points" in Bill 2.338/23 based on the wording of its 4th substitute text, dated November 28, 2024, which also began to recognize copyright protection as one of the law's foundations, alongside intellectual property and commercial and industrial secrecy.

2.1 Rights of rights holders and copyright limitations

Articles 63 and 64 of the 4th substitute text of Bill 2.338/23 address the limitations and main rights of copyright and related rights holders, such as the right to prohibit the use of content they own in developing AI systems [40].

As seen, considering that Articles 46 to 48 of the LDA, even if broadly interpreted, do not establish clear copyright limitations for text and data mining processes to develop, train, and use AI systems, Article 63 of the 4th substitute text of Bill 2.338/23 introduces an innovation by providing copyright exceptions that qualify the right to prohibit use established in Article 64, aligning with international practices and responding to contemporary research and technological development needs.

However, to preserve authors' interests, especially economic interests, the exception is limited to situations in which the public interest prevails. Use is permitted by educational, research, and journalism organizations and institutions, museums, archives, and libraries [41], provided that access was obtained lawfully (item I), the use has no commercial purpose

40. Article 64. Copyright and related rights holders may prohibit the use of content they own in developing AI systems in situations not covered by Article 61 of this Law, as regulated. Sole paragraph. Prohibiting the use of protected works and content in an AI system's databases after training does not exempt the AI agent from liability for moral and material damages under applicable legislation.

41. Article 63. Automated use of protected content in text and data mining processes for researching or developing AI systems by research, journalism, museum, archive, library, and educational organizations and institutions does not constitute infringement of copyright and related rights, provided that the following conditions are observed:

(item II), the activity does not aim to reproduce, display, or disseminate the original work (item III), and use is undertaken only to achieve its objective without harming rights holders' economic interests or competing with the normal exploitation of protected works and content (item IV).

Of these requirements, perhaps the one raising the most questions is the prohibition on commercial purposes arising from mining. As discussed by Miguel Bastos Alvarenga [42], it is important to remember that even research activity may result in publications offered for sale. Tying the exception to a strictly noncommercial purpose could therefore affect the dissemination of scientific work and compromise various research activities.

On this point, the prohibition on commercial purposes is understood to require further refinement through assessing whether prohibiting interference with the normal exploitation of the work to the detriment of the rights holder's economic interests is sufficient, particularly since Article 46 of the LDA itself permits exceptions involving profit-making purposes [43].

Beyond these points, the legal provision also establishes duties concerning security and appropriate retention periods for any copies of protected content used in AI system training (paragraph 1), and extends its application to the use of mining processes in artificial intelligence systems to combat civil and criminal infringements of copyright and related rights (paragraph 3) [44].

Although the provisions allow works to be used for mining and artificial intelligence in certain contexts, it is important to emphasize that the Bill does not authorize use broadly. It grants rights holders the right to object to use even when their economic interests are not actually harmed. This prohibition, stricter than in other international legislation, may represent a barrier to investment and technological progress in the country, with impacts on competitiveness. For this reason, further discussion and assessment are also considered important, for example of mandatory compensation mechanisms to protect rights holders' interests without the possibility of prohibiting use

42. ALVARENGA, Miguel Bastos. Mineração de dados, Big Data e Direitos Autorais no Brasil. Thesis (Master's in Public Policy, Strategies, and Development) - Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2019. p. 92. Available at: https://onda.org.br/resources/2020_Miguel%20ALVARENGA_Mest.pdf. Accessed: July 27, 2024.

43. "Article 46. The following does not constitute copyright infringement: I - reproduction: (...) V - the use of literary, artistic, or scientific works, phonograms, and radio and television broadcasts in commercial establishments exclusively for demonstration to customers, provided that those establishments sell the media or equipment that enable their use."

44. It is understood that, for use for this purpose, the requirements in the items of Article 63 do not apply.

in cases where there is no harm to rights holders' economic interests or competition with the normal exploitation of protected works [45].

2.2 Remuneration

One of the greatest concerns raised by AI tools involves guaranteeing remuneration to rights holders for the appropriation of their productions to develop and train AI models.

Until the 2nd substitute text of Bill 2.338/23, dated June 18, 2024, rights holders' remuneration for the use of protected content to train and develop artificial intelligence systems was subject to creating an experimental regulatory environment (sandbox) to discuss remuneration models.

Only with the wording of the 3rd substitute text was the duty to remunerate established in law. Article 65 of the 4th substitute text provides that "an AI agent that uses content protected by copyright and related rights in mining, training, or developing AI systems must remunerate the respective rights holders for that use."

Regarding the right to remuneration, it is important to mention the rejection on 04/07/2024 of amendments 56 [46], 61 [47], and 72 [48]. These sought, respectively, (i) the precedence of a final fixed-price offer to be set by the Sectoral Authority or the Private Arbitration Chamber if negotiations between AI agents and copyright and related rights holders proved unfeasible; (ii) deletion of the copyright-related provisions; and (iii) dispensing with prior authorization for AI system development, with possible remuneration to rights holders. Their rejection was based on the reasoning that guaranteeing rights to the creative industry is important to encourage responsible innovation and protect the fruits of the human mind.

Although some [49] argue that remuneration for economically exploiting protected works is already supported by the Federal Constitution of 1988 [50] and the LDA, making it redundant to address the issue in artificial intelligence legislation, Bill 2.338/23 recognizes specific features in the AI context that do not fit the forms of use provided for in

45. A situation more likely to arise in cases involving generative AI systems.

46. Authored by Senator Weverton, submitted on 18/06/2024.

47. Authored by Senator Astronauta Marcos Pontes, submitted on 18/06/2024.

48. Authored by Senator Astronauta Marcos Pontes, submitted on 18/06/2024.

49. Amendments 61 and 72 seeking to delete articles affecting copyright are examples of this.

50. Article 5, XXVII of the
Federal Constitution.

the LDA [51]. Therefore, providing for remuneration in these situations is crucial to curb abuses arising from ambiguities and the obsolescence of current legislation, and to clarify how this right will be exercised in the new technological context involving the use of large volumes of data.

On this subject, the paragraphs and items of Article 65 of the Bill's 4th substitute text provide that remuneration will be due to rights holders domiciled in Brazil or in countries ensuring reciprocal protection (item V, subitems a and b), only when AI systems are commercially made available (item IV), with the possibility of deferred payment deadlines for startups and small businesses (item VI), ensuring: (i) the ability to negotiate directly or collectively, for payment or free of charge (item I), with direct negotiation not dependent on regulation (paragraph 2); (ii) that the amount considers the AI agent's economic power, the degree of content use and competitive effects in relation to the original content, the AI system's complexity, the economic realization cycle, and the work's relative value over time (item II); (iv) free negotiation, promoting a research and experimentation environment without restricting freedom of contract (item III).

That is, subject to the limitations introduced by Article 63, provided that prior use of content owned by the rights holder has been authorized, the rights holder must be remunerated by the AI agent using their works.

Although the provision responds to the creative industry's concerns, its current wording is considered insufficient to guarantee the desired legal certainty, particularly because it refers generically to the duty of "artificial intelligence agents." It is important to delimit to what extent and on which agent the duty to remunerate will fall, to remove doubts arising from multiple agents' involvement in the AI system lifecycle. The criteria for calculating remuneration are subjective, making practical application difficult. More objective criteria are needed to measure "economic power," "degree of use," "competitive effects," "AI system complexity," "economic realization cycle," and "the work's value over time," in order to guide negotiations without ignoring freedom of contract.

Beyond these points, while the importance of mechanisms to protect copyright and related rights holders is recognized, especially from an economic perspective and regarding the use of works by generative AI systems—with greater potential for competitive

51. Indeed, it creates an exception for using works to mine, train, and develop AI systems.

impacts and harm to authors' interests—the technical difficulty of controlling and obtaining prior authorization for data use raises concerns, including in view of the importance of training models on Brazilian content to reflect nuances and ensure appropriate application in the country. From this perspective, including to preserve Brazil's competitiveness and sovereignty in the global AI landscape, further discussion and assessment of alternatives such as collective compensation funds and compulsory licensing at a standard rate become relevant.

2.3 Transparency and the regulatory sandbox

Transparency is crucial to enable rights holders' oversight and ensure the effective exercise of the rights to prohibit and receive remuneration for the use of their works.

Although Digital Rights Management (DRM) technologies, blockchain, digital marks, and watermarks can be employed to control and monitor access to and use of works, placing the burden of control and oversight on rights holders could make the full exercise of rights unviable. Accordingly, Article 62 of the 4th substitute text of Bill 2.338/23 requires AI developers using content protected by copyright and related rights to make public what content was used in AI system training, by publishing a summary on an easily accessible website or as provided for in regulations.

Limiting responsibility to the AI developer, following acceptance of amendment 44 [52], represents significant progress. This not only clarifies who must comply with the legal obligation but also reflects the fact that, as the system's "creator," the developer is best positioned to monitor and report the use of copyright- and related-rights-protected content. By simplifying the chain of responsibility, the provision also reduces costs associated with other AI agents' compliance with legal obligations, encouraging competitiveness and innovation.

Although the assignment of responsibility is unequivocal, how this obligation will be implemented still raises numerous questions, particularly regarding the technical feasibility of listing all content accessed and obtaining prior authorization for its use when the exceptions in Article 63 do not apply.

52. Authored by Senator Chico Rodrigues, proposed on 17/06/2024.

Precisely for this reason, the provision's effectiveness depends on regulation of the subject, which may draw on experiences gathered in an experimental regulatory environment (sandbox) established by the National Artificial Intelligence Regulation and Governance System (SIA) and the competent sectoral body [53], under Chapter X, Section I of the 4th substitute text.

This environment, initially referenced specifically in Section IV of the Bill, devoted to copyright and related rights, was originally intended to address both transparency and remuneration until the 2nd substitute text. In the 3rd substitute text, its scope was narrowed to transparency alone, and finally, in the 4th substitute text, it was removed from this section entirely.

In this context, although creating a regulatory sandbox to test and adapt rules to ensure transparency in the use of protected works aligns with international experiences, it is crucial to consider the risk of abuse and rights violations in this more flexible environment, which may have justified its exclusion from Section IV.

Nevertheless, the difficulty of implementing transparency measures and the uncertainties arising from the lack of specific regulation deserve attention. Any discussion of the duty of transparency within an experimental regulatory environment must be preceded by clear definition of the sandbox's parameters and limits, together with robust oversight mechanisms and the involvement of all stakeholders, to ensure that regulatory flexibility does not compromise copyright protection.

2.4 Personality rights and use of images

Article 66 of the 4th substitute text of Bill 2.338/23 provides that the use of images, audio, voice, or video portraying or identifying people must respect personality rights under the Civil Code and relevant legislation.

As a way to combat disinformation caused, for example, by deepfakes, Article 19 also deserves attention. It requires synthetic content generated by AI systems to be identified so that its authenticity and the characteristics of its provenance, modifications, and transmission can be verified. This provision reflects the incorporation of generative artificial intelligence rules contemplated in Bill No. 3.592 of 2023; Bill No. 145

53. Before the 3rd substitute text, the exclusive responsibility of the sectoral authority, after hearing the competent central body, and of the SIA had been advocated. In this regard, amendment 45, authored by Senator Chico Rodrigues and partially accepted, argued that the integrity of sandbox decision-making by the sectoral authority would be compromised because, being composed of departments and federal bodies within the direct administration, the authority could face political interference.

of 2024; and Bill No. 146 of 2024—incorporated into the text of Bill 2.338/23 to harmonize the various initiatives on the subject—and acceptance of amendment No. 4 [54].

Regarding the provisions relating to personality rights, the Bill has been criticized for apparent redundancy with provisions of the Civil Code, the LDA, and the LGPD.

In this regard, as can be seen from the justifications for proposed amendments No. 61, 72, 109, and 128, some provisions of the new rules would actually reaffirm what is already addressed in the Civil Code, specifically Articles 11 and 20 [55]. These protect personality rights, ensuring that the use of a person's image, voice, and other personal attributes may occur only with authorization or in specific situations, such as maintaining public order.

Similarly, Brazilian copyright legislation is said already to contain mechanisms to protect authors' rights regarding the use of their works by AI systems [56]. Articles 29 and 31 provide that any use, transformation, or adaptation of a copyright-protected work—such as creating derivative content through generative AI—requires the rights holder's express authorization. These provisions would therefore be sufficient to address most problems raised by AI use relating to the modification or generation of derivative content from protected works, such as images, voices, or texts, even if used only for system training.

Furthermore, as noted by the ANPD [57], Bill 2.338/23 and the LGPD intersect regarding the collection and use of personal data and the exercise of data subjects' rights [58], so creating a new regulatory authority responsible for overseeing AI system use could generate regulatory fragmentation.

54. Authored by Senator Vanderlan Cardoso, submitted on 18/04/2024, proposing the inclusion of identifying marks in content generated or manipulated by artificial intelligence.

55. Article 11. Except in cases provided for by law, personality rights are nontransferable and unwaivable, and their exercise may not be voluntarily limited.
Article 20. Unless authorized or necessary for the administration of justice or maintenance of public order, the disclosure of writings, transmission of speech, or publication, display, or use of a person's image may be prohibited at their request, without prejudice to any compensation due, if they affect the person's honor, good reputation, or respectability, or are intended for commercial purposes. Sole paragraph. In the case of a deceased or absent person, the spouse, ascendants, or descendants have standing to request this protection.

56. See Technical Note No. 2/2024 of the General Coordination for Copyright Regulation at the Ministry of Culture. Available at: https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJlqCNXRK_Sh2SMdn1U-tzNsXmaDPgth6TWQbVegDsJUpxKCGrIfpqgd2LPweVjfrVUs865P0Y_aohlycyNue1ge1wXB9NlS-a8VWrNBh-Xw. Accessed: 13/10/24.

57. See Technical Note No. 16/2023/CGTP/ANPD: Suggestions for legislative input on bills concerning Artificial Intelligence regulation in Brazil, focusing on Bill No. 2338/2023.

58. For example, the rights to information, an explanation, and requesting a review could be subject to simultaneous regulation and supervision.

From this perspective, to achieve greater harmony with current legislation and avoid overlap or inconsistent application of the new law, it is advisable to delimit scenarios and include guidelines specifically addressing AI use [59] in the context of copyright and personality rights, such as clear mechanisms for authors' authorization and compensation when their works are used to train models.

Final considerations

This study first addressed definitions based on applicable copyright legislation and subsequently mapped the related provisions in Bill 2.338/23 regulating copyright and related rights in AI. Through analysis of legislative definitions, specialist legal scholarship, the text of the Bill's 4th substitute text, and the proposed amendments, four main points addressed by the new rules were identified, along with issues requiring further refinement and possible adjustments to the current wording.

In conclusion, although Bill No. 2338/2023 is an important milestone in balancing protection of authors' rights with the promotion of technological innovation and the integration of artificial intelligence, significant uncertainties remain regarding the application and effectiveness of the proposed measures. The complexity of establishing protection for authors' rights without making mining activities and the use of protected content for system development and training unviable highlights the challenges faced. Issues such as fair remuneration, transparency in use, and implementation of licensing models also depend on more detailed provisions for effective practical application.

To ensure that legislation keeps pace with technological innovation without becoming an obstacle to the country's development and competitiveness, while also promoting a robust oversight system capable of ensuring respect for copyright and related rights, it is essential that debates on rights holders' rights, copyright limitations, and guarantees of transparency and remuneration continue to

59. In contrast to delimiting specific situations, it is worth mentioning the rejection, on the grounds that the Bill confines artificial intelligence rules to Civil Law in a general, principles-based manner, of amendments No. 20, 102, 103, and 112. These addressed, respectively, criminalizing deepfakes in the Penal Code; indicating AI use in advertising; rules for commercial use through AI of a deceased person's image and audio; and excluding the requirement to identify synthetic content in artistic and literary works created for cultural purposes where editorial responsibility exists.

mature, with equitable multistakeholder participation and attention to international experiences. Bringing the subject into debate enriches the legislative process by allowing diverse perspectives to be gathered and controversies mapped.

Since the Bill is still under discussion, this study remains open to further development, for example by comparing the final text of the approved regulation with the wording analyzed here.

References

ABRÃO, Eliane. *Direitos de autor e direitos conexos.* São Paulo: Ed. do Brasil, 2002.

ALVARENGA, Miguel Bastos. Mineração de dados, Big Data e Direitos Autorais no Brasil. Thesis (Master's in Public Policy, Strategies, and Development) – Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2019. p. 92. Available at: https://onda.org.br/resources/2020_Miguel%20ALVARENGA_Mest.pdf. Accessed: July 27, 2024.

BITTAR, C.A. Direito de Autor. 5th ed., revised, updated, and expanded by Eduardo C.B. Bittar. Rio de Janeiro: Forense, 2013.

BRANCO, Sérgio. Direitos autorais na Internet e o uso de obras alheias. Rio de Janeiro: Lumen Juris, 2007. Available at: https://repositorio.fgv.br/items/9d286b3c-c77e-46f2-ad95-1bc48debd48c. Accessed: July 13, 2024.

BRANCO, Sérgio. PARANAGUÁ, Pedro. Direitos Autorais. 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: July 13, 2024.

BRAZIL. National Data Protection Authority. Preliminary analysis of Bill No. 2338/2023, which provides for the use of Artificial Intelligence. Brasília, 2023. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf. Accessed: July 27, 2024.

BRAZIL. National Data Protection Authority. Technical Note No. 16/2023/CGTP/ANPD: Suggestions for legislative input on bills concerning Artificial Intelligence regulation in Brazil, focusing on Bill No. 2338/2023. Brasília, 2023. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Accessed: 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 makes other provisions. Brasília: Chamber of Deputies, 2020. Available at: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340&fichaAmigavel=nao. Accessed: July 20, 2024.

BRAZIL. Coordination of Special, Temporary, and Parliamentary Inquiry Committees. Final report of the Commission of Legal Experts responsible for informing the drafting of a substitute text on artificial intelligence in Brazil. Available at: https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4. Accessed: July 20, 2024.

BRAZIL. Federal Senate. Bill No. 5691 of 2019. Establishes the National Artificial Intelligence Policy to encourage an environment favorable to developing Artificial Intelligence technologies. Brasília: Federal Senate, 2019. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/139586. Accessed: July 20, 2024.

BRAZIL. Federal Senate. Bill No. 5051 of 2019. Establishes principles for the use of Artificial Intelligence in Brazil. Brasília: Federal Senate, 2019. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/138790. Accessed: July 20, 2024.

BRAZIL. Federal Senate. Bill No. 872 of 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: 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: November 29, 2024.

CABRAL, Plinio. A Nova Lei de Direitos Autorais. 4th edition. Editora Harbra. 2003.

CANTALI, Fernanda Borghetti. Inteligência artificial e direito de autor: tecnologia disruptiva exigindo reconfiguração de categorias jurídicas. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência. Porto Alegre. v. 4. pp. 1–21. July/December 2018. Available at: https://www.indexlaw.org/index.php/revistadipic/article/view/4667/pdf. Accessed: July 20, 2024.

CARBONI, Guilherme. Direito Autoral, Diversidade das Expressões Culturais e Pluralidade de Autorias. In: Direito da Propriedade Intelectual, Vol II: estudos em homenagem ao Pe. Jorge Hammes (edited 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: July 13, 2024.

EUROPEAN PARLIAMENT NEWS. What is artificial intelligence and how is it used? September 4, 2020. Available at: https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used. Accessed: July 13, 2024.

INSTITUTO DE DEFESA DE CONSUMIDORES (IDEC). Contribuição do Idec ao Substitutivo da CTIA ao Projeto de Lei 2.338/2023 (Inteligência Artificial). May 2024. Available at: https://idec.org.br/sites/default/files/2024_idec_-_analise_do_substitutivo_ao_pl_2338_23_-_inteligencia_artificial_08.05.2024_.docx.pdf. Accessed: July 13, 2024.

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET (LAPIN). Projeto de Lei nº 2338/2023 – Nota Técnica. August 2023. Available at: https://direitosnarede.org.br/2023/08/23/coalizao-direitos-na-rede-divulga-nota-tecnica-sobre-o-pl-2338-2023-que-busca-regular-a-ia/. Accessed: 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?yPDszXhdoNcWQHJaQlHJmJlqCNXRK_Sh2SMdn1U-tzNsXmaDPgth6TWQbVegDsJUpxKCGrIfpqgd2LPweVjfrVUs865P0Y_aohlycyNue1ge1wXB9NlS-a8VWrNBh-Xw. Accessed: October 13, 2024.

ROCHA, Maria Victória. Prospeção de texto e dados (text and data mining) na diretiva relativa aos direitos de autor e direitos conexos no mercado único digital. RRDDIS – Revista Rede de Direito Digital, Intelectual & Sociedade, Curitiba, v. 2, no. 4, pp. 99-164, 2022, p. 103. Available at: https://revista.ioda.org.br/index.php/rrddis/article/view/76/45. Accessed: 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, pp. 354-400. Available at: https://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf. Accessed: July 13, 2024.

SCHIRRU, Luca. Direito autoral e inteligência artificial: autoria e titularidade nos produtos da IA. Thesis (Doctorate in Public Policy, Strategies, and Development) – Instituto de Economia, Universidade Federal do 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. Accessed: July 13, 2024.

SOUZA, Allan Rocha de. Direitos morais do autor. Civilistica.com. Rio de Janeiro, year 2, no. 1, January–March/2013. Available at: https://civilistica.emnuvens.com.br/redc/article/view/73/53. Accessed: July 27, 2024.

SOUZA, Allan Rocha de. SCHIRRU, Luca. Alvarenga. MIGUEL BARROS. Mineração de textos e dados na pesquisa em saúde: reflexões sobre direitos autorais. Cadernos de Saúde Pública 2024. Available at: https://cadernos.ensp.fiocruz.br/ojs/index.php/csp/article/view/8597/19335. Accessed: July 27, 2024.

STAUT JÚNIOR, Sérgio Said. *Direitos Autorais: entre as relações sociais e as relações jurídicas.* Moinho do Verbo. Curitiba. 2006.

TURING, A. M. Computing Machinery and Intelligence. Mind, v. 59, no. 236, pp. 433-460, October 1950. Available at: https://academic.oup.com/mind/article/LIX/236/433/986238. Accessed: July 13, 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

7

Algorithmic Originality: Is There Originality in the Outputs of Generative Artificial Intelligence?

TAIS BIGARELLA LEMOS

Contents: Introduction. 1. The concept of originality in copyright law. 2. But how does artificial intelligence work? 3. Metrics for assessing the originality of outputs generated by artificial intelligence. Final considerations. References. Annex I.

Introduction

Artificial intelligence is increasingly prominent not only in academic and professional circles but also in more informal settings in people's everyday lives. Consequently, there is sometimes an incorrect perception of what it means, including the notion that artificial intelligence is associated with robots and futuristic items such as flying cars. Artificial intelligence, however, is a field of study known for developing and using machines capable of performing tasks that would normally require human intelligence. [2]

Developing artificial intelligence involves "machine learning" and "deep learning." "Machine learning" is a branch of artificial intelligence and computer science that studies the use of data and algorithms to enable artificial intelligence to imitate how humans learn, improving its accuracy. [3] "Deep learning," in turn, uses multiple layers of neural networks to simulate the complex decision-making process of the human mind. [4]

Artificial intelligence thus consists of different "machine learning" models, distinguished by how they use and understand data. [5] Artificial intelligence software is becoming increasingly complex, producing work never before performed by computers. [6] For example, the latest generation of generative artificial intelligence, which

1. Master of Laws from the Universidade Federal do Rio Grande do Sul (2022). Bachelor of Legal and Social Sciences from the Universidade Federal do Rio Grande do Sul (2018). A judicial assistant to an appellate judge at the Tribunal de Justiça do Rio Grande do Sul. Email: 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: August 02, 2024.

3. IBM. What is machine learning?. IBM, 2024. Available at: https://www.ibm.com/topics/machine-learning. Accessed: August 02, 2024.

4. HOLDSWORTH, J.; SCARPICCHIO, M. What is deep learning?. IBM, 2024. Available at: https://www.ibm.com/topics/deep-learning. Accessed: August 02, 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: August 02, 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 public and raising new questions, especially with the launch of ChatGPT, can learn and synthesize not only human language but also other data, such as images and videos. [7] These systems are a type of artificial intelligence model called a large-scale language model, normally referred to by its English name “Large Language Model” or simply the acronym “LLM,” and can perform various language understanding and text generation tasks at an unprecedented level. [8] Several strategies can be used to train these models to think and act, including document selection, linking to search engines, and training question-answering systems. [9] “Inputs” are entered into the system, resulting in “outputs.”

These new technologies challenge the legal system, including in matters of copyright protection for both the documents used to train a system and the results it produces, its “outputs.” Regarding data used for model learning, there has been much discussion of the possibility of using copyright-protected works, especially following the well-known case in which The New York Times sued OpenAI and Microsoft over the use of its articles to train artificial intelligence systems. [10]

Another prominent issue is whether artificial intelligence could be the author of an intellectual work, considering the understanding that only natural persons have that capacity because they alone can create a work. [11] However, one essential aspect for a creation to be protected by copyright appears to receive little attention when artificial intelligence products are analyzed, even though copyright protection cannot exist without it: originality.

7. IBM. What is artificial intelligence?. IBM, 2024. Available at: https://www.ibm.com/topics/artificial-intelligence. Accessed: August 02, 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: August 06, 2024.

11. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima. Rio de Janeiro: Lumen Juris, 2010. p. 434.

Only creations that possess something more are protected, enabling them to qualify as works. [12] Whether called originality, creativity, individuality, or a minimum contribution, this something more must exist for copyright protection to apply. In this regard, even before considering the authorship of artificial intelligence outputs, it seems essential to analyze whether those results possess that something more warranting copyright protection. If the “creation” is not considered a protected intellectual work, there is no reason to debate who would hold rights as its author, since it would not even be an object of protection.

Thus, this study’s research question is whether originality exists in the results/outputs obtained by users of generative artificial intelligence systems, considering copyright scholarship.

To this end, the first chapter will analyze the concept of originality in copyright law, followed by an examination of how artificial intelligence works in the second chapter. The third and final chapter will conclude with metrics for assessing output originality and approaches to the subject in other legal systems.

1. The concept of originality in copyright law

Understanding the scope of copyright is complex and raises many questions when analyzing specific cases. Unlike rights protected by Industrial Property, [13] Copyright Law No. 9.610/98, [14] hereafter referred to by its acronym LDA, defines the object of its protection more broadly, requiring each creation to be analyzed to determine whether it meets the requirements for protection.

Beginning with the legislative analysis, the opening provision of Article 7 of the LDA defines protected intellectual works as “creations of the mind expressed through any medium or fixed in any tangible or intangible support, known or

12. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima. Rio de Janeiro: Lumen Juris, 2010. p. 307.

13. The Industrial Property Law (No. 9.279/96) protects intellectual property rights with narrower characteristics and more requirements, including registration with the National Institute of Industrial Property (INPI), such as patents, industrial designs, and trademarks. It is therefore very common to understand that, when a product/creation does not fit any of these rights, there is an attempt to classify it as a creation eligible for copyright protection.

14. BRAZIL. Law No. 9.610 of February 19, 1998. Amends, updates, and consolidates copyright legislation and makes other provisions. Available at: <https://www.planalto.gov.br/ccivil_03/leis/l9610.htm>.

invented in the future, such as" the examples listed in its thirteen items. [15] These include texts of literary, artistic, or scientific works, audiovisual works, musical compositions, illustrations, and drawings.

As can be seen from the wording of the article's opening provision, the legal definition is quite broad, and the list in its items is merely illustrative. [16] Other intellectual works not listed may therefore be protected, provided they meet the remaining legal requirements. In this regard, it is important to emphasize that copyright stems from a protection policy seeking to balance society's access to works with incentives for authors [17] by granting a monopoly right over a work.

It is therefore of utmost importance first to analyze whether a creation has the attributes necessary for copyright protection, as this may affect the balance between public access and the monopoly granted to the author. In this regard, examining whether a creation is original is essential to determine whether it qualifies for protection. This is because originality, also called a "minimum contribution" or creativity in legal scholarship, is the only filter in the Brazilian legal system and serves as an incentive for the author, the subject, to express their creative spirit by creating something distinct from what came before. [18]

There is, however, no unanimous understanding of what characterizes originality. Traditionally, a distinction is drawn between interpretations of the term in common-law countries that adopt copyright, [19] such as the United

15. Article 7. Protected intellectual works are creations of the mind expressed through any medium or fixed in any tangible or intangible support, known or invented in the future, such as:

I - texts of literary, artistic, or scientific works; II - lectures, speeches, sermons, and other works of the same nature; III - dramatic and dramatic-musical works; IV - choreographic and pantomimic works whose stage performance is fixed in writing or in any other manner; V - musical compositions, with or without lyrics; VI - audiovisual works, with or without sound, including cinematographic works; VII - photographic works and works 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, drafts, and visual works concerning geography, engineering, topography, architecture, landscaping, scenography, and science; XI - adaptations, translations, and other transformations of original works presented as a new intellectual creation; XII - computer programs; XIII - collections or compilations, anthologies, encyclopedias, dictionaries, databases, and other works that, through the selection, organization, or arrangement of their content, constitute an intellectual creation.

16. ABRÃO, Eliane Yachouh. Direitos de autor e Direitos conexos. 1st ed. São Paulo: Editora do Brasil, 2002. p. 97.

17. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima. Rio de Janeiro: Lumen Juris, 2010. p. 309.

18. BARBOSA, Pedro Marcos Nunes. Originalidade em Crise. Revista Brasileira de Direito Civil, vol. 15, 2018, pp. 38-39. Accessed via HeinOnline.

19. Copyright originated in England with the Statute of Anne and later influenced the United States of America, adopting a society-oriented perspective to promote the dissemination of works. For more 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. pp. 991-1031.

States of America, which used the “sweat of the brow doctrine” before moving to the theory of de minimis creativity, and countries of the Romano-Germanic or civil-law tradition, which use the idea of the creativity doctrine. [20]

The “sweat of the brow doctrine,” translated as the theory of sweat on the brow, holds that labor and industry, even without any creativity, could suffice to meet the originality requirement for copyright. [21] Copyright arose from the idea of a certain materialization of authors’ rights because, as the name itself indicates, its purpose was to protect the “right to copy”; thus, the basis of the right was the copyable work. In this system, the original idea was that the copy’s economic usefulness would be more relevant than the creativity of its subject matter. [22] The sweat of the brow theory therefore emerged in this context, where less importance was indeed given to the creativity involved in a work’s creation.

The creativity doctrine, in turn, holds that a minimum amount of creativity must be established for copyright protection, even if modest, and requires that the work not be a copy of another. Under this reasoning, a mere compilation of information without a minimum of creativity could not be protected. [23]

In the United States of America, the 1991 decision in Feist [24] rejected application of the “sweat of the brow” theory, establishing that a work must demonstrate a minimum level of creativity to meet the originality requirement. [25] The case concerned a compilation, and it was held that its selection, coordination, and arrangement did not satisfy the constitutional minimum for copyright protection because they were commonplace, consisting only of an alphabetical listing. The theory of de minimis creativity is thus understood to have been applied.

Turning to the Brazilian context, the LDA is unclear about which theory was adopted. However, since Brazil belongs to the

20. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão.* Belo Horizonte: Arraes Editora, 2012. p. 43.

21. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão.* Belo Horizonte: Arraes Editora, 2012. p. 44.

22. ASCENSÃO, José de Oliveira. Direito de autor sem autor e sem obra. Stvdia Ivridica, Ad Honorem – 3, Boletim da Faculdade de Direito, Universidade de Coimbra, 1991. p. 88.

23. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão.* Belo Horizonte: Arraes Editora, 2012. p. 45.

24. UNITED STATES OF AMERICA. U.S. Supreme Court. Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc., 499, U.S. 340. Appellant: Feist Pubs. Inc. Appellee: Rural Tel. Svc. Co., Inc. Opinion by Justice Sandra Day O’Connor, March 27, 1991. Available at: https://supreme.justia.com/cases/federal/us/499/340/. Accessed: July 27, 2024.

25. As stated in part of the opinion in Feist: “Originality requires only that the author make the selection or arrangement independently (i.e., without copying that selection or arrangement from another work), and that it display some minimal level of creativity”. Available at: https://supreme.justia.com/cases/federal/us/499/340/. Accessed: July 27, 2024.

Romano-Germanic tradition, there is a leaning toward the creativity theory. [26] Furthermore, drawing on the Berne Convention and TRIPs, Leonardo Pontes explains that, under Brazilian legislation:

> the term “intellectual creation” would be more correctly interpreted in the sense of the creativity doctrine, insofar as, through that doctrine, the law would not protect compilations of productions, since these represent nothing more than something trivial or mechanical in nature. [27]

Barbosa, Souto Maior, and Tinoco explain that it appears to be part of the collective consciousness of both Brazilian legal scholarship and case law that “something more,” a minimum contribution, must be present for a creation to be considered a work. The term used to identify this contribution may vary in legal scholarship, with terms such as “creativity,” “originality,” “individuality,” and the like.

José de Oliveira Ascensão, for example, when defining creativity, states that a work must possess a minimum of creativity or originality. He explains that when one moves from creation to description, when the object dictates the result rather than the author’s vision playing the predominant role, one is no longer within the scope of copyright protection. [28]

This study uses the expression “originality” in the sense of the creativity doctrine, understanding that a work must display a minimum degree of creativity, a minimum contribution, to receive copyright protection. The term “originality” is also chosen because it is considered the most popular term for this attribute of authored creation, including being an expression commonly used in English [29] and therefore more appropriate here, where the focus is originality in artificial intelligence.

Having established the concept of originality in copyright law, we now turn to analyzing artificial intelligence and possible metrics for assessing output originality.

26. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão.* Belo Horizonte: Arraes Editora, 2012. p. 49.

27. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão.* Belo Horizonte: Arraes Editora, 2012. p. 51.

28. ASCENSÃO, José de Oliveira. Direito autoral. 2nd ed., revised and expanded. Rio de Janeiro: Renovar, 1997. p. 57.

29. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima. 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 intended to simulate biological cognition, human intelligence, using machines. Most artificial intelligence currently uses “machine learning,” which, as also mentioned, employs algorithms that can “learn” or improve performance on specific tasks based on programmed instructions. Artificial intelligence can, however, be understood as a “black box,” since the programmer sees only what they put in to “feed” the system, the “input,” and the result, the “output,” without being able to observe the machine’s learning process specifically. [30]

This study focuses on generative artificial intelligence, whose outputs or results are creations that could be considered objects of copyright protection. As noted in the chapter above, Article 7 of the LDA lists some types of creations that could be protected. For this analysis, texts of literary works and illustrations stand out among the types listed in its items. [31]

This is because artificial intelligence systems currently appear capable of generating these types of creations. The best-known tool is ChatGPT, a chatbot capable of creating coherent paragraphs by predicting the most likely next word in a sentence. [32] This tool can create complete texts that might, at first glance, be considered literary works. ChatGPT is a large-scale language model, normally referred to in English as a “Large Language Model” or LLM, built by training on a massive number of documents/texts. The models incorporate information obtained from the dataset and thereby learn word patterns for a given context, enabling the user to obtain the most likely combination of words as a result and generating more natural language. [33]

Annex I of this study demonstrates a response provided by the tool when asked to “Write a literary work of romance,

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 No. 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: August 02, 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-timess-about-face/. Accessed: August 06, 2024.

in four paragraphs, portraying a love story with a happy ending." The result confirms that, on initial analysis, a reader might even intuitively understand the text as a literary work, especially without knowing its origin, that is, that it was produced by artificial intelligence.

Another very interesting generative artificial intelligence tool is DALL-E, also developed by OpenAI, the same company behind ChatGPT. This tool does not generate text but, as its website explains, is a system capable of creating realistic images or art from a user's description. [34] As noted for ChatGPT, its output might likewise appear, at first glance, eligible for copyright protection because it creates illustrations and visual works.

Both systems are protected in Brazilian law by the Software Law (Law No. 9.609/98), which protects a computer program as the "expression of an organized set of instructions in natural or coded language, contained in a physical support of any nature, necessarily employed in automated information-processing machines, devices, instruments, or peripheral equipment based on digital or analogous techniques, to make them operate in a specified manner and for specified purposes" [35]. However, as the legislator clearly states, this protection applies to the expression of the organized set of instructions, that is, the model itself used, and not necessarily the products obtained from it. There is therefore a difference between protection of the software itself, the code used by artificial intelligence, which appears undisputedly covered by the Software Law, and its outputs, whose eligibility for copyright protection is debated.

It is therefore essential to analyze what the Terms of Use of the platforms mentioned, ChatGPT and DALL-E, provide regarding ownership and protection of their results. Their Terms of Use are the same, since both services are offered by OpenAI. [36] The first clarification is that the Terms of Use constitute an agreement between the user and OpenAI, including important dispute-resolution provisions, and that by using the services, the user agrees to these Terms. The existence of other Terms of Use for residents of the European

34. According to information at: OpenAI. DALL-E 2. OpenAI, 2024. Available at: https://openai.com/index/dall-e-2/. Accessed: August 03, 2024.

35. Under Article 1 of Law No. 9.609/98. BRAZIL. Law No. 9.609 of February 19, 1998. Provides for intellectual property protection of computer programs, their commercialization in the country, and other matters. Available at: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm.

36. The terms of use are available at: OpenAI. Terms of use. OpenAI, 2024. Available at: https://openai.com/policies/terms-of-use/. Accessed: August 04, 2024.

Union, Switzerland, and the United Kingdom is also noted. Those terms will not be analyzed in this study, which focuses on Brazilian regulation.

That said, regarding outputs specifically, the Terms of Use state that inputs and outputs are jointly called “content.” Content ownership, in turn, is provided for in the sense that, to the extent permitted by applicable law, users retain ownership rights over the inputs they provide and also own the outputs. The provision states:

> Ownership of content. As between the user and OpenAI, to the extent permitted by applicable law, the user (a) retains ownership rights over the input and (b) owns the output. We hereby assign to the user all our rights, title, and interests, if any, in the output. [37]

Regarding the existence of copyright over these results specifically, the Terms of Use make no mention of it, containing only a section referring to the possibility of users submitting a notice if they believe the platform is infringing their copyright. It is interesting, however, to note that the Terms include a section listing activities users may not undertake (“What you cannot do”), including representing output as human-generated when it was not. [38]

Thus, at least in the Terms of Use, the company does not expressly claim that the results obtained would be protected by copyright. Even if they were, rights over these works are assigned to users, subject to the qualification that the results cannot be presented as human-generated because they were not.

It seems reasonable for the Terms of Use not to presume copyright protection over these results. As already noted, a creation must meet various requirements to be protected by copyright, including originality, the subject of this study. We therefore turn to metrics for assessing the originality of these results/outputs.

37. The author’s free translation in the source 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: August 04, 2024.

38. The original provision reads: “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: August 04, 2024.

3. Metrics for assessing the originality of outputs generated by Artificial Intelligence

To assess whether a minimum amount of originality or creativity exists to justify copyright protection, also called a minimum contribution in legal scholarship, it is first essential to consider the definition of a work, since a creation cannot be called a work unless a minimum of creativity is present in its making. [39] To identify a creation as a work, legal scholarship holds that one should first look to its creator: it can be a work only if its intellectual creator is a human person to whom the final result can be attributed. It is then necessary to establish that the creation has been externally expressed, is not subject to legal prohibitions, and finally displays a minimum contribution. [40]

The minimum contribution, in turn, is characterized by the minimum creativity necessary for a work to exist and also helps distinguish works from one another, so that where a minimum contribution exists, there is no plagiarism. [41] In this regard, it is important to understand that if a minimum contribution differentiates one work from another, even if the first was based on the second, a work is understood to exist; however, these are called derivative works. Derivative works include translations and adaptations and therefore require authorization from the original work's rights holder. Nevertheless, they are granted original ownership as intellectual creations with sufficient creativity, independently of the copyrights in preexisting works, which remain intact. [42]

To measure the amount of creativity or originality necessary for a work's copyright protection, Leonardo Machado Pontes suggests three criteria: (i) the person responsible for composing the work and its direct development must be the author, rather than someone who merely follows orders to carry it out; (ii) the greater the mechanical participation in the work's production process, the more the author must demonstrate that they deserve protection; and (iii) authorship equates to originality and creativity. [43]

39. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima. Rio de Janeiro: Lumen Juris, 2010. p. 446.

40. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima. Rio de Janeiro: Lumen Juris, 2010. p. 449.

41. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima. Rio de Janeiro: Lumen Juris, 2010. p. 470.

42. COSTA NETTO, José Carlos. Direito Autoral no Brasil. Coordinated by Hélio Bicudo. São Paulo: FTD, 1998. p. 63.

43. PONTES, Leonardo Machado. Direito de Autor: a teoria da dicotomia entre a ideia e a expressão. Belo Horizonte: Arraes Editora, 2012. pp. 88-94.

The first criterion concerns the distinction between the work's author and a mere executor who simply follows a third party's orders without any improvement. The second criterion concerns the need, even when a work is created with machines' assistance, to follow a standard, however low, demonstrating an expression of creativity, even if minimal. Protection would exist only when the work is identified as not being a machine's automatic production, but an author's expression. [44] Finally, the third and last criterion concerns the understanding that, ultimately, for copyright protection to exist, originality and creativity mean only that the creation must arise from the author's work and not be a copy of another work. [45]

Thus, assessing whether originality or creativity exists in generative artificial intelligence outputs, even in a minimal amount, requires analyzing whether they meet these three criteria. From the premises established in the previous sections, we know that the artificial intelligence systems studied here function so that a user request (input) yields a result or output that may superficially resemble a copyright-protected work.

However, analyzing the criteria necessary to recognize a work's originality and warrant its protection, none of them appears to be present in creations produced by these artificial intelligence systems.

Beginning with the first requirement, it seems difficult to interpret artificial intelligence as anything other than a mere executor of orders, since it simply predicts the most coherent response based on what it has learned and the user's request. [46] Thus, the system's result more closely resembles a machine's automatic production, also failing the second criterion mentioned, since the machine is taught to reason and make inferences based on its training. In this regard, the greater the interactivity between machine and user, the greater the chance of obtaining a better result or output. [47]

44. PONTES, Leonardo Machado. Direito de Autor: a teoria da dicotomia entre a ideia e a expressão. Belo Horizonte: Arraes Editora, 2012. pp. 88-89 and 91.

45. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão.* Belo Horizonte: Arraes Editora, 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: August 02, 2024. Explains that ChatGPT is a chatbot capable of predicting the most likely next word in a sentence based on numerous 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 2302.07842. p. 9.

Regarding the third and final criterion, it is also interesting to consider whether, since the results obtained from these systems are based on the data entered into them, which enable their learning and teach them to reason, we might in a certain sense be facing a form of plagiarism.

As already noted, for works to be distinguished and understood as separate, rather than constituting plagiarism, there must be a minimum contribution from the author. In generative artificial intelligence, using images and articles to teach a system in order to obtain the most accurate result possible leads to the conclusion that the result obtained when asking ChatGPT, for example, to produce a text is ultimately a combination of the various data entered to “teach” the model. Thus, even if not a direct copy of the documents feeding the system, outputs are possible and display the desired accuracy partly because of those documents.

In this regard, it is interesting to highlight The New York Times’ lawsuit against OpenAI and Microsoft over 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 article use is aggravated by two factors: the large-scale language model memorizes portions of works and may therefore generate results reproducing them; and it produces “synthetic” search results that may enable readers to read Times articles unavailable without paying for a newspaper subscription, harming its business model. [48]

These arguments are interesting for this analysis because they raise the same questions about the originality of these AI models’ outputs, which may even constitute evident plagiarism by reproducing articles used to train the language model.

In this regard, it is important to reflect that humans invariably draw on and are inspired by other works when creating, but can reason, think, make connections, and use that information in various ways. Artificial intelligence systems, by contrast, do not possess “intelligence” as such but make predictions, with machines’ improving abilities yielding increasing accuracy and the desired result. However, this is not comparable to human intelligence, which can obtain

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: August 06, 2024.

information from one source and use it in various ways, being transferable, unlike machines' "intelligence." [49] Furthermore, to avoid plagiarism, human authors must also cite their sources, a characteristic not observed in results obtained from artificial intelligence.

Similarly, legal systems appear to be tending toward recognition that artificial intelligence results lack sufficient creativity for copyright protection. This is because machines lack internal awareness and sensitivity to what they are doing and do not draw inspiration at a subconscious level, [50] requirements normally demanded for a protected work, as can also be seen in the Feist decision mentioned above. The United States Supreme Court indicated the need for an author to prove the "existence of those facts of originality, of intellectual production, of thought, and conception." [51]

The same interpretation can also be identified in other legal systems, such as Japan's Intellectual Property Strategic Program 2016, which indicates that products created automatically by artificial intelligence are not eligible for copyright protection under the current legal system. It can also be inferred from French decisions that, although results produced by humans with machines' assistance may be protected, machines are denied the ability to replace humans and perform the work independently. [52]

China's approach, however, has been moving in the opposite direction. Since 2019, Chinese courts have stated that artificial-intelligence-generated products constitute copyright-protected works. [53] Chinese law does not specifically address the subject, but the courts' interpretation affirms the possibility of protection based on four factors: (i) adopting a broader interpretation of human participation, considering the requirement met

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: August 02, 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. According to UNITED STATES OF AMERICA. U.S. Supreme Court. Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc., 499, U.S. 340. Appellant: Feist Pubs. Inc. Appellee: Rural Tel. Svc. Co., Inc. Opinion by Justice Sandra Day O'Connor, March 27, 1991. Available at: https://supreme.justia.com/cases/federal/us/499/340/. Accessed: July 27, 2024. The author's free translation in the source 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. Juridical Tribune, vol. 13, no. 2, June 2023, pp. 243-244. Accessed via HeinOnline.

53. DAI, Zhe; and JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. Juridical Tribune, vol. 13, no. 2, June 2023, p. 245. Accessed via HeinOnline.

even if human participation occurs only at the preparatory stage, before artificial intelligence operations; (ii) not distinguishing between machine assistance and results generated by artificial intelligence; (iii) adopting an objective standard for the concept of originality, which may be met even without human participation, since artificial-intelligence-generated content is understood to reflect selection, judgment, and analysis of relevant data, sufficient to satisfy the originality requirement; and finally, what may be understood as the main reason for the difference between China's approach and that of other countries, (iv) the strong utilitarian principles of its copyright law. Human participation carries less weight in Chinese legislation, with protection focused less on who created a work and more on whether protection serves society's interests. [54]

Although analyzing China's approach is interesting, its adoption by other countries seems unlikely given their current copyright legislation, particularly in the Romano-Germanic family, which adopts the creativity theory and places greater emphasis on human characteristics, the connection between authors and their works, and what only humans could do. In any event, the debate is inevitable, as generative artificial intelligence models are gaining increasing prominence and space, including economically. Understanding how to regulate them and what protection they will receive, including for their outputs or results, is therefore essential.

Final considerations

Although no longer new, artificial intelligence is becoming increasingly present and prominent in people's everyday lives. Among the various challenges this technology poses to the legal system are those concerning copyright protection of its outputs or results, which may initially resemble copyright-protected works such as literary texts and illustrations.

However, for a creation to be eligible for copyright protection, it must possess originality, displaying a minimum amount of creativity that differentiates it from creations already produced by third parties and justifies the author's monopoly, with only that author holding rights over the

54. DAI, Zhe; and JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. Juridical Tribune, vol. 13, no. 2, June 2023, pp. 249-254. Accessed via HeinOnline.

work. Artificial intelligence outputs, however, do not appear to possess this characteristic, since these models seem more like mere executors of orders, whose results would constitute a machine's automatic production rather than being original.

Furthermore, the fact that these models' results are based on data entered into them, sometimes copyright-protected texts and images, leads to the conclusion that they lack sufficient originality to be understood as autonomous works deserving copyright protection. On the contrary, they could even constitute plagiarism by merely reproducing protected works used for learning.

It is therefore concluded that artificial intelligence systems' outputs generally do not display sufficient originality to be objects of copyright protection.

References

ABRÃO, Eliane Yachouh. Direitos de autor e Direitos conexos. 1st ed. São Paulo: Editora do Brasil, 2002.

ASCENSÃO, José de Oliveira. Direito autoral. 2nd ed., revised and expanded. Rio de Janeiro: Renovar, 1997.

ASCENSÃO, José de Oliveira. Direito de autor sem autor e sem obra. *Stvdia Ivridica,* Ad Honorem –3, Boletim da Faculdade de Direito, Universidade de Coimbra, 1991.

BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; and RAMOS, Carolina Tinoco. O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima. Rio de Janeiro: Lumen Juris, 2010.

BARBOSA, Pedro Marcos Nunes. Originalidade em Crise. Revista Brasileira de Direito Civil, vol. 15, 2018, pp. 33-48. Accessed via HeinOnline.

BRAZIL. Law No. 9.609 of February 19, 1998. Provides for intellectual property protection of computer programs, their commercialization in the country, and other matters. Available at: <https://www.planalto.gov.br/ccivil_03/leis/l9609.htm>.

BRAZIL. Law No. 9.610 of February 19, 1998. Amends, updates, and consolidates copyright legislation and makes other provisions. Available at: <https://www.planalto.gov.br/ccivil_03/leis/l9610.htm>.

COSTA NETTO, José Carlos. Direito Autoral no Brasil. Coordinated by Hélio Bicudo. São Paulo: FTD, 1998.

DAI, Zhe; and JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. Juridical Tribune, vol. 13, no. 2, June 2023, pp. 241-260. Accessed via HeinOnline.

UNITED STATES OF AMERICA. U.S. Supreme Court. Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc., 499, U.S. 340. Appellant: Feist Pubs. Inc. Appellee: Rural Tel. Svc. Co., Inc. Opinion by Justice Sandra Day O'Connor, March 27, 1991. Available at: https://supreme.justia.com/cases/federal/us/499/340/. Accessed: 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: August 02, 2024.

HOLDSWORTH, J.; SCARPICCHIO, M. What is deep learning? IBM, 2024. Available at: https://www.ibm.com/topics/deep-learning. Accessed: August 02, 2024.

IBM. What is artificial intelligence? IBM, 2024. Available at: https://www.ibm.com/topics/artificial-intelligence. Accessed: August 02, 2024.

IBM. What is machine learning? IBM, 2024. Available at: https://www.ibm.com/topics/machine-learning. Accessed: August 02, 2024.

OpenAI. DALL-E 2. OpenAI, 2024. Available at: https://openai.com/index/dall-e-2/. Accessed: August 03, 2024.

OpenAI. Terms of use. OpenAI, 2024. Available at: https://openai.com/policies/terms-of-use/. Accessed: August 04, 2024.

PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão.* Belo Horizonte: Arraes Editora, 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: August 06, 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. Accessed via HeinOnline.

Annex I – ChatGPT Response

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

8

The Challenges Surrounding the Use and Regulation of Artificial Intelligence in the Face of Algorithmic Discrimination

MARIA FERNANDA LONGATO MATURANA

Contents: Introduction. 1. How artificial intelligence learns and the heart of the problem of algorithmic discrimination. 2. The challenges surrounding artificial intelligence regulation to ensure the promotion of equality and prevent discrimination. 3. New horizons in internet networks in light of Bill No. 2.338/2023. Final considerations. References.

Introduction

Amid the constant evolution of the modern world, artificial intelligence has established itself as one of the most transformative technologies with the greatest projected use in the modern era, enabling innovative, rapid, and relevant transformations and solutions in various fields, from healthcare to the broadest areas of agribusiness.

The aim of using artificial intelligence technology lies in “humanizing” the machine so that its responses can be relevant to society, since the machine becomes a reflection of it. This thinking has enabled various technological advances, but at the same time, the use of artificial intelligence algorithms raises complex and concerning issues for society, especially regarding algorithmic discrimination, since artificial intelligence aims to reflect society’s thinking, including its imperfections.

Algorithmic discrimination occurs when artificial intelligence systems reproduce or even amplify discriminatory stereotypes together with existing prejudices within society, resulting in biased decisions and creations that negatively affect groups of people already subject to structural discrimination.

The problem of algorithmic discrimination arises in various ways and from various sources, including training data biased by discriminatory stereotypes, inadequate design choices, and even a lack of diversity among artificial intelligence developers. These challenges not only compromise equity and fairness in automated decisions but also reveal structural problems in society. Understanding and addressing these challenges is therefore crucial to ensure that

1. A postgraduate student in Digital Law at the Universidade do Estado do Rio de Janeiro (UERJ) in partnership with the Instituto de Tecnologia e Sociedade (ITS). An attorney at Abramides e Gonçalves. Email: mariafernandalm@icloud.com

artificial intelligence is used to assist society by promoting inclusion and equity, rather than perpetuating inequalities.

This article aims to explore the various aspects of algorithmic discrimination, analyzing the roots of its causes, its impacts on society, and possible solutions. First, it provides an overview of the fundamental concepts related to how artificial intelligence learns, highlighting the sensitive points that allow algorithmic discrimination and presenting real cases in which these problems have arisen, with their social and ethical consequences. It then discusses the ethical challenges surrounding data science in artificial intelligence. Finally, it examines strategies and best practices for mitigating algorithmic discrimination and promoting the sound development of this technology.

1. How artificial intelligence systems learn and the core of the problem of algorithmic discrimination

There is much discussion of algorithmic discrimination, but understanding the heart of this debate requires an understanding of how the various kinds of artificial intelligence learn.

Artificial intelligence learning is a technique, a complex process that, in brief, involves analyzing a variety of cases and establishing relationships among them. In this way, artificial intelligence analyzes a diverse range of data and acquires knowledge through these data patterns.

Algorithms and all the systems involved in artificial intelligence are extremely volatile, constantly adapting to achieve objectives. This is possible only through the technique known as machine learning, which allows systems to learn and improve their performance through a dataset, enabling them to perform various actions without having been explicitly programmed to do so. [2]

To put it more clearly, machine learning is based on a dataset. Through repeated training, the machine calculates these data and

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: July 17, 2024.

begins to find patterns, generating answers that assist in a wide variety of fields of human activity, from disease prognoses to fraud detection and even the familiar applications of facial and voice recognition.

On this subject, Arthur Samuel [3] states: “Machine learning is the field of study that gives computers the ability to learn without being explicitly programmed.”

Depending on the questions posed and the availability of data, there are several ways to implement machine learning. Authors Lloyd, Mohseni, and Rebentrost identify three types of machine learning. [4]

The first model is known as supervised learning, in which algorithms are trained on labeled datasets. The machine is trained to classify predictions for these data, with each input example associated with a desired output. The aim is for the machine to interactively classify various features so that it can ultimately achieve the desired result on the basis of the features classified.

The second model is unsupervised learning. Unlike the first model, its 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 that require learning from large-scale data, popularly known as big data. This model enables better segmentation within a customer base, generating more effective communication with the system operator’s target audience.

The third model is known as reinforcement learning and differs most from the others mentioned. Here, algorithms operate by using rewards and penalties for the actions performed. The objective is to learn a policy that maximizes the cumulative reward over time. It is commonly used in games. [5]

With all these technologies available, the market is advancing every day, and the use of artificial intelligence is becoming increasingly

3. SAMUEL, A. Some studies in machine learning using the game of checkers. IBM Journal of Research and Development, v. 3, no. 3, pp. 210-229, 1959. Available at: https://people.csail.mit.edu/brooks/idocs/Samuel.pdf. Accessed: 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: 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: July 17, 2024.

dynamic, reaching various groups of consumers of this product across different areas of society. As a wide range of artificial intelligence systems has become widespread, the mistaken idea has emerged that this technology is neutral and that all its decisions are made from an entirely neutral standpoint. This understanding brings us to the heart of the problem discussed in this article.

On this subject, Safiya Umoja Noble states: “Algorithms are not neutral; they reflect the priorities, values, and judgments of those who have the power to shape them.” [6]

People forget that the way artificial intelligence functions is closely tied to how it was programmed and to the database used in its programming. Its results will therefore always be related to the data supplied to the machine. These data are not neutral; quite the contrary, they may be closely associated with various discriminatory biases held by their programmers and by society as a whole.

Human society is far from ideal and is becoming increasingly steeped in prejudice. In this context, the core issue in algorithmic discrimination begins with the algorithms themselves, which may embody the ideological biases of their programmers. Passing on these biases does not necessarily involve a malicious intention to transmit such prejudices; it may stem from human error that has been transferred to the programming without being noticed. In any event, however, this transmission will directly affect the results of the tool’s decisions.

Even when algorithms are not imbued with their programmers’ ideological biases, however, they may still contain discriminatory biases embedded in their own datasets. These algorithms can therefore generate clearly prejudiced results when fed completely distorted concepts and values.

Artificial intelligence systems replicate what they have been taught and thus learn from the biases in the data made available to them. It is consequently very easy for programmers to create artificial intelligence systems imbued with wholly discriminatory data,

6. NOBLE, S. U. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press, 2018.

so that all their decisions will be imbued with those same biases, spreading these prejudices even further. In today's society, such discriminatory thinking is rapidly increasing, and artificial intelligence systems built on distorted and discriminatory data are becoming increasingly common.

These points lead to the conclusion that the machine itself is not prejudiced and does not hold discriminatory biases. However, the human beings behind its development can introduce these distorted biases into the way it learns, affecting all its decisions [7].

Algorithmic discrimination works like a mathematical formula: whenever a system is fed data containing discriminatory biases, its algorithmic decisions will reproduce those same biases, resulting in even more discrimination and, consequently, a serious violation of human rights. One example is the use of algorithms in a policing system based on explicitly biased crime statistics. The decisions made by this policing system tend toward greater monitoring of neighborhoods with larger immigrant populations. The system thus suggests deploying more police officers to these locations, where every police incident is then recorded, suggesting that neighborhoods with larger immigrant populations have high crime rates. That conclusion, however, is untrue. What happens is that, because more police officers are present, every incident is recorded. In other neighborhoods, by contrast, fewer officers are deployed, so fewer incidents are recorded and the crime rate is consequently lower. This type of predictive policing must be analyzed and used with extreme caution, since it can create a cycle of highly biased and dangerous results in which prejudiced human decisions are amplified, leading to new decisions that reinforce discriminatory positions and, consequently, seriously violate human rights. [8]

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/discriminatingsystems.pdf. Accessed: July 22, 2024.

8. BORGESIUS, F. J. Z. Strengthening legal protection against discrimination by algorithms and artificial intelligence. The International Journal of Human Rights, v. 24, no. 10, pp. 1572-1593, 2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561441. Accessed: July 18, 2024.

On this subject, Frank Pasquale explains: “The algorithm is a mirror: it reflects our priorities and prejudices, but amplified and rendered invisible.” [9]

Everything presented above leads to the conclusion that algorithmic discrimination in artificial intelligence begins even before the decisions of these technologies are introduced into the real world. The basis of algorithmic discrimination thus lies in machine learning itself, showing that the heart of the issue is the moment when artificial intelligence is being developed. This suggests that oversight of artificial intelligence should begin when the technology is created.

In this discussion, Joy Buolamwini and Timnit Gebru stress: “The danger of algorithmic discrimination is that it can scale at a pace and on a scale that exceed human capacities for monitoring and intervention.” [10]

This statement makes it clear that algorithmic discrimination requires attention. The world of technology is immeasurable, and its consequences are equally vast and will not necessarily be positive.

The statement by Joy Boulamwini and Timnit Gebru underscores the point discussed in this chapter: algorithmic discrimination must be addressed when artificial intelligence is created. Once data containing discriminatory biases are fed into artificial intelligence, the consequences of its decisions are immeasurable. They constitute a serious violation of human rights and the Constitution, and reinforce discriminatory principles mistakenly embedded in society many years ago. [11]

2. The challenges of regulating artificial intelligence to promote equality and prevent discrimination

There is consensus on the need to regulate artificial intelligence; however, the difficulty of putting this regulation into effect 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: July 18, 2024.

10. BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, v. 81, pp. 1-15, 2018. Available at: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Accessed: July 15, 2024.

11. Ibid.

clear. This technology is among the areas urgently requiring regulation, yet little is known about how to implement truly effective regulation.

Regulating artificial intelligence involves several areas of law, but algorithmic discrimination clearly requires greater attention in light of the striking recent cases involving this technology.

Although there is no specific legislation regulating artificial intelligence and its effects, Brazilian law guarantees the promotion of equality for all and punishes any and all discriminatory conduct.

The Federal Constitution expressly states: “Art. 5. All persons are equal before the law, without distinction of any kind, and Brazilians and foreign nationals residing in the country are guaranteed the inviolability of the rights to life, liberty, equality, security, and property.” [12]

Law No. 7,716, popularly known as the Racial Crime Law, provides in its first article: “Crimes resulting from discrimination or prejudice based on race, color, ethnicity, religion, or national origin shall be punished under this Law.” [13]

The aforementioned Law No. 7,716 also provides that committing any discriminatory act is a crime and is subject to punishment. It further emphasizes that any discriminatory act carried out over the World Wide Web is also a crime and carries a heavier penalty:

> Art. 20. To practice, induce, or incite discrimination or prejudice based on race, color, ethnicity, religion, or national origin. Penalty: imprisonment for one to three years and a fine. § 2. If any of the crimes provided for in this article is committed through the mass media, publication on social media, the World Wide Web, or a publication of any kind. Penalty: imprisonment for two to five years and a fine. [14]

12. BRASIL. Constituição (1988). Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed: July 19, 2024.

13. BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. Diário Oficial da União: seção 1, Brasília, DF, p. 240, January 6, 1989. Available at: https://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Accessed: July 19, 2024.

14. Ibid.

With these points clarified, and reiterating the idea already mentioned, there is consensus on the need to advance the pursuit of algorithmic justice, especially to mitigate the risks of direct discrimination (disparate treatment) and indirect discrimination (disparate impact) in algorithmic decisions. Yet there is still no answer as to how this regulation will be implemented. One possible way to mitigate these risks is to invest in research that clarifies the nature of the ethical risks and provides sound, transparent guidance for governing algorithm design and the use of technology. [15]

Tsamados's idea is extremely relevant, but it again raises the problem that none of these strategies has ever moved beyond the realm of ideas. Regulation therefore becomes increasingly remote, while discrimination involving artificial intelligence expands every day. The regulation of these discriminatory acts thus ends up moving in the opposite direction from what appears to be the solution.

As long as there is no legislation regulating artificial intelligence, the effects of its misuse will persist. The root of this problem lies in the lack of transparency in the mechanisms and data associated with artificial intelligence, resulting in a lack of protection for individual rights. [16]

Regarding the lack of transparency in the mechanisms and data associated with artificial intelligence, it should be noted that this information has no clear author. No one is responsible for the data used to make these decisions. Given the discriminatory biases of the algorithms, this lack of transparency makes it extremely difficult to identify the source and hold it accountable for such discrimination. [17]

Transparency is essential to prevent discriminatory biases and avoid a situation of uncertainty for users of this technology. On this subject, the following is emphasized:

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, pp. 215–230, 2022. Available at: https://link.springer.com/article/10.1007/s00146-021-01154-8. Accessed: July 22, 2024.

16. AZEVEDO, Ingrid Borges de. Reconhecimento facial e direito: propostas para uma IA antidiscriminatória. 2021. 65 leaves. Undergraduate thesis (Law degree)—Universidade de Brasília, Brasília, 2021. Available at: https://bdm.unb.br/handle/10483/29805. Accessed: July 22, 2024.

17. BONA, Celito de; SCHONS, Eduarda Arruda; LOPES-FLOIS, Luiza. Inteligências artificiais: existe ética na implementação de algoritmos? Ciências Sociais Aplicadas em Revista, [S.L.], v. 25, no. 45, pp. 225-246, August 18, 2023. Universidade Estadual do Oeste do Paraná - UNIOESTE. Available at: https://e-revista.unioeste.br/index.php/csaemrevista/article/view/31510/22369. Accessed: July 21, 2024.

> This absence of regulation, accountability, auditing, and transparency in the use of AI has had harmful legal and social consequences, as it perpetuates and expands the discrimination and selectivity that permeate the criminal justice system and its agencies. All of this occurs under the illusory impression that it is based on impartial, precise, and objective mathematical models. In truth, the results are laden with subjectivity and racist biases that tend to channel clearly defined social groups toward marginalization and discrimination. [18]

Given the difficulty of regulation, a new discussion arises concerning the liability of the company or programmer that developed the artificial intelligence.

The main question in analyzing the liability of the company or programmer is the developer's intention: whether there was any intention to generate discriminatory results or any ability to monitor those results. Thus, if it is shown that the developer had clear influence over, or intended, the discriminatory results, the developer must be held accountable.

Here, the lack of regulation again becomes a problem, since the only way to analyze the developer's intention and monitoring is through the traceability of the algorithm used by the machine. This information is available only to the developer. Because the matter is unregulated, the information becomes inaccessible, consequently hindering the accountability of those involved in the discriminatory results of artificial intelligence.

The regulation of artificial intelligence in Brazil seems to be moving further from reality every day. However, a law regulating the processing of personal data already exists: Law No. 13,709/2018, the General Data Protection Law (LGPD). It regulates the processing of personal data in Brazil, both online and offline, by individuals or legal entities, whether governed by public or private law. Its main objectives are to protect the fundamental rights to 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. Segregação racial e vieses algorítmicos: máquinas racistas no âmbito do controle penal. Revista Brasileira de Direito, [S.L.], v. 19, no. 2, pp. 1-30, September 22, 2023. Complexo de Ensino Superior Meridional S.A. Available at: https://doi.org/10.18256/2238-0604.2023.v19i2.4768. Accessed: July 22, 2024.. Revista Brasileira de Direito, [S.L.], v. 19, no. 2, pp. 1-30, September 22, 2023. Complexo de Ensino Superior Meridional S.A. Available at: https://doi.org/10.18256/2238-0604.2023.v19i2.4768. Accessed: July 22, 2024.

The General Data Protection Law is an important milestone in the protection of personal data in Brazil. However, it falls short of regulating data in a way that prevents algorithmic discrimination, and its provisions therefore do not solve the problems outlined in this chapter. Some articles of this legislation can serve as a basis for specific legislation on the subject, but regulations complementing the General Data Protection Law are clearly needed.

Article 6 of the General Data Protection Law affirms principles concerning discrimination in the use of data:

> Art. 6. Personal data processing activities shall observe good faith and the following principles: (...) VIII – prevention: adoption of measures to prevent harm arising from the processing of personal data; (...) IX – non-discrimination: the impossibility of processing for unlawful or abusive discriminatory purposes; [19]

The aforementioned Article 6 makes clear that personal data may not be used for unlawful or abusive discriminatory purposes. However, this provision remains incomplete: although it clearly prohibits this discriminatory use of data, there is no punishment for such conduct. Everyone is therefore left to understand that, even though the conduct is prohibited, it will not be punished if it occurs.

Algorithmic justice is widely discussed today, and the subject is being studied around the world in relation to the regulation of artificial intelligence. However, no predictive analysis can reliably establish that artificial intelligence systems will pose no risk of discrimination. [20]

The only way to begin an attempt to eradicate algorithmic discrimination will therefore emerge when the developers of this technology and governments start working together to ensure that artificial intelligence is used ethically and fairly. The technology must be regulated by a legislative framework with a

19. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, p. 1, August 15, 2018. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed: July 22, 2024.

20. HUPFFER, Haide Maria; SANTANNA, Gustavo da Silva. Inteligência artificial e discriminação algorítmica: marcos regulatórios e parâmetros éticos. Available at: http://www.guaritadigital.com.br/casaleirialivros/iasg/iasg.4.pdf. Accessed: July 15, 2024.

set of rules that the tool must follow so that it recognizes discriminatory acts and data without spreading them. [21]

In a society where technology is used on a large scale, a law regulating artificial intelligence is essential to protect citizens' individual rights, especially those of the most vulnerable populations. The rules must be grounded in ethical principles so that algorithmic decisions are transparent and non-discriminatory.

3. New horizons on internet networks in light of Bill No. 2338/2023

Everything discussed in this article makes it clear that artificial intelligence needs to be regulated. However, even with comprehensive regulation, significant changes in algorithmic discrimination will occur only when society becomes aware of the broader issue of discrimination, not just in the digital world but throughout the real world.

Society is persistently trying to combat all discriminatory and prejudiced acts, but this struggle remains far from ideal. Despite so many social advances, discriminatory culture continues to spread around the world. The internet is not exempt from this wave, so new horizons must be sought on the networks to combat these acts.

To address all these ethical challenges, public awareness must be aligned with strong regulation. This regulation, in turn, must be developed by specialists so that it has real effects, moving beyond the realm of ideas to regulate the subject and punish those who spread acts involving discriminatory biases.

The United Nations (UN) explains the need for new horizons in the regulation of artificial intelligence:

> Artificial intelligence promises to drive advances across several sectors, but its deployment must be carefully managed to avoid adverse impacts on human rights and social values.

21. SINGAPURA. Comissão de Proteção de Dados Pessoais. Modelo de Estrutura de Governança de IA. Available at: .https :// www.p.gov.sg/ajuda-e-recursos/2020//01 /model-ai -vai-estrutura. Accessed: 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 evaluated for biases 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 be widely shared and that safeguards be in place to protect against unintended consequences. [22]

The OECD (Organisation for Economic Co-operation and Development) takes a position aligned with that of the UN:

> The governance of artificial intelligence must be grounded in principles that emphasize inclusion, transparency, and accountability. Regulatory frameworks must be forward-looking, anticipating the rapid evolution of AI technologies and their potential social impacts. Policies must encourage the responsible development and deployment of AI, ensuring that it is aligned with democratic values and human rights. This involves creating mechanisms for the continuous monitoring and evaluation of AI systems, as well as promoting international cooperation to address the global challenges posed by AI. By adopting a holistic approach to AI regulation, we can harness its transformative potential while guarding against risks and ensuring that its benefits are distributed equitably. (OECD, 2019, authors' translation) [23]

These positions show that the world is coming to understand the importance of regulating artificial intelligence and is beginning a regulatory movement that ushers in a new era of horizons on the networks. Brazil is currently far behind other countries on this issue. One example is the European Union, which, as a global reference point, enacted the Artificial Intelligence Act in May 2024, regulating the entire subject and emphasizing the fight against algorithmic discrimination.

22. NAÇÕES UNIDAS. 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: July 17, 2024.

23. OCDE. Principles on Artificial Intelligence. 2019. Available at: https://www.oecd.org/going-digital/ai/principles/. Accessed: July 17, 2024.

In Brazil, there are more than 46 bills concerning the regulation of artificial intelligence. Despite this broad array of proposals, the country is still far from effective regulation. Of the 46 bills, the most advanced is Bill (PL) No. 2338/2023, with Senator Eduardo Gomes (PL-TO) as rapporteur. Even this progress is limited, since its vote was postponed for the third time on July 09, 2024.

Bill (PL) No. 2338/2023 has several clear objectives: promoting technological innovation for the sustainable development of artificial intelligence, establishing transparency guidelines concerning the explainability of artificial intelligence systems, and, most importantly for this article, ensuring respect for fundamental rights, human dignity, and privacy.

Bill (PL) No. 2338/2023 emphasizes the principle of transparency in artificial intelligence, an essential principle for combating algorithmic discrimination. AI systems must be designed transparently, allowing people to understand how they work and how decisions are made. Transparency also requires disclosure of information about the data used and the criteria adopted for automated decisions. This makes it possible to understand how potentially discriminatory decisions would be generated and, consequently, to punish those who use these technologies to promote discriminatory acts.

Article 5 of Bill (PL) No. 2338/2023 highlights non-discrimination in 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 – the right to non-discrimination and to the correction of direct, indirect, unlawful, or abusive discriminatory biases; (BRASIL, Bill No. 2338, 2023). [24]

Article 19 further states that measures will be adopted to combat algorithmic discrimination:

24. BRASIL. Congresso Nacional. Projeto de Lei nº 2338, de 2023. Dispõe sobre a regulamentação da inteligência artificial. Available at: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1720798347645&disposition=inline. Accessed: July 24, 2024.

> Art. 19. Artificial intelligence agents shall establish governance structures and internal processes capable of ensuring the safety of systems and upholding the rights of affected persons, under the terms of Chapter II of this Law and the relevant legislation, which shall include, at a minimum: (...) III – appropriate data management measures to mitigate and prevent potential discriminatory biases; (BRASIL, Projeto de Lei nº 2338, 2023). [25]

Bill (PL) No. 2338/2023 demonstrates an attempt to combat algorithmic discrimination, laying the groundwork for the necessary regulation of this issue in an effort to eliminate discrimination in digital technologies.

Bill (PL) No. 2338/2023 has drawn various criticisms concerning its content and how it would operate. In Thiago Marcílio's view, the bill does not reflect the actual needs of artificial intelligence regulation and even conflicts with the General Data Protection Law (LGPD) itself. Nevertheless, it opens new horizons for networks in Brazil and should therefore be understood as a step toward the ideal in the world of networks. [26]

Although these proposals represent a normative ideal, their effective implementation in Brazil remains a distant prospect. The country still lacks a robust and effective legal framework for regulating artificial intelligence, preventing these objectives from being achieved in the near future. From an optimistic perspective, however, the very creation of a strong bill, even one with various problems, already marks the beginning of a path toward that ideal.

Final considerations

Algorithmic discrimination presents a critical challenge in the growing use of artificial intelligence technologies, reflecting and amplifying the biases and prejudices already present in society. This phenomenon does not arise from the technology itself, but from how data are collected and processed, as well as the biased choices made by the developers themselves. Therefore,

25. Ibid.

26. MARCÍLIO, Thiago. Quatro polêmicas sobre o projeto que regula a inteligência artificial. Consultor Jurídico, 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: October 14, 2024.

artificial intelligence, if not properly regulated and monitored, can perpetuate and intensify algorithmic discrimination, sustaining discriminatory guidelines that are rooted in society.

To combat algorithmic discrimination effectively, artificial intelligence regulation must be robust and effective. In Brazil, although the Constitution and the Racial Crime Law already prohibit discriminatory acts, there remains a significant gap in specific legislation addressing the unique challenges posed by artificial intelligence. A lack of transparency and the difficulty of tracing responsibility for the data and algorithms used make it harder to impose penalties and ensure algorithmic justice.

Artificial intelligence regulation must be developed with great care and an emphasis on 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 protects individual rights and promotes equity.

The global movement toward regulating intelligence, exemplified by the European Union's recent Artificial Intelligence Act, underscores the urgency and importance of this effort. In Brazil, Bill No. 2338/2023 represents a significant step, but there is still a long way to go.

In conclusion, algorithmic discrimination reflects society's thinking and has become a complex issue requiring a multifaceted approach involving legislation, monitoring, and broader social awareness. Only through a coordinated, sustained effort across society will it be possible to ensure that artificial intelligence contributes to a fairer and more inclusive society, rather than perpetuating the inequalities entrenched in society today.

References

AZEVEDO, Ingrid Borges de. Reconhecimento facial e direito: propostas para uma IA antidiscriminatória. 2021. 65 leaves. Undergraduate thesis (Law) – Universidade de Brasília, Brasília, 2021. Available at: https://bdm.unb.br/handle/10483/29805. Accessed: July 22, 2024.

BONA, Celito de; SCHONS, Eduarda Arruda; LOPES-FLOIS, Luiza. Inteligências artificiais: existe ética na implementação de algoritmos? Ciências Sociais Aplicadas em Revista, [S.L.], v. 25, no. 45, pp. 225-246, August 18, 2023. Universidade Estadual do Oeste do Paraná – UNIOESTE. Available at:

https://e-revista.unioeste.br/index.php/csaemrevista/article/view/31510/22369. Accessed: July 21, 2024.

BORGESIUS, F. J. Z. Strengthening legal protection against discrimination by algorithms and artificial intelligence. The International Journal of Human Rights, v. 24, no. 10, pp. 1572-1593, 2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561441. Accessed: July 18, 2024.

BRASIL. Congresso Nacional. Projeto de Lei nº 2338, de 2023. Dispõe sobre a regulamentação da inteligência artificial. Available at: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1720798347645&disposition=inline. Accessed: July 24, 2024.

BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, v. 81, pp. 1-15, 2018. Available at: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Accessed: July 15, 2024.

CHAVES JUNIOR, Airto; GUASQUE, Bárbara; PÁDUA, Thiago Santos Aguiar de. Segregação racial e vieses algorítmicos: máquinas racistas no âmbito do controle penal. Revista Brasileira de Direito, [S.L.], v. 19, no. 2, pp. 1-30, September 22, 2023. Complexo de Ensino Superior Meridional S.A. Available at: https://doi.org/10.18256/2238-0604.2023.v19i2.4768. Accessed: July 22, 2024.

HENRIQUES, Isabella Vieira Machado; SAMPAIO, Inês Vitorino. Discriminação algorítmica e inclusão em sistemas de inteligência artificial – uma reflexão sob a ótica dos direitos da criança no ambiente digital. Available at: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5993/pdf. Accessed: July 19, 2024.

HUPFFER, Haide Maria; SANTANNA, Gustavo da Silva. Inteligência artificial e discriminação algorítmica: marcos regulatórios e parâmetros éticos. Available at: http://www.guaritadigital.com.br/casaleirialivros/iasg/iasg.4.pdf. Accessed: 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: 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: July 17, 2024.

MARCÍLIO, Thiago. Quatro polêmicas sobre o projeto que regula a inteligência artificial. Consultor Jurídico, 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: 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: July 17, 2024.

NOBLE, S. U. *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: 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: July 18, 2024.

RESMINI, Carol; PAGLIARINI, Eduarda; MORAES, Júlia D'Alascio Rangel de; LANDMEIER, Laura Vardanega. Os desafios sociais na era da inteligência artificial: um enfoque na lacunar equidade racial. Available at: https://ojs.sites.ufsc.br/index.php/avant/article/view/7661/6164. Accessed: July 17, 2024.

SAMUEL, A. Some studies in machine learning using the game of checkers. IBM Journal of Research and Development, v. 3, no. 3, pp. 210-229, 1959. Available at: https://people.csail.mit.edu/brooks/idocs/Samuel.pdf. Accessed: July 17, 2024.

SINGAPORE. Personal Data Protection Commission. Modelo de Estrutura de Governança de IA. Available at: https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework. Accessed: 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, pp. 215–230, 2022. Available at: https://link.springer.com/article/10.1007/s00146-021-01154-8. Accessed: 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/discriminatingsystems.pdf. Accessed: July 22, 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

9

A critical analysis of discriminatory algorithmization in criminal law

LUISA AMELIA

Contents: Introduction. 1. Artificial intelligence: concept, evolution, and developments. 2. Algorithmic discrimination and its effects. 3. A critical analysis of the use of discriminatory algorithms in criminal law. Final considerations. References.

Introduction

Modern society, known as the information society [2], is driven by data at a wide range of levels concerning people, their habits, and their characteristics. Only after years of advances in data collection technologies did it become possible to mine and understand these data, a process known as processing. In this setting, everything we do—and even what we do not do, such as opening a sales page but deciding not to buy something online—remains recorded and is considered browsing data.

In this context, data have always been an important asset, but the ways of interpreting them, even with computational resources, have not always been so accurate. This has been changing, however, with the rise of data processing technologies and, more recently, artificial intelligence.

As a result, activities once considered highly complex have become simple because systems perform them accurately, and their use has expanded into fields such as medicine and law. In Brazil, for example, the Supreme Federal Court (STF) permits AI to analyze filed appeals to identify issues involving repetitive appeals, an approach that has proved efficient in terms of procedural speed and economy.

However, despite the importance of this technology for scientific progress worldwide, its use and rise are accompanied by concerns about its social, ethical, and legal implications, since these

1. Associate attorney at Peter Fernandes e Marihá Viana Advogados Associados. She holds a law degree from Centro Universitário de Brasília (UniCEUB) and a master's degree in Criminology, specializing in Criminal Policy, from Universitat de Barcelona, Spain. She is currently pursuing postgraduate studies in Digital Law at the Institute for Technology and Society (ITS), in partnership with the Universidade do Estado do 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 must not take precedence over people's rights [3]. This highlights the need to discuss the ethical, transparent, and responsible use of AI, as well as the regulation it requires. At the same time, this discussion must not lose sight of the need for continuing technological progress to coexist with effective protection of citizens' rights.

This study therefore seeks to critically analyze the risks of discriminatory decisions made by artificial intelligence in criminal law, together with their implications and possible proposals for addressing the situation. The study used a dialectical-deductive method, drawing on a literature review of scholarly articles, books, and relevant legislation, and was structured into three chapters.

The first chapter analyzes artificial intelligence, specifically its concept, uses, and the dynamics of the debate in Brazil. It also addresses the views set out in the literature, competition and ethical issues, regulatory proposals, and what is expected of effective regulation in Brazil.

The second chapter addresses algorithmic discrimination, considering the associated risks in AI decision-making. Given the possibility of decisions biased by negative human prejudices and preconceptions, it proposes an examination of the ethical limits and legal requirements involved.

Finally, the third chapter considers the hypothetical use of artificial intelligence in criminal law. The relevant literature shows that its use can perpetuate racist and segregationist decisions. The proposed response is therefore to prevent the use of systems that may exhibit discriminatory biases, in accordance with Resolution No. 332 of the National Council of Justice (CNJ) [4] and the new draft resolution developed by the Working Group on Artificial Intelligence in the Judiciary (GTIA), also of the CNJ [5]. It also emphasizes the importance of including human participation in AI decision-making processes.

3 MOURÃO, Licurgo; INDUSTRIAL, Revolução. Regulação da inteligência artificial no Brasil. Intellegentiae artificialis, imperium et civitatem, pp. 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: July 27, 2024.

4. Conselho Nacional de Justiça. Resolução n. 332, de 21 de agosto de 2020. Available at: https://atos.cnj.jus.br/atos/detalhar/3429. Accessed: July 29, 2024.

5 CONSELHO NACIONAL DE JUSTIÇA (CNJ). Minuta de proposta da resolução 332. Brasília: CNJ, 2024. Available at: https://www.cnj.jus.br/wp-content/uploads/2024/09/minuta-proposta-resolucao-332-cnj-rev.pdf. Accessed: October 13, 2024.

The final considerations highlight the risks of using automated systems in matters involving criminal law, given that it is already a discriminatory system in its own right.

1. **Artificial intelligence**: concept, evolution, and developments

The scientific community defines the term “artificial intelligence” as “the reasoning capacity of machines that reproduces the workings of the human mind” [6], as demonstrated by ChatGPT [7] (Generative Pre-Trained Transformer), software developed by OpenAI.

It is a prominent topic in social, political, and legal debates and in major media worldwide. This is due, in particular, to its promise to transform the way society is organized, marking the peak of technological development on a global scale. As a result, a race for development has emerged among countries seeking to lead the development and use of AI—a race concentrated, it should be noted, among established powers such as the United States and China. [8]

This rapid development, combined with its transformative potential, has underpinned the view that the planet is entering a new era. These technologies do indeed have substantial potential for change, raising the question of whether some professions will soon be replaced. AI is therefore transforming social structures, including how human beings interact with technology, leading the literature to describe the rise of a fourth Industrial Revolution. [9]

Indeed, the Organisation for Economic Co-operation and Development (OECD), in assessing the transformative potential of this technology, has drawn attention to the need to define ethical limits on its use, particularly because of the implications it may have for competition and democracy, as Mourão explains:

6. MOURÃO, Licurgo. Regulação da inteligência artificial no Brasil. Intellegentiae artificialis, imperium et civitatem, p. 73, 2022. Available at: https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74. Accessed: July 27, 2024.

7. ChatGPT “works from an up-to-date knowledge base that allows it to decode words to provide textual responses to people. It is a model trained on text data available on the internet” (FIA, 2024).

8. PARENTONI, Leonardo Netto; VALENTINI, Rômulo Soares; ALVES, Tárik César Oliveira E. Panorama da Regulação da Inteligência Artificial no Brasil: com ênfase no PL’s N. 5.051/2019. Revista Eletrônica do Curso de Direito da UFSM, v. 15, no. 2, p. 2, 2020.

9. MOURÃO, Licurgo; INDUSTRIAL, Revolução. Regulação da inteligência artificial no Brasil. Intellegentiae artificialis, imperium et civitatem, p. 73, 2022. Available at: https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74. Accessed: July 27, 2024.

> [...] the Organisation for Economic Co-operation and Development (OECD), recognizing that artificial intelligence is transforming societies, economic sectors, and the future of work, and that it has the potential to help address major global challenges, stressed that the transformations brought about by technological progress may affect societies and economies unevenly. This is particularly true of competition, labor market transitions, inequalities, and implications for democracies and human rights, privacy and data protection, and digital security. In this setting, growing worldwide concern can be seen over defining ethical standards and limits for the use of artificial intelligence, seeking to regulate new technologies in a way that safeguards citizens' rights. [10]

In a short period, artificial intelligence has developed the ability to make decisions autonomously—that is, without human intervention after an algorithm has been formulated. This has been made possible through machine learning mechanisms combined with deep learning techniques. These developments have been so remarkable that, in 2024, a particular artificial intelligence system already has the ability to create another, as well as to integrate with other systems to improve results. [11]

In Brazil, for example, since 2020, the Supreme Federal Court (STF) has used machine learning models to analyze appeals received by the Court that concern matters of general repercussion. [12]

This use of the mechanism by Brazil's Supreme Court has made it possible to achieve “speed and accuracy in analyzing a substantial number of cases and situations, encompassing the important principles of speed, efficiency, and economy” [13]. This demonstrates the advantage of using such systems, insofar as they facilitate human activity and can

10. MOURÃO, Licurgo. Regulação da inteligência artificial no Brasil. Intellegentiae artificialis, imperium et civitatem, pp. 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: July 27, 2024.

11. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, v. 11, no. 3, p. 3, 2022. Available at: https://civilistica.emnuvens.com.br/redc/article/view/804/650. Accessed: July 24, 2024.

12 MAIA FILHO, Mamede Said; JUNQUILHO, Tainá Aguiar. Projeto Victor: perspectivas de aplicação da inteligência artificial ao direito. Revista de Direitos e Garantias Fundamentais, v. 19, no. 3, p. 218, 2018.

13 PEIXOTO, Fabiano Hartmann. Projeto Victor: relato do desenvolvimento da inteligência artificial na repercussão geral do Supremo Tribunal Federal. Revista Brasileira de Inteligência Artificial e Direito-RBIAD, v. 1, no. 1, p. 18. Available at: https://www.rbiad.com.br/index.php/rbiad/article/view/4/4. Accessed: July 25, 2024.

deliver a positive outcome for society. As noted earlier, however, a positive outcome in this respect does not remove the need to handle the subject with the care it requires. Nor does it diminish the urgency of regulation establishing ethical and legal criteria, so that development continues in strict compliance with the law.

Regarding this last point, Brazil's General Personal Data Protection Law (Law No. 13.709/2018 – LGPD) opened the door to regulation by allowing data subjects to request a review of automated decisions, as provided in Art. 20 [14]. However, far from regulating the subject, the law merely highlighted the need to address it carefully, since its impact extends beyond personal data to a range of other rights and social issues.

In 2020, Resolution No. 332/2020 of the National Council of Justice [15] established rules on ethics, transparency, and governance for the use of artificial intelligence by the judiciary [16]. This legislation was an important milestone in addressing the issue within the Brazilian judiciary, particularly given the alarming evidence of biased decisions of a discriminatory and even racist nature, which will be discussed specifically later in this study. A new draft resolution has now been developed by the Working Group on Artificial Intelligence in the Judiciary (GTIA), also of the CNJ. [17]

The federal executive branch is likewise working to develop a “Brazilian Artificial Intelligence Strategy” (EBIA), established by MCTI Ordinance No. 4.617/2021. Its premise is to “guide the Brazilian state's actions toward developing initiatives, across their various dimensions, that encourage research, innovation, and the development of artificial intelligence solutions, as well as their conscious, ethical use in the pursuit of a better future” [18].

14. Art. 20. Data subjects have the right to request a review of decisions made solely on the basis of automated processing of personal data that affect their interests, including decisions intended to define their personal, professional, consumer, and credit profiles or aspects of their personality.

15. Conselho Nacional de Justiça. Resolução n. 332, de 21 de agosto de 2020. Available at: https://atos.cnj.jus.br/atos/detalhar/3429. Accessed: July 29, 2024.

16 MOURÃO, Licurgo; INDUSTRIAL, Revolução. Regulação da inteligência artificial no Brasil. 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: July 27, 2024.

17 CONSELHO NACIONAL DE JUSTIÇA (CNJ). Minuta de proposta da resolução 332. Brasília: CNJ, 2024. Available at: https://www.cnj.jus.br/wp-content/uploads/2024/09/minuta-proposta-resolucao-332-cnj-rev.pdf. Accessed: October 13, 2024.

18 BRASIL. Ministério da Ciência, Tecnologia e Inovação. Inteligência Artificial. Available at: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial. Accessed: July 29, 2024.

EBIA represents a notable initiative by the federal executive branch, through the Ministry of Science and Technology. It enabled a cross-cutting discussion of the subject, from the opening of a public consultation that allowed participation by various sectors of society to the publication of a framework covering several areas. The literature nevertheless argues that it is far from being a strategy, resembling little more than a statement of intent because its proposals are generic and lack a pragmatic approach. [19]

It is therefore clear that the few steps taken in practice by the Brazilian state still do not meet legitimate expectations for regulation of this matter, despite its urgency and necessity.

It is also important to note that several bills to regulate the subject are being considered by the National Congress (CN). Particular attention should be paid to Bill 2.338/2023, introduced by Senator Rodrigo Pacheco (PSD/MG). Its proposals are founded on the centrality of the human person (Art. 2, item I of the Bill) and also take free enterprise as a premise (Art. 2, item VII), with an approach expressly oriented toward Economic Freedom. After lengthy consideration by various congressional committees, however, the breadth of the issue meant that consensus in the legislature remained elusive in the second half of 2024.

Much of the discussion in the National Congress therefore concerns the search for a balance between the centrality of the human person, with the corresponding protection of dignity and fundamental rights, and the continuation of technological and scientific development.

Against this backdrop of shaping a regulatory framework for artificial intelligence, Mourão observes:

> Given the challenges arising from the use of artificial intelligence, the main regulatory principles that should guide the drafting of laws on the subject are: a) the general interest, ensuring inclusion and equity, since public authorities must not seek to satisfy private interests at the expense 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. A Inteligência Artificial no Brasil ainda precisa de uma estratégia. Fundação Getúlio Vargas, Rio de Janeiro, 2021. Available at: https://direitorio.fgv.br/sites/default/files/2022-08/ebia-pt-br.pdf. Accessed: July 27, 2024.

> carried out by artificial intelligence systems; c) transparency, to ensure that their operation can be understood (with regard to algorithms, data, tests, and validations performed, as well as the list of areas using these technologies). [20]

This shows the particular importance of the general interest, human rights, and transparency. At the same time, the need to ensure technological progress toward ever more suitable solutions must not be overlooked. In other words, AI regulation should not be seen as a barrier to progress. On the contrary, it should ensure that AI evolves in accordance with justice and ethics, with this balance regarded as the high point of regulation.

2. Algorithmic discrimination and its effects

The use of artificial intelligence in everyday processes offers advantages such as saving time, establishing parameters for choices, and facilitating various activities. There are even views within the scientific community that reliance on automated decision-making [21] is linked to its neutrality, given its objectivity and use of mathematical criteria. In theory, this could solve problems associated with human decision-making, which is subject to errors and cognitive biases. [22]

As already explained, however, various difficulties arise in practice, depending on how AI is used. In this context, AI has several characteristics, including:

> “i) opacity, which often means that even developers do not know precisely why algorithms reached their conclusions.” Questions can also be raised about “ii) the quality of the data used to ‘run’ algorithms, which may carry biases implicit in their programming or acquire them later through network interaction, making automated decisions fertile ground for discrimination, particularly against more vulnerable groups.” [23]

20. MOURÃO, Licurgo; INDUSTRIAL, Revolução. Regulação da inteligência artificial no Brasil. 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: July 27, 2024.

21. An algorithmic or automated decision refers to a decision made by an algorithm without human intervention.

22. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, v. 11, no. 3, p. 3, 2022. Available at: https://civilistica.emnuvens.com.br/redc/article/view/804/650. Accessed: July 24, 2024.

23. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, v. 11, no. 3, p. 2, 2022. Available at: https://civilistica.emnuvens.com.br/redc/article/view/804/650. Accessed: July 24, 2024.

See Costa Requião's explanation detailing the algorithm's discriminatory bias:

> [...] AI and the algorithmic process are not only incapable of correcting subjective human error; they can also replicate and even reinforce prejudices that exist in society, producing distinctions, preferences, or exclusions capable of affecting equal treatment among individuals, particularly vulnerable groups. This is known as the algorithm's discriminatory bias or, simply, algorithmic discrimination.[24]

The author further explains that algorithmic discrimination can occur in two ways: "i) when algorithms reflect human prejudices (conscious or otherwise) embedded in their programming; ii) when they encounter databases containing prejudicial biases, causing the algorithm to 'learn' to discriminate."[25]

On this subject, Mendes and Mattiuzzo make an interesting observation:

> [...] 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 they concern not as individuals in their own right, but merely as members of a group. This is because, in our view, a classification, even one that is statistically consistent, can in some cases prove unfair.[26]

In the same article, the authors identify 4 (four) types of algorithmic discrimination, without ruling out other types. They describe "discrimination caused by statistical error," referring to technical errors, such as flaws in the algorithm's code that may lead to an incorrect analysis of data. They also identify "discrimination through generalization," which occurs when an algorithm treats a generalization as

24. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, vol. 11, no. 3, p. 4, 2022. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Accessed July 24, 2024.

25. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, vol. 11, no. 3, p. 4, 2022. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Accessed July 24, 2024.

26. MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. Direito Público, vol. 16, no. 90, p. 51, 2019. Available at: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>. Accessed July 24, 2024.

absolute truth, disregarding variations and exceptions, which is an error in the context of probability.[27]

The third type is “discrimination through the use of sensitive information,” referring to the use of data such as health or religion to make decisions. It involves data that should not be used for certain purposes and whose use for those purposes is prohibited under Brazilian law. Finally, there is “discrimination that limits the exercise of rights,” arising when the relationship between the information used and the right is so direct that it restricts or impairs a person’s ability to exercise that right.[28]

This understanding makes clear that its occurrence undermines important fundamental rights, such as equality and equal treatment under the law, by restricting people’s rights and benefits through generalizations. Moreover, using these generalizations as the basis for decision-making “may have side effects; that is, discrimination against certain groups in society may be intensified.”[29]

On this subject, Wimmer and Doneda consider AI systems inherently prone to failure, particularly because they make choices using mechanisms that are neither precise nor neutral. This may produce unacceptable outcomes arising, for example, from the internalization of cultural biases and racial and gender stigmas, while also harming individuals belonging to specific ethnic and social groups.[30]

An analysis of generalizations and the feeding of data thus shows that AI decisions express the human status quo, making predictions and perpetuating patterns of inequality. “Worse still, they can reinforce them even further: by deliberately ignoring the structural inequalities in the data they use, they end up magnifying them.”[31]

Thus, for the digital system to function coherently, there must be, at a minimum, large-scale data

27. MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. Direito Público, vol. 16, no. 90, pp. 52-53, 2019. Available at: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>. Accessed July 24, 2024.

28. MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. Direito Público, vol. 16, no. 90, pp. 52-53, 2019. Available at: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>. Accessed July 24, 2024.

29. MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. Direito Público, vol. 16, no. 90, p. 54, 2019. Available at: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>. Accessed July 24, 2024.

30. WIMMER, Miriam and DONEDA, Danilo. “Falhas de IA” e a Intervenção Humana em Decisões Automatizadas: Parâmetros para a Legitimação pela Humanização, Revista de Direito Público, Brasília, vol. 18, no. 100, p. 380, October/December 2021.

31. BEZERRA, Arthur Coelho; COSTA, Camila Mattos. Pele negra, algoritmos brancos: informações e racismo nas redes sociotécnicas. Liinc em Revista, Rio de Janeiro, vol. 18, no. 2, p. 6, e6043, November 2022.

mining[32] (data mining), since data feed and guide the operation of applications and artificial intelligence solutions.

Various protocols must be adopted in this process, particularly because much of the data routinely used by the technology is sensitive and receives stronger protection.

3. The use of discriminatory algorithms in criminal law

Given the discriminatory phenomenon in some algorithms, a brief analysis of the application of artificial intelligence in Brazilian criminal law is particularly relevant. This field also perpetuates segregation, as Black and Brown (pardo) people and people with low levels of education make up most of the prison population, according to the 2023 Criminal Information Report.[33]

As noted, this branch of public law involves various complexities associated with discrimination that results in social labeling and selectivity in the criminal justice system.

On social labeling, Howard S. Becker observes:

> Because deviance is, among other things, a consequence of others' reactions to a person's act, those studying deviance cannot assume that they are dealing with a homogeneous category when they study people labeled as deviant. That is, they cannot assume that these people have actually committed a deviant act or broken a rule, because the labeling process may not be infallible: some people may be labeled as deviant without actually having broken a rule. Nor can they assume that the category of those labeled includes everyone who has actually broken a rule, because many rule-breakers may escape detection and thus fail to be included in the population of "deviants" they study.[34]

32. Data mining refers to the process of exploring large datasets to discover meaningful patterns, trends, and relationships (Gropp, Motta, 2020).

33. SENAPEN – National Secretariat for Penal Policies. Sistema Nacional de Informações Penais. 15th SISDEPEN Cycle. Period: July to December 2023. Relatório de Informações Penais. Brasília, 2024. Available at: <https://www.gov.br/senappen/pt-br/servicos/sisdepen/relatorios>. Accessed July 03, 2024.

34. BECKER, Howard. Outsiders. Translated by Maria Luiza X. de Borges; technical review by Karina Kuschnir. Rio de Janeiro: Zahar, 2008, p. 22.

According to this criminological approach, for particular conduct to be considered a crime, it undergoes a labeling process in which that action, performed by a particular person, must be characterized as such. As the quoted passage indicates, many people may engage in conduct described as criminal without being considered deviant, and vice versa.

In other words, an individual's identity matters much more than the conduct itself. Selectivity in the criminal justice system thus emerges as an interrelated and logical consequence.

In the context of criminalization, Vera Batista comments on this process of selectivity:

> [...] it is far more accurate to call 'recorded criminality' criminalization, because the criminal justice system's operational selectivity, by qualitatively and quantitatively shaping the ultimate outcome of secondary criminalization—that is, who and how many enter the records—makes it a process that shapes 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 that reason by traffic authorities (criminalization). Yet it is only through this second number, which is actually a human construct dependent on factors as diverse as the officer's mood, the location of the surveillance camera, and so on, that we can study the incidence of violations.[35]

In this sense, it bears emphasizing once again that the labeling present in society is reflected in the prison population, as Luisa Silva explains:

> Selectivity demonstrates the existence of a preferred profile among those subjected to imprisonment in Brazil. It consists of filtering between latent criminality and criminality pursued by the authorities, occurring in both primary and secondary criminalization. The reasons include factors such as social standing, education, ethnicity, and ways of dressing, communicating, and behaving. The last three reveal the class to which an individual belongs in relation to the first two, among other mechanisms of social division. It must also be considered that, since state control agencies lack the means necessary to effectively process every act that meets the statutory definition of an offense, they

35. BATISTA, Vera Malaguti. Introdução crítica à criminologia brasileira. 2nd edition. Rio de Janeiro: Revan, 2012, p. 22.

> determine the quality of the attention given to the incidents that come to their knowledge.[36]

This phenomenon of selectivity is itself a problem arising in the racist and class-based context of modern society. It becomes worse, however, when automated decision-making systems, fed with data reflecting social reality, reproduce stigmas and prejudicial biases through generalizations and the replication of human prejudices.

Many advocates of using AI in justice systems, particularly in criminal law, argue that automating proceedings can bring benefits such as cost savings and faster proceedings. However, these benefits ultimately come at the expense of human rights and human dignity, as Piló and Brasil explain.[37] Against this backdrop, Bichara, Cascardo Junior, and Perazzoni explain:

> Using AI to examine crime-related data brings a risk of intensifying stereotypes and prejudices already present in society. Algorithms used to predict offenses or identify suspects tend to replicate biases in the data used, perpetuating racial and social inequalities.[38]

Thus, in analyzing the use of AI in criminal justice, Santos, Torres, and Celestino found that Black people were more likely to be incarcerated than White people because of the generalizations made by the machine.[39]

The authors further explain, in discussing police security services:

> In the criminal justice sector, it is argued that, because the predictions of machine learning algorithms depend on the quality of the training data, public police security services in different regions may be affected in at least

36. SILVA, Luisa Cypriano Moreira da. Sistema carcerário brasileiro: uma análise do perfil dos presos a partir das teorias da seletividade penal e do etiquetamento social. 2019, p. 20. Universidade Federal de Ouro Preto. Department of Law. Monograph. Available at: <https://monografias.ufop.br/bitstream/35400000/2399/7/MONOGRAFIA_SistemaCarcer%c3%a1rioBrasileiro.pdf>. Accessed July 29, 2024.

37. PILÓ, Xenofontes Curvelo; BRASIL, Deilton Ribeiro. A utilização da inteligência artificial no direito penal e seus reflexos nas garantias e direitos fundamentais. Revista EJEF, no. 1, pp. 294-295, 2022.

38. BICHARA, Anderson Andrade; CASCARDO JR, Agostinho Gomes; PERAZZONI, Franco. Racismo algorítmico, reforço de preconceitos e uso de IA: perspectivas e desafios para a investigação criminal digital. Boletim IBCCRIM, vol. 32, no. 379, p. 24, 2024.

39. SANTOS, Adriane de Almeida; TORRES, Marck de Souza; CELESTINO, Victor. Discriminação algorítmica e o acirramento do racismo estrutural: revisão de escopo. Revista Científica Integrada, vol. 7, no. 1, p. 5, e202415-e202415, 2024. Available at: <https://revistas.unaerp.br/rci/article/view/3233/2422>. Accessed July 24, 2024.

> two distinct ways: (1) communities with a history of troubled relations with the police may underreport criminal activity in their area. When these data are used in algorithmic decision-making systems, the system may assign the area crime and safety levels that do not reflect reality and fail to allocate adequate police resources and assistance; (2) algorithmic systems not trained [sic] on data incorporating racial stereotypes associated with crime may indicate that areas with greater police pressure than areas with a higher density of Black residents should receive greater police pressure than areas whose populations are predominantly White. The combination of these algorithmic practices contributes to concentrating security resources in privileged areas inhabited predominantly by White people, while peripheral areas with predominantly Black populations are subjected to police coercion, further entrenching racial disparities.[40]

The case described makes clear the potential for segregation in algorithmic decisions, which may extend from devising a strategy to address a problem to the action taken in a particular case.

It is therefore important to consider the risk of allowing AI to adopt a more punitive approach toward specific groups at the expense of others. In other words, what is already seen in everyday Brazilian legal practice may be aggravated in the context of AI, which uses this type of metric to rationalize patterns through generalization.

In this context, there are already explicit cases of discriminatory algorithmic processing in AI systems used in Brazilian criminal law. One example is facial recognition, which police authorities are widely using to identify possible offenders. Although this type of technology has proved problematic in countries such as the United States, where racist and segregationist bias and low accuracy in identifying people have been demonstrated, Brazil imported the model to help arrest individuals wanted by the police.[41]

However, the same outcome is occurring in Brazil, according to the literature on the subject:

40. SANTOS, Adriane de Almeida; TORRES, Marck de Souza; CELESTINO, Victor. Discriminação algorítmica e o acirramento do racismo estrutural: revisão de escopo. Revista Científica Integrada, vol. 7, no. 1, p. 5, e202415-e202415, 2024. Available at: <https://revistas.unaerp.br/rci/article/view/3233/2422>. Accessed July 24, 2024.

41. CHAVES JÚNIOR, Airto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Segregação racial e vidas algorítmicas: máquinas racistas no âmbito do controle penal. Revista Brasileira de Direito, vol. 2, p. 19, 2023. Available at: <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768>. Accessed August 05, 2024.

> [...] after about a year of use, statistics concerning the model's bias had already begun to emerge. A survey by the Rede de Observatórios da Segurança found that, of the 151 arrests made through facial recognition systems in the country, 90% involved Black people (Chaves Jr., Guasque, De Pádua, 2023, p. 20).

It is noteworthy that, internationally, there is a growing movement of cases challenging algorithmic discrimination in facial identification, some even calling for this type of technology to be banned. In Brazil, by contrast, the states are encouraging the use of such tools, with federal government funding, as a form of public security policy.[42]

Catiane Steffen explains that criminal law is one of the fields with the greatest potential for discrimination by AI-based algorithms.[43] The author discusses techniques that, at first glance, could theoretically help authorities establish who committed crimes and whether the offenses occurred, thereby improving the production of evidence. However, she states:

> [...] while the state's preventive and punitive capacity increases, so does the possibility of violating citizens' rights over their personal data stored—with or without their consent—in government public security databases. Another of the many possible violations of rights involves creating criminal profiles that infer an individual's potential to cause harm from physical, emotional, and social characteristics, intensifying state intervention in groups already stigmatized or discriminated against in a given society.[44]

In view of all the difficulties discussed, CNJ Resolution No. 332 was an important milestone in addressing this issue by regulating the use of AI within the judiciary. Mourão explains the solution provided by the resolution for cases in which an AI system may exhibit discriminatory biases:

42. CHAVES JÚNIOR, Airto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Segregação racial e vidas algorítmicas: máquinas racistas no âmbito do controle penal. Revista Brasileira de Direito, vol. 2, p. 20, 2023. Available at: <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768>. Accessed August 05, 2024.

43. STEFFEN, Catiane. A inteligência artificial e o processo penal: a utilização da técnica na violação de direitos. Revista da EMERJ, vol. 25, no. 1, p. 112, 2023.

44. STEFFEN, Catiane. A inteligência artificial e o processo penal: a utilização da técnica na violação de direitos. Revista da EMERJ, vol. 25, no. 1, p. 113, 2023.

> The resolution requires the development, deployment, and use of artificial intelligence to respect fundamental rights, and requires the use of technology to seek to ensure legal certainty and equality. To this end, it provides that, before deployment, the system must undergo approval to identify whether prejudices or generalizations influenced its development, producing discriminatory tendencies in its operation. If the discriminatory bias cannot be remedied, the model may not be used.[45]

In this case, the CNJ had already anticipated the need for approval and testing capable of assessing an AI system's discriminatory bias before it is authorized and subsequently used within the judiciary, including decisions in criminal law.

The resolution addressed the issue specifically in the criminal context in Article 23, as follows:

> Art. 23. The use of Artificial Intelligence models in criminal matters should not be encouraged, particularly with regard to suggestions for predictive decision models. § 1. The provision in the main paragraph does not apply to computational solutions intended for automation and for providing support for calculating sentences and limitation periods, checking recidivism, mapping, classifying, and screening case files for caseload management. § 2. Artificial Intelligence models intended to check criminal recidivism must not indicate a conclusion more detrimental to the defendant than the one the judge would reach without using them. (BRASIL, 2020).

Chaves Júnior, Guasque, and De Pádua attest that the absence of regulation on this subject poses risks in every sphere, particularly the indiscriminate use of AI by the criminal justice system. According to the authors:

> This lack of regulation, accountability, auditing, and transparency in the use of AI has had harmful consequences from a legal and social standpoint, as it perpetuates and expands the discrimination and selectivity that permeate the criminal justice system and its constituent agencies. All of this occurs under the illusory impression that it is based on mathematical models that are impartial, precise, and

45. MOURÃO, Licurgo; INDUSTRIAL, Revolução. Regulação da inteligência artificial no Brasil. 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 July 27, 2024.

> objective. In reality, the results are laden with subjectivity and racist biases that tend to push clearly defined segments of society toward marginalization and discrimination.[46]

The specialized legal literature has likewise proposed limiting the collection and processing of sensitive personal data as a solution to the problems identified here. It has also drawn attention to the algorithmic governance tools provided by the LGPD, such as auditing machine decisions. However, this alone is still insufficient to resolve the issue, since "in a scenario of interaction with big data, in which all data are potentially sensitive, merely ensuring 'algorithmic neutrality' and subsequent control of the algorithm is not enough to mitigate discrimination."[47] In this context, Requião and Costa emphasize:

> According to the specialized literature, resolving the problem of opacity requires strict adherence to the principle of transparency, understood through the right to an explanation of algorithmic decisions. On the basis of this principle, it is necessary to ensure that every stage of the algorithm can be explained in a way that a nonspecialist can understand. Algorithm designers must also always retain the ability to provide transparency regarding the entire algorithmic process involved and explanations for the decisions and outcomes reached.[48]

However, this solution alone is insufficient, because the discussion is not limited to the principles of nondiscrimination, transparency, and explanation, given AI systems' high degree of complexity and autonomy.[49]

Accordingly, Wimmer and Doneda consider the need for human participation in machine decision-making, particularly because

46. CHAVES JÚNIOR, Airto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Segregação racial e vidas algorítmicas: máquinas racistas no âmbito do controle penal. Revista Brasileira de Direito, vol. 2, p. 20, 2023. Available at: <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768>. Accessed August 05, 2024.

47. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, vol. 11, no. 3, pp. 2-3, 2022. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Accessed July 24, 2024.

48. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, vol. 11, no. 3, p. 6, 2022. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Accessed July 24, 2024.

49. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, vol. 11, no. 3, pp. 6-7, 2022. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Accessed July 24, 2024.

many of their errors arise from a lack of critical understanding of the situation being assessed.[50]

The presence of discriminatory algorithms in AI tools therefore makes human intervention important. However, the fact that the data entered into these systems reflect society cannot be disregarded. Specifically in criminal law, then, the use of artificial intelligence does not currently appear sound until effective regulation is in place, as it poses a systemic risk to human dignity.

Final considerations

An analysis of the literature, including actual cases, led to the conclusion that using artificial intelligence in everyday criminal law practice poses an alarming risk in a field already marked by selectivity, stigmas, and prejudices.

In other words, the use of artificial intelligence in criminal law is extremely risky, given the evidence of the discriminatory bias the technology may adopt and the consequences of its generalization model. These practices reinforce social stigmas and perpetuate injustices associated with the criminalization of Black people and people with low incomes.

In this sense, the use of AI in criminal matters is premature, both because of the algorithm's discriminatory risks and because of the technology's margins of error. CNJ Resolution No. 332 is therefore right to discourage automated systems in criminal law, emphasizing the sensitivity of the issue and the risks to people.

It also became clear that, if AI is used, human participation in decision-making stages is necessary, without these technologies making autonomous decisions, particularly when individual and collective fundamental rights may be affected. This intervention is justified as a means of ensuring compliance with ethical limits.

Finally, the study demonstrates the importance of an educational foundation covering subjects such as structural racism, criminology,

50. WIMMER, Miriam and DONEDA, Danilo. "Falhas de IA" e a Intervenção Humana em Decisões Automatizadas: Parâmetros para a Legitimação pela Humanização, Revista de Direito Público, Brasília, vol. 18, no. 100, p. 382, October/December 2021.

and other topics, directed at developers of artificial intelligence programs so that they can interrupt the reproduction of society's racism.

Technology could then be developed with due regard for ethics, human dignity, and all other constitutionally guaranteed fundamental rights. This would represent a preventive approach incorporating a safety protocol from the outset of technological development and would prevent problems during use.

References

BATISTA, Vera Malaguti. Introdução crítica à criminologia brasileira. 2nd edition. Rio de Janeiro: Revan, 2012.

BECKER, Howard. Outsiders. Translated by Maria Luiza X. de Borges; technical review by Karina Kuschnir. Rio de Janeiro: Zahar, 2008.

BEZERRA, Arthur Coelho; COSTA, Camila Mattos. Pele negra, algoritmos brancos: informações e racismo nas redes sociotécnicas. Liinc em Revista, Rio de Janeiro, vol. 18, no. 2, e6043, November 2022.

BICHARA, Anderson Andrade; CASCARDO JR, Agostinho Gomes; PERAZZONI, Franco. Racismo algorítmico, reforço de preconceitos e uso de IA: perspectivas e desafios para a investigação criminal digital. Boletim IBCCRIM, vol. 32, no. 379, pp. 23-26, 2024.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. Inteligência Artificial. Available at: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial. Accessed July 29, 2024.

_____. Conselho Nacional de Justiça. Resolução n. 332, de 21 de agosto de 2020. Available at: https://atos.cnj.jus.br/atos/detalhar/3429. Accessed July 29, 2024.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). Minuta de proposta da resolução 332. Brasília: CNJ, 2024. Available at: https://www.cnj.jus.br/wp-content/uploads/2024/09/minuta-proposta-resolucao-332-cnj-rev.pdf. Accessed October 13, 2024.

_____. Presidência da República. Lei nº 13.709, de 14 de agosto de 2018. Provides for the protection of personal data and amends Law No. 12.965, of April 23, 2014 (Brazilian Civil Rights Framework for the Internet). Brasília, DF: Presidência da República, 2018. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed July 31, 2024.

_____. Senado Federal. Projeto de Lei nº 2338, de 2023. Provides for the use of Artificial Intelligence. Brasília, DF: Senado Federal, 2023. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Accessed July 31, 2024.

CHAVES JÚNIOR, Airto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Segregação racial e vidas algorítmicas: máquinas racistas no âmbito do controle penal. Revista Brasileira de Direito, vol. 2, p. 4768, 2023. Available at: https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768. Accessed August 05, 2024.

FIA – Fundação Instituto de Administração. ChatGPT: o que é, como funciona e como usar a ferramenta. Available at: https://fia.com.br/blog/chat-gpt/. Accessed July 25, 2024.

GASPAR, Walter Britto; MENDONÇA, Yasmin Curzi de. A Inteligência Artificial no Brasil ainda precisa de uma estratégia. Fundação Getúlio Vargas, Rio de Janeiro, 2021. Available at: https://direitorio.fgv.br/sites/default/files/2022-08/ebia-pt-br.pdf. Accessed July 27, 2024.

MOURÃO, Licurgo. Regulação da inteligência artificial no Brasil. Intellegentiae artificialis, imperium et civitatem, pp. 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 July 27, 2024.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. Direito Público, vol. 16, no. 90, 2019. Available at: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Accessed July 24, 2024.

MAIA FILHO, Mamede Said; JUNQUILHO, Tainá Aguiar. Projeto Victor: perspectivas de aplicação da inteligência artificial ao direito. Revista de Direitos e Garantias Fundamentais, vol. 19, no. 3, pp. 218-237, 2018.

PARENTONI, Leonardo Netto; VALENTINI, Rômulo Soares; ALVES, Tárik César Oliveira E. Panorama da Regulação da Inteligência Artificial no Brasil: com ênfase no PL's N. 5.051/2019. Revista Eletrônica do Curso de Direito da UFSM, vol. 15, no. 2, 2020.

PEIXOTO, Fabiano Hartmann. Projeto Victor: relato do desenvolvimento da inteligência artificial na repercussão geral do Supremo Tribunal Federal. Revista Brasileira de Inteligência Artificial e Direito-RBIAD, vol. 1, no. 1, pp. 1-22, 2020. Available at: https://www.rbiad.com.br/index.php/rbiad/article/view/4/4. Accessed July 25, 2024.

PILÓ, Xenofontes Curvelo; BRASIL, Deilton Ribeiro. A utilização da inteligência artificial no direito penal e seus reflexos nas garantias e direitos fundamentais. Revista EJEF, no. 1, pp. 269-299, 2022.

REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, vol. 11, no. 3, pp. 1-24, 2022. Available at: https://civilistica.emnuvens.com.br/redc/article/view/804/650. Accessed July 24, 2024.

SANTOS, Adriane de Almeida; TORRES, Marck de Souza; CELESTINO, Victor. Discriminação algorítmica e o acirramento do racismo estrutural: revisão de escopo. Revista Científica Integrada, vol. 7, no. 1, pp. e202415-e202415, 2024. Available at: https://revistas.unaerp.br/rci/article/view/3233/2422. Accessed July 24, 2024.

SENAPEN – National Secretariat for Penal Policies. Sistema Nacional de Informações Penais. 15th SISDEPEN Cycle. Period: July to December 2023. Relatório de Informações Penais. Brasília, 2024. Available at: https://www.gov.br/senappen/pt-br/servicos/sisdepen/relatorios. Accessed July 03, 2024.

SILVA, Luisa Cypriano Moreira da. Sistema carcerário brasileiro: uma análise do perfil dos presos a partir das teorias da seletividade penal e do etiquetamento social. 2019. Universidade Federal de Ouro Preto. Department of Law. Monograph. Available at: https://monografias.ufop.br/bitstream/35400000/2399/7/MONOGRAFIA_SistemaCarcer%c3%a1rioBrasileiro.pdf. Accessed July 29, 2024.

STEFFEN, Catiane. A inteligência artificial e o processo penal: a utilização da técnica na violação de direitos. Revista da EMERJ, vol. 25, no. 1, pp. 105-129, 2023.

WEBSTER, Frank. Theories of the information society. London: Routledge, 1995.

WIMMER, Miriam and DONEDA, Danilo. “Falhas de IA” e a Intervenção Humana em Decisões Automatizadas: Parâmetros para a Legitimação pela Humanização, Revista de Direito Público, Brasília, vol. 18, no. 100, pp. 374-406, October/December 2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

10

Between Brain and Computer: Dialogues on Neurorights and Artificial Intelligence

HENRIQUE SEGOLIN MOLINA

Contents: Introduction; 1. How neurotechnologies and AI are influencing the creation of new rights; 2. Pathways and proposals for realizing neurorights; 2.1. Analysis of laws and regulations around the world; 2.3. The Chilean Case: Girardi v. Emotiv Inc.; Final Considerations; Bibliographic References

Introduction

The human brain differs from every other organ because it generates all our mental and cognitive activities, allowing us to consider it the most complex and powerful computer in the world.[2]

The search for new ways to understand and expand the limits of our mental capacities has been the subject of research and development for several decades. It lies at the heart of neuroscience and invasive technologies that allow machines to interact directly with regions of the brain.

In 1924, Hans Berger performed the first electroencephalogram (EEG) on humans, an achievement that represented a true revolution at the time. Using silver electrodes and a galvanometer, Berger captured and recorded the first brain waves, now known as alpha and beta waves. This historic moment not only demonstrated the feasibility of recording and analyzing the human brain's electrical activity but also launched a promising new field of scientific research.

Later, the invention of cochlear implants in 1957 marked a crucial point in the development of neurotechnologies intended to control electrical devices, such as lamps, using electrodes that can measure and respond to brain signals. These constitute what we now call brain-computer interfaces (BCIs).[3]

Normally, when we want to interact with an object in our environment, our nervous system goes through several preliminary neurological stages before sending the nerve impulses that will allow the interaction to occur. BCIs, in turn, shorten this

1. Postgraduate student in Digital Law and New Technologies at the Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS RIO), in partnership with the Universidade do Estado do Rio de Janeiro (UERJ). Graduate of the Pontifícia Universidade Católica de São Paulo (PUC-SP). Attorney.

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 June 10, 2024.

3. LOTTE, F. NAM, C. S. 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. Available at: https://inria.hal.science/hal-01656743/document. Accessed June 10, 2024.

path by using software and technologies that identify the intended action and execute it promptly. For this reason, they have potential applications in a variety of fields.

On this subject, around mid-2017, Brazilian neuroscientist Miguel Nicolelis expressed an optimistic and provocative view of BCIs' potential 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 listen to and decode increasingly complex neural symphonies, neuroscience will ultimately expand human capacity to almost unimaginable limits, allowing it to be expressed far beyond the boundaries and limitations imposed both by our fragile primate bodies and by our sense of self [...] Surprisingly, future
> BCI applications promise to extend far beyond the boundaries of medicine. Within a few generations, their technological development will enable our descendants to perform actions and experience sensations that few today could imagine how to put into words. BCIs may transform the way we interact with the tools we make to engage with the world around us, the way we communicate with one another, and our interaction with the distant environment and other worlds. To understand what this future might hold, you would first need to imagine how our lives would change dramatically if some of our most routine tasks could be performed directly under the control of our brain's electrical activity, freely transmitted through the air just as radio waves travel today [...] The prospect of this wonderful liberation, which may still sound to some like magic, a 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. (emphasis added)[4]

Today, we can say that we are in the "second machine age,"[5] in which new discoveries occur simultaneously in a wide range of fields, in a complete fusion of the most advanced technology with the physical, digital, biological,[6] and neuroscientific domains.

4. NICOLELIS, M. Muito além do nosso eu: a nova neurociência que une cérebro e máquinas – e como ela pode mudar nossas vidas. 1st edition. São Paulo: Planeta, 2017. pp. 25-28.

5. MCAFEE, A. BRYNJOLFSSON, E. *A segunda era das máquinas*. Rio de Janeiro: Alta Books, 2014.
6. SCHWAB, K. *A quarta revolução industrial* – São Paulo: Edipro, 2016. 115 p.

By suggesting that future applications of these tools could extend beyond the boundaries of medicine, Nicolelis anticipated that the technologies would open the door to experiences and actions that were difficult to conceive at the time but are already proving possible today. This is largely due to the integration of artificial intelligence (AI) into this field[7] and algorithms' ability to analyze large quantities of data and identify underlying patterns, thereby improving BCIs' accuracy and efficiency in interpreting neural data.[8]

This integration has enabled the growth of large-scale, high-quality datasets, helping expand the applications of brain-machine interfaces. In addition to assisting people with disabilities, these interfaces now enhance human capacities by broadening our understanding of the brain's complex functioning and fostering the emergence of new markets.

One of the best-known players in this field is Neuralink, which has made headlines worldwide because of its advanced stage of development. 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 had been inaccessible to him.[9]

Another company bringing products to market in this field is NextMind. Besides 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. In other words, any image you imagine would be recreated on a computer screen—something like the image-generation model used by AI applications including DALL-E and Midjourney.[10]

However, despite the great enthusiasm surrounding advances in BCIs, as these technologies continue to mature, questions arise concerning their development and ethical, responsible use. These questions must be addressed so that the technologies improve lives without causing unanticipated and potentially serious harm, particularly 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. Accessed 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 June 11, 2024.

9. DREW, L. Elon Musk's Neuralink brain chip: what scientists think of firts human trial. Nature, 2024. Available at: https://www.nature.com/articles/d41586-024-00304-4. Accessed June 11, 2024.

10. AR - SNAP AR. Welcome Nextmind. Available at: https://ar.snap.com/welcome-nextmind. Accessed June 11, 2024.

many of the threats associated with BCIs are already apparent in the way technology companies exploit neural data in everyday life.[11]

According to Adrian Carter, artificial intelligence tools and algorithms that interpret eye movements and detect changes in skin color and temperature are already being used to read the outputs of brain activity and thereby predict and influence behavior, allowing certain companies to make billions from these data.[12]

Moreover, the neural data arising from these activities are inherently extremely sensitive information, since they can reveal very intimate details about consumers.

In this regard, in a very recent study by Jared Genser, Stephen Damianos, and Rafael Yuste, the authors identified the mining of neural data for commercial purposes as one of the most pressing concerns raised by these advances. As consumers increasingly use neurotechnology devices, the authors explain, companies are building larger databases of brain images and other neural data that, like genetic material and fingerprints, could allow individuals to be identified immediately.

The study also finds that advances in AI are rapidly increasing the ability to decode information, providing companies with unprecedented insights into consumers' cognitive states and inner worlds, as well as helping predict personality traits, addictions, mental health, and various disorders.[13]

It is therefore not difficult to imagine how corporations could misuse these data. This poses complex challenges, particularly concerning the development of these tools and the protection of privacy and user autonomy—especially where users have limited control over implanted brain-machine interfaces and the data they produce—as well as the security of data and devices.

Faced with this situation and anticipating neuroscience and neurotechnology's growing ability to access and influence human mental processes, Marcello Ienca and Roberto Andorno highlighted 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. Accessed July 12, 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 June 17, 2024.

13. GENSER, J. DAMIANOS, S. YUSTE, R. Op. cit., pp. 17-18.

which rights individuals should exercise over their own mental dimension to protect integrity, privacy, and autonomy, and to ensure that people control their own thoughts, memories, and decisions and are protected against possible abuses or manipulation arising from these advances. In particular, they advocated creating new human rights, which they called “neurorights.”[14]

Brain-computer interfaces represent technological advances that, despite their potential to bring positive transformation, already face nontechnical obstacles that could limit their use unless there is a broad and sophisticated understanding of how to develop them. This article therefore aims to analyze the ethical and regulatory challenges of advances at the intersection of BCIs and AI, focusing on: (i) the urgent need for consent; and (ii) safeguarding individuals’ neurorights in the processing of neural data.

To achieve this objective, the methodology adopted among the traditional scientific methods will be hypothetico-deductive. In the legal field, the study will employ hermeneutic, empirical, and argumentative methods and adopt a critical methodological approach. These dimensions will encompass descriptive research involving a reflective analysis of academic and legal scholarship on the topics addressed, as well as a detailed analysis of applicable regulations and proposals, if any.

1. How are neurotechnologies and AI influencing the creation of new rights?

To begin, a World Health Organization (WHO) report states that one in six people, approximately 16% of the global population, experiences some form of significant disability.[15] In Brazil, the population with disabilities was estimated at 18.6 million people. The survey data also show that these individuals are less integrated into the labor market and schools and consequently face greater difficulty accessing income.[16]

14. 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 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 July 31, 2024.

16. BRASIL, Ministério dos Direitos Humanos e da Cidadania. Brasil tem 18,6 milhões de pessoas com deficiência, indica pesquisa divulgada pelo IBGE e 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 July 31, 2024.

Although various neurotechnology techniques are already used in everyday life, such as electroencephalography and functional magnetic resonance imaging, along with techniques for stimulating the brain to alleviate symptoms of diseases such as Parkinson's or epilepsy, the most interesting and controversial innovations have emerged from their relationship with cognitive technologies.

The interaction between BCIs and data obtained about brain functions through machine learning and deep learning, as well as natural language processing, is 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 through thought alone, communicating through synthesized speech, moving prosthetic limbs, operating a computer, and performing other important functions that improve quality of life for people with disabilities.[17]

In this context, as Rafael Yuste and Sara Goering aptly observe:

> Technological advances suggest that we are moving toward 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 assist 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 the technology could also exacerbate social inequalities and offer 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 bounded by their bodies. (emphasis added)[18]

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 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 June 18, 2024.

The global BCI market, currently valued at approximately US$1.2 billion, is advancing impressively, with a projected compound annual growth rate of 13–15% through 2030 19. However, the sector's rapid expansion raises significant concerns about the privacy and security of neural data. On the one hand, we cannot disregard the fact that our personal data are already processed on a large scale and that the actors mentioned by the authors already build an individual profile of each person. On the other hand, the drive to generate wealth enables various harms to the population's social and mental well-being, influencing people without their even realizing that they are being manipulated.

This situation creates a need to address what ethicists have called neurorights: the fundamental normative rules for protecting and preserving the human brain and mind.[20] The absence of clear regulations can lead to abuses, exacerbate social inequalities, and compromise individuals' mental integrity.

It is therefore imperative to develop ways of regulating these rights to ensure that the benefits of BCIs are harnessed ethically and fairly.[21]

2. Pathways and proposals for realizing neurorights

Having presented these considerations, and given that most existing privacy laws do not explicitly address neural data or neurorights, we turn to a comparative analysis of legislation and other frameworks on the subject to establish legal safeguards for the brain and the processing of these data.

The following subsection will therefore provide an overview of legislative efforts around the world, particularly in the European Union, Latin

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 June 19, 2024.

20. 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 June 20, 2024.

21. RODRÍGUEZ, J. Inteligencia artificial y neuroderechos. Retos y perspectivas. Cuestiones Constitucionales, Revista Mexicana de Derecho Constitucional, No. 46, January-June 2022. ISSN (electronic edition): 2448-4881. Available at: https://www.scielo.org.mx/pdf/cconst/n46/1405-9193-cconst-46-93.pdf. Accessed July 26, 2024.

America, and the United States, to identify common features of the challenges of protecting mental privacy in the neurotechnology era.

2.1 Analysis of laws and regulations around the world

In discussions of innovation, data protection, and new technologies, the European Union (EU) is usually seen as a pioneer in global regulation, standing out in an environment that lacks regulation and is rife with potential, irreparable harm due to the speed of technological development.

This EU stance is nothing new. By positioning itself as a global benchmark, this economic bloc seeks to encourage other nations to broaden the debate, accelerate their legislative proposals and guidelines on BCI and AI systems, and plan technological development ethically, thereby gaining a place in discussions worldwide.

Examples include its pioneering personal data regulations, first Directive 95/46 and then the General Data Protection Regulation (GDPR), which also served as a basis for Brazil's General Personal Data Protection Law (LGPD), and, more recently, the AI Act, Europe's new legislation regulating AI.

In discussions of BCIs, neurorights, and neural data, however, the EU is a pioneer only in the academic sphere, since debate remains within the remit 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 to deepen understanding of the human brain and advance the development of neurotechnologies. Active for 10 years, the project generated more than 3,000 academic publications, developed more than 160 digital tools and medical and technological applications, and created the open research infrastructure EBRAINS. It also drove significant advances in brain research and medical technology development, such as personalized brain medicine and new brain-inspired technologies, including AI and neuromorphic computing tools.[22]

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 July 22, 2024.

Another notable European initiative is the Council of Europe's "Strategic Action Plan," which focuses on human rights and new biomedical technologies, including recent developments in neurotechnology.

In a departure from the usual pattern, Latin America stands out in incorporating these concepts into legal systems. Chile, in particular, has become a reference point on the subject as the first country in the world to incorporate them into its Constitution. It approved a constitutional amendment through Law 21.383 [23], modifying Article 19 to protect brain activity and related information and emphasizing the need to balance physical and mental integrity with advances in neurotechnologies.

Another crucial milestone in Latin America[24] was the Organization of American States' (OAS) adoption of the Inter-American Declaration of Principles on Neurosciences, Neurotechnologies, and Human Rights[25] around mid-2023, demonstrating a regional commitment to protecting 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 toward regulating neurotechnologies and providing safeguards for brain integrity and neural data. The latter countries are at a more advanced regulatory stage: as of the time of writing, two bills concerning "neuroprivacy" were found to be under consideration in Mexico, alongside 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 July 22, 2024.

24. DO, B. SPIVACK, J. BADILO, M. Privacy and the rise of "neurorigts" in Latin America. Future of Privacy Forum, 2024. Available at: https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/. Accessed July 23, 2024.

25. OEA - ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Declaração Interamericana de Princípios sobre Neurociências, Neurotecnologias e Direitos Humanos. Available at: https://www.oas.org/es/sla/cji/temas_culminados_recientemente_Neurociencias_Neurotecnologias_y_Derechos_Humanos.asp. Accessed July 23, 2024.

Table 01 – Regulation of Neurorights in Latin America

Country	Proposal/ regulation	Key points	Current status	Sources
Chile	Ley 21383	Amends the Constitution to establish parameters for scientific and technological development in the service of people, protecting individuals' physical and psychological integrity and requiring consent to use these tools.	In force	Biblioteca del Congresso Nacional de Chile
Mexico	Proposed by Deputy María Eugenia Hernández Pérez	Uses wording identical to the Chilean constitutional amendment.	Under discussion	Sistema de ~~Información Legislativa~~
	Proposed by Senator Alejandra Lagunes Soto Ruiz	Amends Article 73 of the Constitution to regulate artificial intelligence, cybersecurity, and neurorights in a unified manner.	Under discussion	Senado de la Republica
Uruguay	Legislative initiatives based on dialogue with Chilean experts and legislators	Regulate neurorights	In the preliminary stages of discussion	Unesco
Argentina	Bill 2446/23	Creates a specific committee to develop new regulations on neurorights	Under discussion	Senado de la nación Argentina
Costa Rica	Proposed amendment to the data protection law	Classify neural data as biometric data	Under discussion	Unesco
Colombia	Proposed amendment to the data protection law	Creates a specific section to establish guiding parameters for processing these data through AI and neurotechnologies	Under discussion.	Unesco

(continued)

Table 01 – Regulation of Neurorights in Latin America

(continuation)

Country	Proposal/ regulation	Key points	Current status	Sources
Peru	Bill No. 5968/2023-CR (Carlos Javier Zeballos Madariaga)	Seeks to protect people's fundamental rights by regulating the use of neuroscientific evidence in court proceedings.	Under review by the Committee on Justice and Human Rights of the Congress of Peru since September 2023	Peruvian Congress
Brazil	Proposed Constitutional Amendment (PEC) 298 of 2023 (Rio Grande do Sul)	Amends the State Constitution to include neurorights, elevating mental integrity to the status of a constitutional principle.	In force in Rio Grande do Sul.	Legislative Assembly of Rio Grande do Sul
	PEC No. 29/2023 (Senator Randolph Rodrigues)	Introduces provisions to protect mental integrity and algorithmic transparency on the premise that mental integrity is inextricably linked to human dignity in this new social context.	Stalled in the Senate, awaiting a rapporteur.	Federal Senate
	Bill (PL) 2174/2023 (Rubens Pereira Júnior)	Establishes rules and principles to protect fundamental rights relating to the human brain and nervous system, with the aim of ensuring the protection and promotion of individuals' neurorights.	Awaiting appointment of a rapporteur in the Committee on Constitution and Justice and Citizenship (CCJC)	Chamber of Deputies
	Bill (PL) 1229/2021 (Carlos Henrique Gaguim)	Amends Law No. 13.709 of August 14, 2018 (General Personal Data Protection Law) to define neural data and regulate their protection.	Withdrawn by the author	Chamber of Deputies

(continued)

Table 01 – Regulation of Neurorights in Latin America

(continuation)

Country	Proposal/ regulation	Key points	Current status	Sources
Brazil	Bill (PL) 522/2022 (Carlos Henrique Gaguim)	Amends Brazil's General Personal Data Protection Law (LGPD) to recognize neural data as a type of sensitive personal data.	Approved by CSAÚDE in October 2023, and Deputy Adriana Ventura (NOVO-SP) was appointed rapporteur on April 10, 2024	Chamber of Deputies
	Preliminary draft updating the Civil Code (2024)	Incorporates neurorights into the Civil Code.	Submitted to the Senate, under review.	Federal Senate

Source: compiled by the author from various official government sources, 2024.

Finally, in the United States, efforts to address neurorights are led by academic and professional organizations and government advisory bodies. Notable contributions come from scholars such as Martha J. Farah and Hank Greely, whose work has been fundamental to the discussion of this subject.

In April, the state of Colorado passed promising legislation to protect consumers using devices that collect brain activity data, promoting the defense of mental integrity and the protection of neural data. Commenting on the issue, Colorado Democratic State Representative Cathy Kipp emphasized that, although the technology has beneficial potential, "there should be safeguards for those who do not want their thoughts read and their biological data used."[26]

More recently, California also 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 June 24, 2024.

misuse, allowing users to control, delete, or limit these data.[27]

The foregoing makes clear that, overall, various countries are seeking ways to address neurorights and neural data management with the aim of regulating new technologies to protect individuals' rights rather than prohibiting them. These measures therefore seek 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 v. Emotiv Inc.

As noted, Chile is so far the only country in the world to incorporate neurorights into its legal system, even granting them the status of fundamental rights. This explicitly recognizes the importance of providing a framework to address emerging ethical and legal challenges in neurotechnology and shape an environment in which innovation can flourish without compromising individuals' rights to cognitive liberty, mental privacy, mental integrity, and psychological continuity.

The first court dispute on the issue was therefore also expected to arise in Chile. That is precisely what happened in August 2023. At the time, the Third Chamber of the Chilean Supreme Court faced a landmark case whose details and grounds for its decision would mark a milestone far beyond the country's borders.[28]

In the case, Mr. Guido Girardi Lavín filed an action for constitutional protection against Emotiv Inc., a bioinformatics company based in San Francisco, United States, that develops and manufactures portable electroencephalography products, neuroheadsets, software development kits, software, mobile applications, and data products.

In his initial filing, the claimant stated that he had purchased a device called "Insight," a headband with sensors that capture information about the brain's electrical activity and obtain data on the user's gestures, movements, preferences, reaction times, and cognitive activity. He stated that he had consequently accepted the software's terms of service, which provided for

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/&gt. Accessed October 16, 2024.

28. CORNEJO-PLAZA, M. I. 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 July 25, 2024.

the company to store his neural data in anonymized form for scientific research purposes.

However, to the claimant's surprise, Emotiv began using his data for other purposes. He alleged that this improper processing had exposed him to various risks, pointing to violations of Article 11 of Law No. 19.628, concerning the due diligence that those responsible for personal data records or databases must exercise in handling such data, and Article 13 of the same law, concerning people's right to have their personal data erased or blocked. Even after his user account had been closed, the company retained information about his brain for scientific and historical research.

In its defense, Emotiv argued that its product was a noninvasive, nontherapeutic neurotechnology device, a type of mobile electroencephalograph designed for self-quantification and field research, and was not sold as a medical device. It also stated that the product and its installation process included a detailed explanation of the terms and conditions, requesting express consent to process personal and brain data, which the claimant had allegedly granted.

In its ruling, the Court upheld the judgment in the claimant's favor, adding only an order directing the Public Health Institute and the customs authority to ensure that the marketing of the Insight device and the use of its data complied with current regulations, while also confirming the request to delete any stored data relating to the claimant's use of the device.

In its reasoning, the Court emphasized the need for informed consent to use information in research, as required by Law No. 20.120. It referred in particular to Article 19 of the Political Constitution of the Republic as a direct mandate to protect neurorights. It also cited 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 applications to human rights. The Court thus established the following position:

> Given the development of new technologies involving ever more aspects of the human person—aspects that would have been unthinkable to know a few years ago—the state must exercise particular attention and care in reviewing them, with the aim of preventing and anticipating possible effects while directly protecting human integrity in its entirety, including its

> privacy and confidentiality, as well as rights relating to mental integrity and the rights of subjects in scientific experimentation [...] Accordingly (...) it becomes absolutely necessary that, before allowing its marketing and use in the country, this technology and its devices be analyzed by the competent authority, given that it raises issues not previously studied [...] the conduct alleged in the proceedings, in the circumstances described, violates the constitutional guarantees contained in paragraphs 1 and 4 of Article 19 of the Political Constitution of the Republic, which concern physical and mental integrity and the right to privacy [...] For these reasons, and considering that the device lacks a Customs Destination Certificate, this action shall be granted as indicated in the operative part of this ruling, so that the health and customs authorities fully examine the Insight device in light of the regulations mentioned in this ruling. (emphasis added)[29]

Beyond its landmark character, this case established fundamental parameters that should guide future analyses of the subject. Notable aspects include: (i) recognizing that neural data also constitute personal data and therefore fall under data protection laws. Although this may seem basic, it is crucial because it shows that data protection emerges as the primary legal basis for analyzing neurotechnologies; (ii) the clear connection between data protection legislation and the fundamental rights to mental integrity and privacy, demonstrating that the absence of consent for the specific processing of brain information constitutes both a statutory and a constitutional violation; and (iii) the discussion of the need for express consent, emphasizing that processing must be grounded in an appropriate legal basis or it will be unlawful.

In this sense, the Chilean judges are considered to have decided correctly, weighing the benefits associated with the development of neurotechnologies and seeking a balanced solution rather than a radical one that could have led to Emotiv Inc.'s activities being banned in the country and consequently discouraged other companies operating in the market.

29. CHILE. Base Jurisprudencial del Poder Judicial. GIRARDI/EMOTIV INC: 09-08-2023 (CIVIL) APELACIÓN PROTECCIÓN), Case No. 105065-2023. In Buscador Jurisprudencial de la Corte Suprema. Available at: https://juris.pjud.cl/busqueda/pagina_detalle_sentencia?k=L2FadjlzYUdmbGx1UWNKWmV6ZjZ3dz09. Accessed July 30, 2024.

This approach thus highlights not only the importance and effectiveness of neurorights in the face of the challenges arising from these new technologies but also the possibility of defining a path of dialogue through which innovation can improve ethically and responsibly.

Final considerations

This article focuses on analyzing how neurotechnologies and artificial intelligence are shaping the creation of new rights. It explores the pathways currently proposed to promote the ethical and responsible development of these innovations, with the aim of protecting so-called neurorights against the risks associated with processing neural data.

The opening sections provide a brief historical overview of brain-computer interfaces (BCIs), highlighting their benefits and their development through integration with AI tools. Several practical BCI applications are examined, showing their transformative potential and positive impact, particularly for people with disabilities. The article also discusses the challenges and concerns these advances may pose for society in the short term, considering the sensitivity and potential harms of neural data processing and emphasizing the importance of studying neurorights.

The following section was divided into two parts. The first analyzes existing proposals and regulations around the world, seeking to identify points of convergence and highlighting how the diversity of proposals and lack of uniform consensus demonstrate growing interest and the need for a regulatory framework to ensure the protection of neurorights. The second offers a detailed analysis of Girardi v. Emotiv Inc., presenting important considerations about the potential application of these rights in practical settings, their realization, and the judicial approach to neurorights.

Finally, although the debate is far from settled, the aim of this article is to encourage deeper and more incisive reflection on the issues presented, seeking to make the protection of neurorights more effective.

Given the complexity of these technologies and the speed of their development, building a robust and adaptable legal framework that balances innovation with the protection of data subjects is a challenge requiring collaboration among legislators, scientists, and civil society.

The study of neurorights must therefore remain continuous and dynamic, seeking to ensure that innovations, however disruptive, respect individuals' dignity and autonomy. This will allow us to navigate the increasingly uncertain terrain of BCIs and AI safely, benefiting from them while preventing abuses and protecting individuals against the risks inherent in processing 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 April 20, 2024.

AR – SNAP AR. Welcome Nextmind. Available at: https://ar.snap.com/welcome-nextmind. Accessed June 11, 2024.

BOSELLI, G. Neurodireitos: a urgência de proteção jurídica das neurotecnologias. Consultor Jurídico, 2024. Available at: https://www.conjur.com.br/2024-fev-06/neurodireitos-a-urgencia-de-protecao-juridica-das-neurotecnologias/. Accessed June 10, 2024.

BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed June 07, 2024.

BRASIL, Ministério dos Direitos Humanos e da Cidadania. Brasil tem 18,6 milhões de pessoas com deficiência, indica pesquisa divulgada pelo IBGE e 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 July 31, 2024.

CANTARINI, P. A nova fronteira da manipulação comportamental e o papel do "compliance" na mitigação de riscos em IA. Jornal da USP, 2024. Available at: https://jornal.usp.br/artigos/a-nova-fronteira-da-manipulacao-comportamental-e-o-papel-do-compliance-na-mitigacao-de-riscos-em-ia/. Accessed 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/&gt. Accessed October 16, 2024.

CHILE. Base Jurisprudencial del Poder Judicial. GIRARDI/EMOTIV INC: 09-08-2023 (CIVIL) APELACIÓN PROTECCIÓN), Case No. 105065-2023. In Buscador Jurisprudencial de la Corte Suprema. Available at: https://juris.pjud.cl/busqueda/pagina_detalle_sentencia?k=L2FadjlzYUdmbGx1UWNKWmV6ZjZ3dz09. Accessed July 30, 2024.

CORNEJO-PLAZA, M. I. 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 July 25, 2024.

DREW, L. Elon Musk's Neuralink brain chip: what scientists think of firts human trial. Nature, 2024. Available at: https://www.nature.com/articles/d41586-024-00304-4. Accessed June 11, 2024.

DO, B. SPIVACK, J. BADILO, M. Privacy and the rise of "neurorigts" in Latin America. Future of Privacy Forum, 2024. Available at: https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/. Accessed 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 June 14, 2024.

FLORES FILHO, E. FIRMO, M. Dignidade humana e neurodireitos na era digital. Revista do Instituto de Direito Constitucional e Cidadania – IDCC, Londrina, vol. 7, no. 2, e063, 2022. Available at: file:///C:/Users/hsmol/Downloads/157-Texto%20do%20Artigo-386-2-10-20230523.pdf. Accessed July 15, 2024.

GAGUIM, C. Projeto de Lei nº 522, de 2022. Câmara dos Deputados, 2022. Available at: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317524. Accessed 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. Accessed July 12, 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 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 July 12, 2024.

HIGGINS, N. Neuralink implanta chip em cérebro humano: o que pode dar errado. Galileu, 2024. Available at: https://revistagalileu.globo.com/tecnologia/noticia/2024/02/neuralink-implanta-chip-em-cerebro-humano-o-que-pode-dar-errado.ghtml. Accessed June 02, 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 July 22, 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 July 15, 2024.

IENCA, M. 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 July 01, 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. Accessed June 11, 2024.

LOTTE, F. NAM, C. S. 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. ffhal-01656743f. Available at: https://inria.hal.science/hal-01656743/document. Accessed June 10, 2024.

MARDEN, C. MARTINS, G. *Direito e neurociência: além das primeiras impressões.* 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/ais-next-frontier-are-brain-computer-interfaces-the-future-of-communication/. Accessed 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 July 10, 2024.

MCAFEE, A. BRYNJOLFSSON, E. A segunda era das máquinas. Rio de Janeiro: Alta Books, 2014.

METHA, D. Como implante cerebral Neuralink de Elon Musk 'amplia as fronteiras da mente". BBC News Brasil, 2024. Available at: https://www.bbc.com/portuguese/articles/cp0gyj3lv01o. Accessed 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 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 June 24, 2024.

NICOLELIS, M. Are we at risk of becoming biological digital machines? Nature Human Behaviour. Nat Hum Behav 1, 2017. Available at: https://doi.org/10.1038/s41562-016-0008. Accessed July 02, 2024.

NICOLELIS, M. Muito além do nosso eu: a nova neurociência que une cérebro e máquinas – e como ela pode mudar nossas vidas. 1st edition. São Paulo: Planeta, 2017. pp. 25-28.

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 August 02, 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 July 08, 2024. p. 03.

OEA - ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Declaração Interamericana de Princípios sobre Neurociências, Neurotecnologias e Direitos Humanos. Available at: https://www.oas.org/es/sla/cji/temas_culminados_recientemente_Neurociencias_Neurotecnologias_y_Derechos_Humanos.asp. Accessed July 23, 2024.

PIVA, S. Neurodireitos: a necessária proteção da mente humana em tempos de avanço de neurotecnologias e da IA. Fenalaw, 2023. Available at: https://www.fenalaw.com.br/fenalawlab/neurodireitos-a-necessaria-protecao-da-mente-humana-em-tempos-de-avanco-de-neurotecnologias-e-da-ia/. Accessed August 02, 2024.

RODRÍGUEZ, J. Inteligencia artificial y neuroderechos. Retos y perspectivas. Cuestiones Constitucionales, Revista Mexicana de Derecho Constitucional, No. 46, January-June 2022. ISSN (electronic edition): 2448-4881. Available at: https://www.scielo.org.mx/pdf/cconst/n46/1405-9193-cconst-46-93.pdf. Accessed July 26, 2024.

SALOMÃO, L. et al. Relatório Final – Comissão de Juristas Responsável pela revisão e atualização do Código Civil. Brasília. Senado Federal, 05.04.2024. Available at: https://legis.senado.leg.br/comissoes/comissao?codcol=2630. Accessed July 28, 2024.

SCHWAB, K. *A quarta revolução industrial* – São Paulo: Edipro, 2016. 115 p.

SILVA, G. A. 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 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 July 22, 2024.

THE NEURORIGHTS FOUNDATION. The Five Neurorights. Available at: https://neurorightsfoundation.org/mission. Accessed June 01, 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 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 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 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 June 18, 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Theme II

Smart Cities and New Technologies

AUTHORS

Carolina Freitas Gomide de Araujo

Cláudio Mendes da Silva

Daniel Santiago Diniz

Luís Henrique de Menezes Acioly

Victor Chame Alvim

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

11

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

CLAUDIO MENDES DA SILVA

Cowards are those who have everything good and supply evil so the favela will die. Criolo.

Contents: Introduction. 1. Smart Cities and Social Inequalities: An Unequal Debate. 2. The “Datafication” 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 twenty-first century have been marked by a massive increase in the use of data, particularly personal data, to sustain a new market model that relies on these inputs to provide products or services. This involves not only corporate actors’ use of big data[2] techniques but also governments’ use of data as cities become computerized and public policies are grounded in information technologies and automation, with a view to building new models of Smart Cities. This study will not address the conceptual dilemmas and controversies surrounding the subject. Instead, it seeks to make the concept more accessible, to varying degrees, by highlighting its practical applications and social implications.

Although citizens undeniably stand to benefit from the products, policies, and conveniences generated through data use, we must also assess its impact on citizens themselves concerning their constitutional rights to privacy, autonomy, and data protection. The last of these was more recently enshrined among fundamental rights in Article 5, LXXIX, of the Constitution of the Federative Republic of Brazil (CRFB/88), through Constitutional Amendment No. 115 of 2022.

In this regard, the General Personal Data Protection Law is also highly relevant. Approved in 2018 as Law No. 13.709 of August 14,

1. Law graduate of the Universidade do Estado do Rio de Janeiro – UERJ; postgraduate student in Digital Law at the Instituto de Tecnologia e Sociedade (ITS Rio), in partnership with UERJ; attorney; legal adviser to Instituto Decodifica.

2. According to a report produced by the Instituto de Tecnologia e Sociedade do Rio de Janeiro do Rio (ITS-Rio), big data is “literally the collection of data whose existence is possible only as a consequence of the massive data collection that has become possible in recent years, thanks to the ubiquity of devices and sensors in everyday life and the growing number of people connected to these technologies through digital networks and sensors.” Big data no Sul Global. Relatório sobre estudos de caso. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2016. Available at: https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf. Accessed July 2024.

2018, it entered into force on September 18, 2020. The law emerged in a context of efforts to establish guidelines for consolidating the regulation of an ecosystem protecting the rights to privacy and personal data. The LGPD thus became Brazil's first general law on the subject.

Innovation, in the broadest sense of the word, should not emerge at any cost. The so-called 4th Industrial Revolution taking place worldwide has been profoundly changing cities' structures, requiring a comprehensive, contextualized reflection on its social and ethical impacts. It has redefined how we interact with urban space, introducing new dynamics of power and control that directly affect citizens' quality of life and individual rights.

This article seeks to offer more local perspectives, initially focused on Brazil, and to examine the impacts and highly harmful potential of these technologies, such as those used for monitoring, particularly in public security. This is especially relevant given the extensive use of data concerning historically vulnerable populations, above all Black populations and those living in urban peripheries. This examination will be conducted in light of civil and constitutional legal guarantees intended to safeguard privacy and data protection rights, even though the LGPD does not apply directly, pursuant to Article 4, III, item "a."

The article also seeks to reflect on the concept of Smart Cities, the state's role as a sovereign entity in formulating and implementing public policies, surveillance technologies and data control in smart cities, and how this state action may influence and potentially reinforce necropolitical practices affecting the lives and rights of historically vulnerable groups, as already mentioned, from Achille Mbembe's perspective.[3]

The subject's urgency stems from the prevailing market model, in which personal data are important assets for different economic actors, with the state playing an active role in this regard. This is in addition to its political power to formulate public policies. It is crucial to emphasize how the absence of citizen participation in formulating these policies can further exacerbate existing inequalities. The question guiding this work can therefore be stated as follows: how, or to what

3. MBEMBE, Achille. *Necropolítica. Biopoder, soberania, estado de exceção, política da morte (ebook).* São Paulo: N-1 edições, 2018.

extent, can Smart Cities provide an environment free from discrimination in the current technological context?

The search for possible solutions or ways to mitigate this increasingly prevalent problem will involve a brief, though not simplistic, analysis and historical, social, and political contextualization of Brazil. The starting point is that what we generally understand as discrimination is not new to the age of information and technological inputs. Rather, it reproduces something already intrinsic to society, both among those who supply these tools—the Global North—and among those who consume them, such as Brazil as a representative of the Global South.

1. Smart Cities and Social Inequalities: An Unequal Debate

To begin, all societies are technological to some degree. The measure of innovation—if such measurement can be considered "fair" for comparative purposes—is the context in which a group or society exists. For example, the stone knife was a major innovation for a society living 3,000 years before Christ (BC), as a sharp object that could be used for hunting and defense.[4] Likewise, in a more recent period, it is also a highly functional technology that serves us in eating, considering, of course, the Western way of life. Using technological devices such as tablets and smartphones, with or without artificial intelligence (AI), therefore does not necessarily define what is modern or innovative.

Smart Cities, in turn, are commonly characterized by the extensive use of technology employing data that, at least in theory, can improve citizens' quality of life, enhance the important element of efficiency in managing resources—financed by and belonging to the population—and improve the sustainability of urban space itself.[5] [6]

4. BOLLA, Carla. Como a França popularizou o uso de talheres. Forbes. September 15, 2022. Available at: https://forbes.com.br/forbeslife/2022/09/carla-bolla-como-a-franca-popularizou-o-uso-de-talheres/. Accessed July 2024.

5. OB.BR. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Cidades Inteligentes. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf. Accessed July 2024.

6. In addition, the ABNT standard based on ISO 37122 (ABNT, 2021) defines a smart city as a city that accelerates the pace at which it delivers social, economic, and environmental sustainability outcomes and responds to challenges such as climate change, rapid population growth, and political and economic instability. It does so by fundamentally improving how it engages society, applies collaborative leadership methods, works across municipal disciplines and systems, and uses data information and modern technologies to provide better services and quality of life for those who inhabit it—residents, businesses, and visitors—now and in the foreseeable future, without unfair disadvantages or degradation of the natural environment. Ibid.

Bill (PL) No. 976, introduced on 19/03/2021 to establish the National Smart Cities Policy (PNCI),[7] defines the term as follows, verbatim:

> Art. 2. For the purposes of this Law, the following definition applies: I – smart city: urban space oriented toward investment in human and social capital, sustainable economic development, and the use of available technologies to improve and interconnect cities' services and infrastructure in an inclusive, participatory, transparent, and innovative manner, focusing on improving citizens' quality of life and well-being.

This current way of life, which we increasingly experience in everyday activities, including and especially the use of technologies in public security, is directly associated with importing a model produced in the Global North, where the sector's most economically powerful companies are concentrated. This dynamic has been driven by the private market within the capitalist system of production, in which large technology companies are the main actors. They regulate contemporary social life, with our personal data collected or sold by or to other companies that use them for their own benefit,[8] since making a profit is a sine qua non of companies' existence as such.

In this regard, we must reflect on the impacts of adopting this model in a context that is already extremely unequal. It is also worth considering that:

> Cities are living, nonstatic organisms. When managed through technological systems, these systems must therefore be flexible enough to accommodate not only changes in direction dictated by residents' needs but also challenges posed by new urban problems. Are current systems capable of such flexibility? Moreover, would these systems be inclusive, or would they target a small segment of the population able to access these resources?[9]

7. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1977843&filename=PL%20976/2021. Accessed July 2024.

8. RIBEIRO, Laura Talho. Tecnologias inteligentes de vigilância: percepções sobre segurança nos centros urbanos. Available at: https://itsrio.org/wp-content/uploads/2018/03/laura_talho_smartsurveillance.pdf. Accessed July 2024.

9. MENDES, Teresa Cristina M. Smart Cities: Solução para as cidades ou aprofundamento das desigualdades sociais? Rio de Janeiro, 2020. p. 4. Available at: https://www.observatoriodasmetropoles.net.br/wp-content/uploads/2020/01/TD-011-2020_Teresa-Mendes_Final.pdf. Accessed July 2024.

Teresa Cristina Mendes emphasizes that technological systems' flexibility is crucial to meeting residents' needs.[10] This raises the question of how Smart Cities can be adapted to avoid perpetuating existing inequalities, considering the social dynamics experienced in cities and understanding the country's historical context as a whole, since this also shapes social inequalities. The Black population's position in the current context cannot be analyzed in isolation. It would be a mistake to ignore almost four hundred years of slavery, the structural limitations endured, and, moreover, the complete alienation of their dignity—an allusion here to the established principle of human dignity—in a situation marked by the stripping away of these people's humanity.

Another well-known fact must be kept in mind to understand how the new dynamic introduced by Smart Cities, imported from a different reality, can be equally harmful and exclusionary, directly and indirectly affecting the Black community. In the process of alienating an entire culture, Portuguese colonizers also developed a mechanism for neutralizing ethnic consciousness through their imperialist ideology of being an "agent of evolution and civilization." Clóvis Moura expressed this process in terms such as "democratic verbalization."[11] Having assimilated this ideological imposition, a significant portion of the Black population sought to pass as White or at least move up the chromatic scale established by colonizers, with Whiteness as the superior model to attain. This phenotypic policy sought, and still seeks, to make members of this group distance themselves from their origins and assimilate White values and standards.

Although we are making a leap in time, it is crucial to emphasize that this ideology remains rooted in our society. We are still engaged in the historical process of reclaiming the Black population's identity, dignity, autonomy, and well-being. For example, Law No. 12.711 of August 29, 2012, the Quota Law, is an extremely recent policy of reparation for slavery in our historical timeline and one of the few explicit policies of its kind, not to mention the Lei Áurea, the law that marked the abolition of slavery in Brazil. These facts reveal how sensitive and urgent the existing social divide is.

10. Ibid.

11. MOURA, Clovis. Escravismo, colonialismo, imperialismo e racismo. Afro-Ásia, Salvador, no. 14, 1983. p. 3. Available at: https://periodicos.ufba.br/index.php/afroasia/article/view/20824/13425. Accessed July 2024.

It is also worth recognizing that “the racialized distribution of Brazilian cities results both from the converging accumulation of countless decisions and instances of inequality and racism and from the adoption of racist ideologies in planned cities.”[12]

In Brazil, a country facing major problems of digital inclusion and deep social and economic inequalities, 24 million people without internet access live in urban areas, 17 million identify as Black or Brown (pardo), and 17 million belong to socioeconomic classes D–E. This points to digital exclusion in the country’s urban peripheries.[13] The Smart Cities concept is thus being adopted in a limited manner, although some sectors, such as public security, receive substantial investment with this model already in mind.[14] The full deployment of technological resources in urban development is still far from a comprehensive reality, amounting instead to a megalomaniacal policy lacking empirical knowledge of its consequences.

Teresa Cristina also addresses this issue, supporting the point:

> Despite inclusive rhetoric, inequality remains present in many initiatives, particularly in less developed countries. Rather than being viewed as potentially active participants, residents are defined as mere consumers of technological solutions.[15]

The lack of adequate infrastructure, high implementation costs, and the absence of effective public policies aggravate the situation. This is in addition to the serious implications of replicating a model, even if it has been effective in a different context, particularly one based on the Global North. Regional inequalities and the concentration of investment in wealthier urban areas further intensify the exclusion of peripheral and rural populations. For Brazil to move closer to genuinely smart cities, it is essential to implement policies that promote digital

12. SILVA, Tarcízio. *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. São Paulo: Edições Sesc São Paulo, 2022. p. 141.

13. CAMARGO, Bianca. Cerca de 84% dos lares brasileiros têm acesso à internet, diz pesquisa. 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 August 2024.

14. Rio de Janeiro Governor Cláudio Castro invested R$236.5 million in purchasing facial recognition equipment. SANTO, Thaís Espírito. RJ anuncia câmeras com reconhecimento facial e leitura de placas em viaturas da PM. G1, Rio de Janeiro, April 03, 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-em-viaturas-da-pm.ghtml. Accessed July 2024.

15. MENDES, Teresa Cristina M. Smart Cities: Solução para as cidades ou aprofundamento das desigualdades sociais? Rio de Janeiro, 2020. p. 6. Available at: https://www.observatoriodasmetropoles.net.br/wp-content/uploads/2020/01/TD-011-2020_Teresa-Mendes_Final.pdf. Accessed July 2024.

inclusion, ensure equitable access to new technologies, and encourage citizen participation in decisions about urban development.

This citizen participation necessarily entails recognizing that peripheral communities have empirical knowledge of the reality they experience, particularly in formulating public policies, monitoring their implementation, and evaluating them. However, multisectoral efforts are needed to enable participation in popular forums, seminars, workshops, and other mechanisms of joint development that ensure informed knowledge and autonomy to deliberate on the issue at hand.[16] Without such efforts, technologies may deepen existing divisions and perpetuate the marginalization of the most vulnerable communities.[17]

2. The "Datafication" of Life and Fundamental Rights in the Digital Age

Stefano Rodotà[18], in a lecture entitled "Transformations of the Body," delivered on November 06, 2015, at the Universidade do Estado do Rio de Janeiro (UERJ) and attended in person by this article's author, discussed the profound transformations the human body was undergoing. The subject remains highly relevant, particularly in the age of information and technology. Rodotà observed that the body, once viewed as an inviolable physical entity, was now being transformed into data and information that third parties could manipulate and use. The digital age introduced the concept of the "electronic body," in which biometric features such as fingerprints, irises, retinas, and even facial expressions are also "datafied" and used to identify and control individuals.

This control extends to technologies such as subcutaneous microchips and smartphones, which allow the constant tracking

16. One example is the Fórum Popular de Segurança Pública, launched in 2022 in Rio de Janeiro, according to Observatório de Favelas. Although recent from a historical standpoint, the event already opens possibilities for a national initiative and for creating a space in which government officials and decision-makers can make better-informed decisions on such a sensitive issue. VELLASCO, Ramon. Fórum Popular de Segurança Pública é lançado no Rio de Janeiro. Observatório de Favelas. Rio de Janeiro. June 29, 2023. Available at: https://observatoriodefavelas.org.br/forum-popular-de-seguranca-publica-e-lancado-no-rio-de-janeiro/. Accessed August 2024.

17. Clarice Nassar Tambelli reaches a similar conclusion: "It is important that the opportunities offered by a smart city do not override other significant issues, such as social inequality, people lacking technological literacy, and differences in access between generations and even genders. On the contrary, these aspects must be raised when considering a solution involving technology. Other solutions that are not based solely on its use must also be explored and applied." TAMBELLI, Clarice Nassar. Smart Cities: uma breve investigação crítica sobre os limites de uma narrativa contemporânea sobre cidades e tecnologia. Available at: https://itsrio.org/wp-content/uploads/2018/03/clarice_tambelli_smartcity.pdf. Accessed July 2024.

18. RODOTÁ, Stefano. Corpo Eletrônico e Privacidade. Lecture delivered at the Universidade do Rio de Janeiro, Rio de Janeiro, November 06, 2015.

of a person, creating a new form of surveillance that threatens privacy and human dignity. Mass surveillance, exemplified by security cameras that can record 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 this regard, Danilo Doneda also observed:

> Personal information—which includes all information relating to a person—therefore takes on importance on various grounds. We can initially identify two factors that almost always feature among the justifications for using personal information: efficiency and control. A range of interests takes shape around these two factors, involving the state and private entities [...][19]

Data protection therefore emerges as a fundamental element in this discussion, particularly in the information age. As individuals' exposure and subjection to technological structures belonging to states and large companies increase, it becomes important not only to develop instruments that give data protection and privacy rights precedence over strictly economic interests,[20] but also to provide citizens with knowledge and information, especially those belonging to historically more vulnerable groups. This is separate from also equipping them with political awareness so that they may question certain public policies justified solely by the primacy of the public interest, such as the use of facial recognition technologies in public security.

It is also important to note that, although the right to privacy theoretically emerged from a desire for seclusion—outside the Brazilian and Global South context—it became more than a desire: it became a right enforceable against third parties from the late nineteenth century, with the consolidation of the Bourgeois Revolutions and the article The Right to Privacy, published on December 15, 1980, authored by Samuel Warren and

19. DONEDA, Danilo. Da privacidade à proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados [e-book]. 2nd edition. São Paulo: Thomson Reuters Brasil, 2019. p. 33.

20. TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. 1st edition. Indaiatuba, SP: Foco, 2022. E-book.

Louis Brandeis.[21] This was the first legal formulation of this right worldwide. Privacy emerged as an individualistic right. Today, however, as it moves into an ecosystem based on personal data, it connects people to society and requires a secure framework to ensure that this happens without harm.

Privacy and data protection thus belong to different spheres but are interconnected. Data protection does not replace privacy; it complements it. This is why they are enshrined in our Constitution,[22] which protects intimacy and private life as fundamental rights under Article 5, X, as well as the right to data protection, including in digital media, under Article 5, LXXIX, of the CRFB/88. The latter provision was introduced more recently through Constitutional Amendment No. 115 of 2022.

There is also the General Personal Data Protection Law, the first and most specific law addressing personal data protection, approved in 2018 as Law No. 13.709 of August 14, 2018, which entered into force on September 18, 2020 [23]. It emerged in a context of efforts to establish guidelines for consolidating the regulation of an ecosystem protecting privacy and personal data rights. Among other objectives, the law seeks to: (i) guarantee substantive equality and the freedom of natural persons; (ii) ensure the free development of human personality; (iii) prevent unlawful or abusive discrimination; and (iv) prevent certain groups from facing improper restrictions on access to goods and situations involving prejudice and stigmatization.

This context is essential to avoid understanding the Smart Cities model as an isolated phenomenon or an apparent symbol of progress, particularly when viewed through public security in a territory as uneven as Brazil's, especially

21. Samuel Warren and Louis Brandeis, "The right to privacy," in: 4 Harvard Law Review 193 (1890).

22. Regarding the primacy of the civil and constitutional law framework in protecting human beings in disputes both between private parties and between private parties and the state, the collective work coordinated by Anderson Schreiber and Carlos Nelson Konder teaches: "It is constitutional provisions that must guide the interpretive process, so the parties cannot choose which source prevails. That primacy will result from interpreting the Federal Constitution and ordinary legislation in its light." SOARES, Felipe Ramos Ribas; MATIELI, Louise Vago; DUARTE, Luciana da Mota Gomes de Souza. Unidade do ordenamento na pluralidade das fontes: uma crítica à teoria dos microssistemas. In: SCHREIBER, Anderson; KONDER, Carlos Nelson (coordinators). Direito civil constitucional. E-book. São Paulo: Atlas, 2016. p. 79.

23. However, as Chiara de Teffé explains, protection of data-related rights had been sought on the basis of provisions established, beyond the Federal Constitution, in sectoral laws directly or indirectly addressing privacy and personal data. Examples include the Consumer Protection Code (Law No. 8.078/90), the Brazilian Civil Rights Framework for the Internet (Law No. 12.965/14), the Access to Information Law (Law No. 12.527/11), and the Positive Credit Registry Law (Law No. 12.414/11). However, this regulatory framework lacked precision and did not provide adequate guarantees for individuals (....). TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. 1st edition. Indaiatuba, SP: Foco, 2022. E-book.

because the inestimable value of privacy and data protection as fundamental rights inherent to citizens must be considered. In this light, the idea of progress associated with that dynamic becomes relative.

In a study arising from a research project at the Centro de Tecnologia e Sociedade of Fundação Getúlio Vargas, associated with its law program in Rio de Janeiro (CTS-FGV),[24] 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. They observed three video surveillance tools: facial recognition, automatic license plate recognition, and cameras. They concluded that enthusiasm for adding new technologies to state authorities' portfolios does not necessarily translate into advances in public security. They also found that material and staffing limitations can lead to discrimination against people and groups already traditionally targeted by police authorities, particularly Black and poor people moving through areas where these technologies are fully operational. Rather than being enhanced, citizens' security is thus potentially threatened by increased suppression of fundamental rights.[25]

The reflections of Stefano Rodotà and, subsequently, Danilo Doneda raise crucial questions about the changing concepts of the body and privacy in the digital age. The notion of the "electronic body" reveals how individuality is increasingly subject to data manipulation, threatening privacy, data protection, and human dignity itself. These authors warn of the need for a legal framework protecting the integrity of personal data. Beyond this, it is crucial to provide citizens with knowledge and tools to defend their rights against both private parties and the state amid growing surveillance. In this regard, civil society organizations' tireless contribution to upholding Brazilian citizens' most basic rights must be emphasized.

24. See more at: https://direitorio.fgv.br/pesquisa/centro-de-tecnologia-e-sociedade.

25. REIA, Jess; BELLI, Luca. Smart Cities no Brasil: regulação, tecnologia e direitos. Belo Horizonte, MG: Casa do Direito, 2021. p. 112. Available at: https://repositorio.fgv.br/server/api/core/bitstreams/390c1729-357b-4c4f-ba30-e236419debf1/content. Accessed July 2024.

The LGPD emerges as an indispensable response for regulating the use of personal information, guaranteeing individuals' freedom and substantive equality in the face of unprecedented resources being directed toward Smart Cities models. Effective data protection calls for a more practical perspective that considers citizen participation and the possibility of joint development. Rather than simply building something in relation to others, we must recognize ourselves as part of the problem to generate an effective solution directly connected to pressing demands for social policies that respect basic fundamental rights. This participatory element can give citizenship a more concrete form, ensuring a leading role for a group underrepresented in the democratic model in which we live.

This approach is essential to ensure that technological innovations do not magnify inequalities but instead 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, from the arrival of the Portuguese in 1500 [26], to the "end" of slavery with the signing of the Lei Áurea, shows that policies reflecting aspects of that era persist to this day. Despite significant legal and social advances, the control, surveillance, and genocide of Black people and people living in urban peripheries remain features of more recent state organization.[27]

It is no coincidence that the state itself defines which legally protected interests receive more or less protection, directly influencing public policy. In this sense, it tends to favor members of the dominant classes with greater possibilities and opportunities to accumulate capital, "placing maximum emphasis on the protection of private property

26. See https://brasil500anos.ibge.gov.br/.

27. One example is the reaffirmation and institutionalization of the policy promoted and carried out by former Rio de Janeiro Governor Wilson Witzel, who was also impeached, under the directive to "aim at the little head." Since his election in 2018, police operations in Rio de Janeiro's favelas have also increased indiscriminately under his successor, Cláudio Castro. Castro also invested heavily in facial recognition technologies without any impact assessment or consideration of the territory's structural conditions. What has been most apparent is the continuing succession of "stray" bullets striking people in Rio's communities, as exemplified by the massacre in the Jacarezinho favela on May 6, 2021, which left 28 people dead, including a police officer. By failing to protect lives in practice, the state is already failing profoundly, particularly given that Rio de Janeiro's public security indicators have not improved significantly. MENA, Fernanda. 'Mirar na cabecinha' é errar o alvo. Folha de São Paulo. November 7, 2018. Available at: https://www1.folha.uol.com.br/colunas/fernanda-mena/2018/11/mirar-na-cabecinha-e-errar-o-alvo.shtml. Accessed August 2024.

to target forms of deviance typical of the socially weakest and most marginalized groups."[28] [29] In doing so, however, this actor does not consider the social processes inherent in its own history.

Achille Mbembe makes a significant contribution to this literature through the concept of necropolitics. Initially considering state action, the concept rests on the idea that sovereignty is the capacity to exercise control over mortality and define life as the deployment and manifestation of power.[30] Given that data also fall within the spectrum of power relations, Smart Cities models conceived without citizen participation essentially express an act of power alone, serving as tools for automating systematic oppression. This further harms those who have historically lacked full enjoyment of their fundamental rights and have traditionally been subjugated and controlled.

The state's social and political power to dictate how some people may live and how others must die, an aspect of Mbembe's concept of necropolitics, leads us to consider more than the biological death of bodies, important as that is in itself. There are also acts that dehumanize, silence, and curtail fundamental rights,[31] such as privacy and data protection. These acts, explained by structural racism and propagated through Smart Cities models, subject Black people to "deaths in life," by analogy with what Mbembe also understands as "invisible killings."[32]

28. BARATTA, Alessandro. Criminologia crítica e crítica do direito penal: introdução à sociologia do direito. Translated by Juarez Cirino dos Santos. Rio de Janeiro: Instituto Carioca de Criminologia/Revan, 3rd edition, 2002. p. 176.

29. State institutions use data, such as social media posts, to trigger investigations that culminate in police operations, as in the Jacarezinho massacre on May 6, 2021, in Rio de Janeiro. Considered the deadliest such event in the city's history, the police operation resulted in the deaths of 28 people, including 1 police officer. It raised numerous suspicions of unlawful conduct and human rights violations. Despite the gravity of the case and the resulting need for transparency, the operation report was classified 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 July 2024. See NUNES, Pablo; SILVA, Mariah Rafaela; OLIVEIRA, Samuel R. de. Um Rio de câmeras com olhos seletivos: uso do reconhecimento facial pela polícia fluminense. Rio de Janeiro: CeSec, 2022, p. 14. Available at: https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Accessed August 2024.

30. MBEMBE, Achille. Necropolítica. Biopoder, soberania, estado de exceção, política da morte (ebook). São Paulo: N-1 edições, 2018. p. 7.

31. In this regard, it is worth recording the account of João Antônio, a young Black football fan who suffered severe humiliation—something that must never be normalized—when detained at a stadium in Sergipe after a "failure" in the recognition system used by the police: "At the Campeonato Sergipano final, I went through a situation I never imagined possible. I am sharing it with shame and indignation so that something happens and it does not happen again. I was extremely embarrassed, trying to hide my face. I did not know what to do because the entire Confiança crowd was looking at me, people I knew and people I did not." After the incident, Sergipe's government suspended the system and announced that it would review its procedures to prevent humiliating situations like João Antônio's. Torcedor é detido por engano em Sergipe após falha da ferramenta de reconhecimento facial. O Dia, 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 August 2024.

32. MBEMBE, Achille. Necropolítica. Biopoder, soberania, estado de exceção, política da morte (ebook). São Paulo: N-1 edições, 2018. p. 38.

This is also a significant concern for the National Data Protection Authority (ANPD), the body responsible for overseeing and regulating the LGPD and an ally in the struggle to ensure Brazilian citizens' full enjoyment of privacy and data protection rights:

> Data collected by governments and companies in various areas of cities can generate information, categorizations, and detailed reports on residents' personal lives, worsening asymmetries of information and power.[33]

This situation highlights the importance of investing in education, a right fundamental to social development. According to Paulo Freire, the patron of Brazilian education, neglecting this issue contributes to maintaining oppressive structures founded on an unjust order and responsible for violence against historically vulnerable individuals who, not by chance, live in the city's communities and peripheries. This further inflames social inequalities.[34]

It is also urgent to ensure citizen participation in decision-making, whether through public consultations or impact assessments. Civil society organizations, including some referenced here, have generally made significant contributions through methodological research assessing the impacts of introducing an extreme surveillance model. We must also consider the lack of diversity among decision-makers, across sectors ranging from governments to social institutions and businesses.[35] This is fundamental to building a culture of greater dialogue among different social groups in all their dimensions, particularly to develop a truly humane perspective on the most vulnerable populations, who are also data subjects. Final Considerations

33. GOB.BR AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Cidades Inteligentes. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf. Accessed July 2024.

34. FREIRE, Paulo. Pedagogia do Oprimido. 78th edition. Rio de Janeiro: Paz e Terra, 2021.

35. The IBGE survey Desigualdades sociais por cor ou raça no Brasil found that 69% of managerial positions in the country are held by White people, while only 29.5% are held by Black or Brown (pardo) people. See IBGE – Instituto Brasileiro de Geografia e Estatística, 2022 (Second Edition). Desigualdades sociais por cor ou raça no Brasil. Available at: https://static.poder360.com.br/2022/11/IBGE-DESIGUALDADES-11.NV_.pdf. Accessed August 2024.

Increasing urbanization and digitization under the Smart Cities label promise significant improvements in quality of life through advanced technologies. However, the reality of many Brazilian cities reveals a complex web of social and economic inequalities that cannot be ignored when importing and implementing these technologies, lest we further automate historical forms of oppression.

This work has discussed how the advance of Smart Cities can either reinforce or mitigate existing social inequalities, depending on the historical and social context of the territory and the economic sector in which technological resources are employed, particularly public security. Citizen participation is vital: without the active inclusion of all voices, especially marginalized communities and groups, technological innovations risk perpetuating historical exclusion and discrimination. As the analysis of Achille Mbembe's concept of necropolitics has shown, technology can be used as a tool for extreme surveillance, social control, biological death, and "death in life," worsening the vulnerability of populations already facing systemic oppression.

The protection of privacy and personal data rights emerges as a central pillar in discussions of fundamental rights in the information age. In Brazil, the LGPD represents a significant advance in regulating personal data processing, seeking to guarantee individuals' privacy and autonomy. However, effective implementation of these protections also depends on broad awareness and a stronger data protection culture, which must be widely accessible to all citizens regardless of socioeconomic background.

If implemented without an inclusive governance structure, the Smart Cities model can amplify existing inequalities and become another layer of social control. For smart cities to contribute to a fairer, more equitable future, it is essential to integrate policies promoting digital equity and social and racial justice, ensuring that all communities have equal access to technology's benefits, provided that technology is centered on human beings.

Finally, smart city development must be guided by transparency, inclusion, and respect for fundamental rights. Citizen participation must not be merely an additional component,

but the foundation on which urbanization and digitization policies are built. Only through a truly participatory approach can we move toward cities that use technology not only to innovate but also to promote the dignity and well-being of all their inhabitants.

References

BARATTA, Alessandro. Criminologia crítica e crítica do direito penal: introdução à sociologia do direito. Translated by Juarez Cirino dos Santos. Rio de Janeiro: Instituto Carioca de Criminologia/ Revan, 3rd edition, 2002. p. 176.

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 July 2024.

BOLLA, Carla. Como a França popularizou o uso de talheres. Forbes. September 15, 2022. Available at: https://forbes.com.br/forbeslife/2022/09/carla-bolla-como-a-franca-popularizou-o-uso-de-talheres/. Accessed July 2024.

BRASIL: 500 anos de Povoamento. Instituto Brasileiro de Geografia Estatística (IBGE). Available at: https://brasil500anos.ibge.gov.br/.

CAMARGO, Bianca. Cerca de 84% dos lares brasileiros têm acesso à internet, diz pesquisa. 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 August 2024.

CENTRO DE TECNOLOGIA E SOCIEDADE. Available at: https://direitorio.fgv.br/pesquisa/centro-de-tecnologia-e-sociedade.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados [e-book]. 2nd edition. São Paulo: Thomson Reuters Brasil, 2019. p. 33.

FREIRE, Paulo. Pedagogia do Oprimido. 78th edition. Rio de Janeiro: Paz e Terra, 2021.

GOB.BR. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Cidades Inteligentes. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf. Accessed July 2024.

Instituto de Tecnologia e Sociedade do Rio de Janeiro do Rio. Big data no Sul Global. Relatório sobre estudos de caso. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2016. Available at: https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf. Accessed July 2024.

Instituto Brasileiro de Geografia e Estatística, 2022 (Second Edition). Desigualdades sociais por cor ou raça no Brasil. Available at: https://static.poder360.com.br/2022/11/IBGE-DESIGUALDADES-11.NV_.pdf. Accessed August 2024.

MBEMBE, Achille. *Necropolítica. Biopoder, soberania, estado de exceção, política da morte (ebook)*. São Paulo: N-1 edições, 2018. p.7.

MENA, Fernanda. 'Mirar na cabecinha' é errar o alvo. Folha de São Paulo. November 7, 2018. Available at: https://www1.folha.uol.com.br/colunas/fernanda-mena/2018/11/mirar-na-cabecinha-e-errar-o-alvo.shtml. Accessed August 2024.

MENDES, Teresa Cristina M. Smart Cities: Solução para as cidades ou aprofundamento das desigualdades sociais? Rio de Janeiro, 2020. Available at: https://www.observatoriodasmetropoles.net.br/wp-content/uploads/2020/01/TD-011-2020_Teresa-Mendes_Final.pdf. Accessed July 2024.

MOURA, Clóvis. Escravismo, colonialismo, imperialismo e racismo. Afro-Ásia, Salvador, no. 14, 1983. Available at: https://periodicos.ufba.br/index.php/afroasia/article/view/20824/13425. Accessed July 2024.

NUNES, Pablo; SILVA, Mariah Rafaela; OLIVEIRA, Samuel R. de. Um Rio de câmeras com olhos seletivos: uso do reconhecimento facial pela polícia fluminense. Rio de Janeiro: CeSec, 2022, p. 14. Available at: https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Accessed August 2024.

O Dia, 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 August 2024.

PROJETO DE LEI Nº 976/2021. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1977843&filename=PL%20976/2021. Accessed July 2024.

REIA, Jess; BELLI, Luca. Smart Cities no Brasil: regulação, tecnologia e direitos. Belo Horizonte, MG: Casa do Direito, 2021. p. 112. Available at: https://repositorio.fgv.br/server/api/core/bitstreams/390c1729-357b-4c4f-ba30-e236419debf1/content. Accessed July 2024.

RIBEIRO, Laura Talho. Tecnologias inteligentes de vigilância: percepções sobre segurança nos centros urbanos. Available at: https://itsrio.org/wp-content/uploads/2018/03/laura_talho_smartsurveillance.pdf. Accessed July 2024.

RODOTÁ, Stefano. Corpo Eletrônico e Privacidade. Lecture delivered at the Universidade do Rio de Janeiro, Rio de Janeiro, November 06, 2015.

SANTO, Thaís Espírito. RJ anuncia câmeras com reconhecimento facial e leitura de placas em viaturas da PM. G1, Rio de Janeiro, April 03, 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-em-viaturas-da-pm.ghtml. Accessed July 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. Unidade do ordenamento na pluralidade das fontes: uma crítica à teoria dos microssistemas. In: SCHREIBER, Anderson; KONDER, Carlos Nelson (coordinators). Direito civil constitucional. E-book. São Paulo: Atlas, 2016.

SILVA, Tarcízio. *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. São Paulo: Edições Sesc São Paulo, 2022.

TAMBELLI, Clarice Nassar. Smart Cities: uma breve investigação crítica sobre os limites de uma narrativa contemporânea sobre cidades e tecnologia. Available at: https://itsrio.org/wp-content/uploads/2018/03/clarice_tambelli_smartcity.pdf. Accessed July 2024.

TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. 1st edition. Indaiatuba, SP: Foco, 2022. E-book.

VELLASCO, Ramon. Fórum Popular de Segurança Pública é lançado no Rio de Janeiro. Observatório de Favelas. Rio de Janeiro. June 29, 2023. Available at: https://observatoriodefavelas.org.br/forum-popular-de-seguranca-publica-e-lancado-no-rio-de-janeiro/. Accessed August 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

12

Implementing Smart Cities and a Regulatory Sandbox: Challenges and Opportunities in Juiz de Fora's Innovation Law

DANIEL SANTIAGO DINIZ

Contents: Introduction. 1. History, Technology, and Governance in Smart Cities. 2. Legislative Foundations for Innovation in Brazil. 3. Juiz de Fora's Innovation Law: 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 as a promising solution to contemporary urban challenges. Central objectives of these initiatives include using information and communication technologies (ICTs) to optimize urban services' efficiency, improve citizens' quality of life, and promote sustainable development. However, the practical implementation of these concepts varies significantly, prompting debates about these strategies' actual effectiveness and inclusiveness.

In Brazil, legislative frameworks and regulations establish the foundations for technological advancement in urban environments, particularly the Legal Framework for Innovation and the Legal Framework for Startups. These instruments promote innovation and experimentation ecosystems across different levels of government, encouraging public-private cooperation. In this context, Juiz de Fora's Innovation Law (Law No. 14.746/2023) exemplifies how a Brazilian city can adapt national guidelines to encourage local innovation. It introduces mechanisms such as the regulatory sandbox, a controlled environment in which innovations can be tested in accordance with specific municipal regulations.[2]

This article seeks to answer the question: "How does Juiz de Fora's Innovation Law implement smart city principles through its regulatory framework and sandbox, and what challenges and opportunities does this approach present?" The article proceeds from the theoretical and historical foundations of smart cities, including the critical perspectives

1. Attorney and public administrator, with a law degree from the Universidade Federal de Juiz de Fora (UFJF); postgraduate student in Digital Law at the Universidade do Estado do Rio de Janeiro (UERJ) and the Instituto de Tecnologia e Sociedade do Rio (ITS Rio).

2. JUIZ DE FORA. Lei nº 14.746, de 04 de dezembro de 2023. Establishes Juiz de Fora's Innovation System; defines the municipality's development hubs; provides for the responsibilities of the Municipal Council for Development, Technology and Innovation (Comdeti), and other measures. Diário Oficial do Município de Juiz de Fora, Juiz de Fora, MG, December 05, 2023.

of authors such as Robert G. Hollands,[3] Evgeny Morozov, and Francesca Bria,[4] to an analysis of the Brazilian legislative foundations facilitating this urban transformation.

The study examines Juiz de Fora's Innovation Law in depth, considering its structure, mechanisms, and expected impacts, with particular attention to Decree No. 16.734/2024 [5], which details how the regulatory sandbox operates. The analysis explores how regulation seeks to balance innovation with social responsibility and promote urban governance aligned with community interests. The final considerations present the main findings and suggestions for improving the application of smart city concepts, emphasizing governance that sustains fair, sustainable, and innovative urban development.

1. History, Technology, and Governance in Smart Cities

Smart cities, as discussed by Robert G. Hollands,[6] are characterized by the use of information and communication technologies (ICTs) to improve urban services' efficiency and citizens' quality of life. However, Hollands argues that the concept is multifaceted and open to various interpretations, which may lead to a superficial or distorted understanding of what constitutes a smart city. He emphasizes that the term "smart" is often associated with positive urban technological innovations but warns that this label can conceal 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 questioning. Many cities call themselves smart 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, vol. 12, no. 3, pp. 303-320, 2008. DOI: 10.1080/13604810802479126.

4. MOROZOV, Evgeny; BRIA, Francesca. A cidade inteligente: tecnologias urbanas e democracia. Translated by Humberto do Amaral. São Paulo: Ubu Editora, 2019. 192 pp. ISBN: 978-85-7126-046-7.

5. JUIZ DE FORA. Decreto nº 16.734, de 20 de agosto de 2024. Regulates the operation of the regulatory sandbox in Juiz de Fora and specifies the conditions for its implementation and supervision. Diário Oficial do Município de 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, vol. 12, no. 3, pp. 303-320, 2008. DOI: 10.1080/13604810802479126.

complex urban problems and suggests that a deeper, more critical understanding of ICTs' social and political implications for cities is needed. He emphasizes the importance of considering social justice and inclusion in discussions of smart cities.

According to the Organisation for Economic Co-operation and Development (OECD),[7] smart cities involve the effective use of digitization to improve residents' quality of life by providing more efficient, sustainable, and inclusive urban services and environments.

Morozov and Bria discuss urban technologies' social and democratic implications.[8] Although ICTs promise more efficient and safer cities, there is a significant risk that they will primarily benefit private interests rather than serve the common good. The authors emphasize 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 turn driven by large corporations has made data an essential element of the neoliberal economy. Filled with sensors and algorithmic systems, smart cities become spaces for constant data extraction, control, and behavioral modulation. To prevent smart cities from becoming machines that make workers' lives more precarious and benefit only private interests, Morozov and Bria propose democratic and inclusive cooperative management of urban technologies. They emphasize the need to regain control of technologies, data, and infrastructure to ensure governance that promotes citizen participation and social equity.

According to Morozov and Bria, urban technology implementation must be accompanied by policies ensuring democratic participation and social inclusion. They suggest creating shared infrastructure and promoting technological sovereignty, with data governance and collaborative practices as essential elements. Cities must therefore adopt approaches allowing citizens to deliberate on the use of their data and actively participate in developing the technologies that shape their urban environment.

7. OCDE. Smart Cities and Inclusive Growth. 2020. Available at: https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf.

8. MOROZOV, Evgeny; BRIA, Francesca. A cidade inteligente: tecnologias urbanas e democracia. Translated by Humberto do Amaral. São Paulo: Ubu Editora, 2019. 192 pp. ISBN: 978-85-7126-046-7.

In discussing smart cities' social and democratic implications, it is crucial to recognize the challenges and opportunities arising from cities' digital transformation. There is potential to improve urban quality of life significantly through efficiency and innovation. However, without careful regulation and orientation toward the common good, these technologies may exacerbate social inequalities and create new forms of exclusion. Innovative legislation therefore plays a fundamental role in ensuring that smart cities not only use advanced technologies but also promote fair and inclusive urban development.

The development of e-government is crucial to the evolution of smart cities. According to Jon Agar,[9] its history can be traced to early efforts to mechanize and computerize government processes. Integrating information technologies into administrative processes profoundly affected government institutions' efficiency and responsiveness. The e-government revolution began with basic office technologies such as typewriters and filing systems and evolved toward computers and digital networks.

In smart cities, e-government means applying digital technologies to improve urban management and public service delivery. Agar argues that government computerization was a crucial step toward implementing smart technologies in cities, allowing administrative tasks to be automated and communication between government departments to improve. Introducing computer systems into public administration transformed how data are collected, stored, and used, facilitating decision-making and more efficient, transparent services.

The interaction between technology and governance is another important aspect of smart cities' evolution. Eden Medina[10] discusses how implementing cybernetic systems in Allende's Chile provides an early example of integrating technology into urban governance to create smarter cities. During Salvador Allende's government, cybernetic systems were introduced to manage the national economy, a pioneering

9. AGAR, 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.

attempt to use advanced technologies to improve public administration's efficiency and transparency.

Medina emphasizes that integrating technologies into urban governance can bring significant benefits, such as improved administrative efficiency, transparency in government operations, and citizen participation. However, she also warns of associated challenges and risks, such as centralized power and the potential exclusion of marginalized groups. The Chilean experience demonstrates the need for a balanced approach that uses technology to empower citizens and promote more inclusive, participatory governance.

The evolution of e-government and the interaction between technology and governance illustrate how cities can become smarter and more efficient through technological integration. The history of e-government described by Agar and the Chilean example of cybernetic systems discussed by Medina show that successfully implementing technologies in cities depends on considering both the benefits and challenges of these innovations.

In this context, introducing regulatory sandboxes represents a significant advance in public administration's experimentalist approach to promoting innovation. According to Quirino, Hocayen, and Cunha,[11] a regulatory sandbox is a controlled environment in which rules applicable to innovative products or services are temporarily suspended to test their market impact. This tool allows local public administration to experiment and adjust its regulations based on evidence, promoting economic development more closely aligned with local needs.

The regulatory sandbox is a strategic tool allowing public administration to create experimental environments in which regulatory rules are temporarily relaxed, facilitating the development and testing of innovative products or services without the restrictions of traditional regulations. According to Quirino, Hocayen, and Cunha, this experimentalist approach is particularly advantageous for local administrations because it offers a safe testing ground. Public administration can observe innovations' impacts under controlled conditions and continuous supervision, promoting more dynamic economic development adapted to each locality's specific needs.

11. QUIRINO, Carina de Castro; HOCAYEN, Helena Gouvêa de Paula; CUNHA, Marcella Brandão Flores da. Sandbox regulatório: instrumento experimentalista à disposição da Administração Pública local como suporte ao desenvolvimento econômico. R. de Dir. Público da Economia – RDPE, Belo Horizonte, vol. 21, no. 84, pp. 9-33, October/December 2023.

A regulatory sandbox's potential lies in the flexibility it offers local governments to implement emerging urban technologies and test innovative solutions that can transform public administration and city life. However, this flexibility presents considerable challenges. For a sandbox to fulfill its role effectively, solid interinstitutional collaboration and comprehensive, inclusive governance of the experimental regulatory environment are essential. Multiple sectors, such as transport, public security, and digital infrastructure, must participate to integrate innovations harmoniously into urban policies and ensure that the results meet collective objectives.

A critical challenge in implementing regulatory sandboxes effectively is defining rigorous criteria and limits for company participation. Without detailed regulations setting operational limits, a sandbox may function as a regulatory loophole rather than a space for responsible experimentation. Hollands, Morozov, and Bria[12] warn of this risk, discussing how the smart city concept is often used rhetorically to promote urban technology without deeply analyzing social impacts or the need for inclusion. They emphasize that, without clear guidelines, urban innovations may favor large corporations and promote data extraction and behavioral control at the expense of collective well-being and social justice.

Transparency in selecting and monitoring participating companies is also fundamental. Regulatory sandboxes must have supervision and monitoring guidelines to ensure companies meet their established responsibilities and emerging risks are identified and mitigated promptly. According to Quirino et al., the sandbox must function as a testing ground with a constant feedback cycle between 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 promotes urban technologies ethically and inclusively.

Another critical factor in regulatory sandboxes' success is adapting to rapid changes in the urban and technological context. The experimental approach offered by the sandbox allows public administration to adjust

12. HOLLANDS, Robert G. Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? City, vol. 12, no. 3, pp. 303-320, 2008; MOROZOV, Evgeny; BRIA, Francesca. A cidade inteligente: tecnologias urbanas e democracia. Translated by Humberto do Amaral. São Paulo: Ubu Editora, 2019.

rules as the technologies being tested develop, but this requires a commitment to adaptive governance and responsible innovation. Morozov and Bria argue that urban technology implementation must be accompanied by mechanisms of technological sovereignty, ensuring citizens control their data and actively participate in building a smart urban environment. This is particularly important in smart cities, where new technologies can directly affect urban life and create new ethical, social, and political challenges.

The regulatory sandbox thus has the potential to promote sustainable and inclusive urban innovation by providing a controlled space to test and evaluate new technologies before large-scale deployment. Challenges involving governance, criteria, and transparent supervision highlight the need for a cautious approach and robust regulation. The sandbox thereby enables innovative solutions to be tested while also contributing to a more responsive public administration committed to ethical and responsible digital transformation.

2. Legislative Foundations for Innovation in Brazil

In response to growing demands for technological development and sustainability, Brazil has consolidated an innovative legislative framework providing a foundation for advances in science, technology, and innovation at various levels. These “legislative foundations for innovation in Brazil” include significant legal frameworks and their specific regulations, such as the Legal Framework for Innovation (Law No. 13.243/2016),[13] the Legal Framework for Startups (Supplementary Law No. 182/2021),[14] and strategic guidelines such as the Brazilian Charter for Smart Cities.[15] These laws and guidelines are fundamental to creating environments conducive to innovative ecosystems, from the federal to the municipal level.

The Legal Framework for Innovation, enacted in 2016, improves on the 2004 Innovation Law (Law No. 10.973/2004)[16] by establishing mechanisms to simplify

13. BRASIL. Lei nº 13.243, de 11 de janeiro de 2016. Provides incentives for scientific development, research, scientific and technological capacity building, and innovation, and amends various laws. Diário Oficial da União: section 1, Brasília, DF, p. 1, January 12, 2016.

14. BRASIL. Lei Complementar nº 182, de 1º de junho de 2021. Establishes the legal framework for startups and innovative entrepreneurship and amends Supplementary Law No. 123 of December 14, 2006. Diário Oficial da União: section 1, Brasília, DF, p. 2, June 2, 2021.

15. Ministério do Desenvolvimento Regional. *Carta Brasileira para Cidades Inteligentes*. Brasília, 2021.

16. BRASIL. Lei nº 10.973, de 2 de dezembro de 2004. Provides incentives for innovation and scientific and technological research in the productive sector, and other measures. Diário Oficial da União: section 1, Brasília, DF, p. 2, December 3, 2004.

cooperation between the private sector and public research institutions, seeking to decentralize support for innovation to states and municipalities. This framework revises nine federal laws and introduces independent measures facilitating science and technology development in the country. Decree No. 9.283/2018 [17], complements the regulation of the Legal Framework for Innovation, establishing incentives such as economic subsidies and technology procurement contracts that strengthen technology transfer from Scientific, Technological and Innovation Institutions (ICTs) to the market. The decree allows direct and indirect public administration bodies, including ICTs, to hold minority equity stakes in innovative companies, encouraging the creation of innovative products and processes.

The regulations also encourage cooperation between public and private entities on Research, Development and Innovation (RD&I) projects, providing greater legal certainty for partnerships and facilitating innovation policies. Public-private partnership programs financing renewable energy and green technology projects exemplify this cooperation.

Regarding the Internet of Things (IoT), Decree No. 9.854/2019 [18], which established the National Internet of Things Plan, advanced the country's objective of implementing and developing IoT. It promotes free competition and the free flow of data while respecting information security and personal data protection guidelines. Developed through a partnership between the Ministry of Science, Technology and Innovation and the Banco Nacional de Desenvolvimento Econômico e Social (BNDES), the plan encourages smart cities that use sensors and IoT networks to improve public services such as transport and security.

Supplementary Law No. 182/2021, known as the Legal Framework for Startups, complements innovation initiatives by establishing a favorable regulatory environment for startups and entrepreneurs. It defines specific guidelines to encourage Brazil's startup ecosystem, including experimental regulatory environments known as regulatory sandboxes, which allow innovations to be tested with regulatory flexibility.

17. BRASIL. Decreto nº 9.283, de 7 de fevereiro de 2018. Regulates Law No. 10.973 of December 2, 2004, and Law No. 13.243 of January 11, 2016, concerning incentives for innovation and scientific and technological research in the productive sector. Diário Oficial da União: section 1, Brasília, DF, p. 1, February 8, 2018.

18. BRASIL. Decreto nº 9.854, de 25 de junho de 2019. Establishes the National Internet of Things Plan and provides for the Management and Monitoring Chamber for the Development of Machine-to-Machine Communication and Internet of Things Systems. Diário Oficial da União: section 1, Brasília, DF, p. 5, June 26, 2019.

Key elements of Supplementary Law No. 182/2021 include a clear definition of a startup, facilitating access to incentive and financing programs; public procurement mechanisms favoring startup participation, such as procurement through technological challenges; tax incentives; and easier access to investment for early-stage startups. Regulatory sandboxes allow new technologies and business models to be tested in a controlled environment, mitigating regulatory risks and promoting innovation. One practical example is the Banco Central do Brasil's regulatory sandbox, which allowed financial startups to develop and test new digital payment solutions.[19]

In 2020, the federal government launched an essential guide to sustainable and innovative urban development in Brazil: the Brazilian Charter for Smart Cities.[20] Developed collaboratively, the Charter seeks to integrate digital transformation and sustainable urban development, addressing issues such as reducing inequalities, digital inclusion, innovative urban governance, and local economic development.

The Charter establishes fundamental guidelines for smart city development. One notable guideline is the importance of specific legislation for implementing smart technologies in Brazilian cities. The legislation must be robust and capable of integrating ICTs in ways that promote sustainability, social inclusion, and urban efficiency.

Legislation plays a crucial role in creating an environment conducive to adopting and developing smart technologies. It provides the necessary legal foundation for cities to integrate ICTs into urban processes, facilitating resource management, public service delivery, and digital inclusion.

To address urban and social challenges, the Charter emphasizes that digital transformation must be accompanied by public policies ensuring equity and sustainability. These include promoting internet accessibility, personal data protection, citizen participation, and transparent governance. The Charter integrates urban development and digital transformation agendas to define a Brazilian concept of

19. AMATO, Lucas Fucci; MISSAGIA, Caio Rezende. Ambientes regulatórios experimentais: o sandbox no sistema financeiro brasileiro. RBSD – Revista Brasileira de Sociologia do Direito, vol. 10, no. 3, pp. 143-171, September/December 2023.

20. Ministério do Desenvolvimento Regional. *Carta Brasileira para Cidades Inteligentes*. Brasília, 2021.

smart cities, present a coordinated public agenda, and support municipalities in their local actions.

Since 2021, Bill (PL) No. 976, which seeks to establish a National Smart Cities Policy (PNCI), has been under consideration. It aims to improve quality of life in municipalities and establishes the policy's guiding principles and guidelines, objectives, actions, and allocable resources. The bill was referred to the Chamber of Deputies' Committee on Constitution, Justice and Citizenship on July 11, 2022, where it remains awaiting the rapporteur's opinion.

Under the ABNT standard based on ISO 37122 (ABNT, 2021),[21] a smart city accelerates the achievement of sustainable social, economic, and environmental outcomes. It also significantly improves social engagement, applies collaborative leadership, integrates municipal disciplines and systems, and uses data and modern technologies to provide better services and quality of life for 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 it, the city underwent a rigorous process assessing as many as 252 indicators, including sustainability, mobility, health, education, and public security.

Innovative legislation's importance lies in its ability to establish a regulatory framework that not only supports but also promotes cities' sustainable and inclusive digital transformation. Global population growth, particularly in urban areas, presents significant economic, social, organizational, and structural challenges. Smart cities will be fundamental to addressing these challenges and meeting the demands of large urban areas.

By following the Brazilian Charter for Smart Cities and the legislation discussed, Brazilian cities can develop more evenly, addressing the challenges of the twenty-first century through technological solutions that improve all citizens' quality of life. In this context, municipal regulations such as Law No. 14.746/2023 and Decree No. 16.734/2024 play a notable role in complementing

21. ABNT NBR ISO 37122:2021. Cidades e comunidades sustentáveis – Indicadores para cidades inteligentes. Associação Brasileira de Normas Técnicas, 2021.

federal frameworks, promoting a robust local innovation ecosystem and applying national guidelines at the municipal level.

3. Juiz de Fora's Innovation Law: Structure, Mechanisms, and Impacts

Law No. 14.746/2023, which establishes Juiz de Fora's Innovation System, sets out objectives and guidelines to promote technological innovation, sustainable development, and economic competitiveness in the city. It seeks to create an environment conducive to the growth of startups, technology companies, and technology-based cooperatives, providing the financial, structural, and regulatory support needed to develop new technologies and business models.

One of the law's main objectives is to stimulate, organize, and support innovation ecosystems and mechanisms in Juiz de Fora and the surrounding region. Law No. 14.746/2023 was regulated by three main decrees: Decree No. 16.372/2024 [22], addressing the composition and responsibilities of the Municipal Council for Development, Technology and Innovation (COMDETI); Decree No. 16.448/2024 [23], defining guidelines for creating and operating the Municipal Innovation System (Simi-JF); and Decree No. 16.734/2024 [24], addressing complementary aspects not covered by the earlier decrees, including details on co-investment funds, minority stakes in special purpose entities, seed capital, and the sandbox's experimental regulatory environment.

As specified in Article 1, the law's mission is to promote startups, sustainable companies, businesses with low social and environmental impacts, local production networks, and technology-based cooperatives. It aims to enhance these organizations' competitiveness, cooperation, and growth, focusing on generating innovative products, processes, and services and transferring and disseminating technologies.

To achieve these objectives, the law establishes the Municipal Innovation System of Juiz de Fora (Simi-JF) and the Municipal Innovation

22. JUIZ DE FORA. Decreto nº 16.372, de 30 de janeiro de 2024. Regulates Articles 39, 40, and 41 of Municipal Law No. 14.746 of December 04, 2023, concerning the composition and responsibilities of the Municipal Council for Development, Technology and Innovation (COMDETI), and other measures. Diário Oficial do Município de Juiz de Fora, Juiz de Fora, MG, January 31, 2024.

23. JUIZ DE FORA. Decreto nº 16.448, de 11 de março de 2024. Regulates Articles 1, 2 (I), and 6 of Municipal Law No. 14.746 of December 04, 2023, concerning the creation, composition, and purposes of Juiz de Fora's Municipal Innovation System. Diário Oficial do Município de Juiz de Fora, Juiz de Fora, MG, March 12, 2024.

24. JUIZ DE FORA. Decreto nº 16.734, de 11 de setembro de 2024. Provides for the municipality's innovation system and other measures. Diário Oficial do Município de Juiz de Fora, Juiz de Fora, MG, September 12, 2024.

Development Fund (FMDI) as its main support instruments, as detailed in Article 2. These mechanisms are fundamental to providing financial and structural support for innovation initiatives, ensuring projects have the resources needed for development and implementation. Capacity building and social inclusion are also priorities, with Article 3 emphasizing the importance of providing the municipal productive sector with additional human resources and specific technologies. The law also seeks to support programs and projects promoting innovation, social inclusion, renewable energy, environmental preservation, and the mitigation of social and environmental impacts, encouraging sustainable city models.

The FMDI, provided for in Article 2, II, is a fundamental financial instrument for supporting municipal innovation projects. It is intended to support projects promoting science, technology, and innovation, providing resources to develop new innovative products, processes, and services. Under Article 21, FMDI resources subsidize technology vouchers, innovation research scholarships, technology procurement contracts, innovative management systems, scientific and technological capacity-building projects, and the organization of and participation in science, technology, and innovation events.

The law allows Juiz de Fora's municipal government and its autonomous agencies, foundations, and controlled companies to participate in co-investment funds and special purpose entities. Registered with the Comissão de Valores Mobiliários (CVM), these funds aim to support innovative companies, primarily those based in Juiz de Fora and focused on technology. As specified in Article 4, the law permits minority equity stakes in special purpose entities and technology-based cooperatives, expanding support for scientific and technological projects in the municipality. This mechanism enables alignment with the city's strategic innovation priorities and stronger public-private connections.

In addition to co-investment funds, the law regulates seed capital contributions to innovative companies undertaken in partnership with Science, Technology and Innovation Institutions (ICTs), following financial and technological impact guidelines. This capital targets companies formally included in strategic innovation areas that present robust business plans aligned with the municipality's economic and social priorities. Management and monitoring of these funds and the municipality's

participation are coordinated by the Municipal Department of Sustainable and Inclusive Development, Innovation and Competitiveness (SEDIC) and the Finance Department.

Another aspect regulated by the law concerns innovation-promoting environments (APIs), defined as financial or virtual spaces intended to encourage innovation and entrepreneurship in Juiz de Fora. The main environments include accelerators, incubators, technology parks, innovation ecosystems, and Living Labs. Under Article 5, business accelerators participate in, monitor, and invest material and financial resources in startups, receiving returns such as equity stakes, royalties, and other revenues. Incubators, in turn, house and support startups, providing guidance and support through graduation as well as the infrastructure needed for their development.

Technology parks and public innovation ecosystems are described in the law as areas enabling the integration of scientific and technological research, businesses, and government organizations, supporting their interrelationships to develop innovative products and processes. The decree also regulates these innovation environments to ensure they meet safety criteria and economic and environmental impact projections.

Decree No. 16.734/2024 also contains provisions for the experimental regulatory environment, or regulatory sandbox, originally introduced by Law No. 14.746/2023. The sandbox allows companies to develop and test technological innovations in a controlled environment under temporary authorization, facilitating experimentation while managing the risks associated with new technologies. The decree establishes clear criteria for creating and operating the sandbox, requiring substantiated proposals with specific innovation plans, objectives, testing methodologies, schedules, and risk assessments. These regulations are essential to ensuring a safe experimental space that encourages innovation.

Regarding governance, Decree No. 16.734/2024 stipulates that COMDETI and SEDIC will supervise sandbox projects through audits and continuous monitoring, ensuring that performance targets and risk mitigation measures are met. Authorization to participate in the sandbox is valid for up to 12 months and may

be extended on technical grounds. Public administration also promotes transparency by publishing official notices, public calls, and evaluation results for innovative projects.

Juiz de Fora's innovation system is governed in a way intended to ensure transparency, effectiveness, and supervision of projects financed and encouraged by the law. COMDETI plays a central role. The Management Council of the Municipal Innovation Development Fund (FMDI) is responsible for planning and allocating the fund's resources under Articles 22 to 24. It comprises representatives of several municipal departments and civil society, ensuring broad and diverse representation.

Its responsibilities include approving the FMDI's budgetary and financial resource programming; evaluating and approving economic development, technology, and innovation projects financed by the fund; preparing the Annual Resource Allocation Plan; creating and publishing the annual activity report; and overseeing resource use to ensure legality and transparency in the allocation of grants. It also evaluates the indicators and targets achieved.

Tax incentives under Articles 25 to 36 include ITBI, ISSQN, and IPTU exemptions for companies in areas designated as Development and Innovation Hubs. These incentives seek to attract and expand technological enterprises in the municipality, creating a favorable environment for innovation and economic growth. Decree No. 16.734/2024 complements them by establishing specific conditions and procedures for granting tax benefits, including analysis of beneficiary companies' economic and social impacts.

Law No. 14.746/2023 and its three implementing decrees, particularly Decree No. 16.734/2024, establish a robust structure of support mechanisms and innovation-promoting environments essential to municipal technological development and economic competitiveness. Through financial investment, strategic partnerships, and comprehensive support infrastructure, Juiz de Fora's legislation creates a favorable environment for startups, technology companies, and technology-based cooperatives. These efforts align 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 de Fora

With the publication of Decree No. 16.734/2024, the regulation of Juiz de Fora's Innovation Law takes a significant step toward implementing the regulatory sandbox, detailing the conditions for creating, operating, and monitoring this experimental regulatory environment. Decree No. 16.734/2024 offers specific, defined guidelines for companies and innovation institutions to develop and test new technologies in a safe, controlled environment under public administration's supervision.

Chapter VI of Decree No. 16.734/2024 defines the regulatory sandbox as a set of special, simplified, temporary conditions allowing companies and institutions to develop, test, and implement technological innovations with specific authorization from regulators. It establishes the proposal submission process, covering both direct company requests and submissions through public calls. Proposals must include technology specifications, justification for creating the sandbox, expected objectives, testing plans, schedules, methodology, and risk assessment, allowing public administration to evaluate each project carefully before granting authorization.

Sandbox selection is based on criteria established by the decree, such as the degree of innovation and originality, potential economic, social, and environmental impacts, technical and economic feasibility, the proposing team's experience, and alignment with the municipality's strategic priorities. A technical committee appointed by COMDETI, comprising public administration representatives and experts in the relevant fields, evaluates proposals. This system seeks to admit only projects with high potential impact while minimizing the risks of experimenting with emerging technologies in an urban environment.

During participation, initially authorized for up to 12 months and extendable for an equal period on technical grounds, companies must submit periodic progress reports with interim results, challenges encountered, and recommendations for possible adjustments. Continuous supervision is performed by the Municipal Department of Sustainable and Inclusive Development, Innovation and Competitiveness (SEDIC),

together with the Finance Department and the Department of Digital and Administrative Transformation (STDA). This constant monitoring, including possible audits and technical visits, seeks to ensure projects meet safety and risk mitigation requirements, promoting innovation aligned with public interests.

The regulations also establish participating companies' responsibilities for maintaining and supporting technologies during testing. The municipality will provide the necessary infrastructure as agreed in the cooperation terms, and confidentiality and intellectual property terms will be defined to protect the data and information generated. At the end of testing, participating companies must submit a detailed final report documenting results, impact assessments, and possible recommendations for adopting or expanding the solution.

These detailed regulations represent a significant advance for Juiz de Fora's innovation ecosystem. In contrast to earlier criticism pointing to the lack of sandbox guidelines, Decree No. 16.734/2024 provides a robust, transparent structure for regulatory experiments. It responds to concerns raised by authors such as Hollands, Morozov and Bria, Agar, and Medina about the risks of unregulated technological initiatives and their possible appropriation by private interests. Through supervision, monitoring, and quality control, the decree seeks to ensure inclusive sandbox initiatives with citizen participation and social responsibility, minimizing the risk that experimentation benefits only private companies or centralizes power.

However, putting sandbox regulations into practice presents challenges. Continuous supervision, rigorous selection criteria, and defined performance indicators raise questions about the human and technical resources available to monitor all approved projects closely. Dependence on municipal oversight structures, even with several departments involved, may limit the sandbox's scope and reach, particularly as project numbers increase. This may affect the efficiency and safety of urban innovation testing if supervision is not structured to accommodate the initiatives' growth.

The authorization's duration also deserves attention. Although extensions offer flexibility for projects needing more testing time, they can create risks if quality control and regulatory compliance are not maintained throughout experimentation. The decree seeks to mitigate these risks through periodic reporting and audits, but their effectiveness depends on administrative capacity to respond to each project's particular circumstances.

The regulations also allow the municipality to assess whether to adopt or expand sandbox innovations at the end of testing, considering results and recommendations. This flexibility is important for urban development because it allows Juiz de Fora to adopt technological solutions demonstrated to be effective and safe. However, adoption decisions must consider not only technical results but also social and environmental impacts, ensuring the updated technology contributes to collective well-being rather than only private benefits.

Juiz de Fora's regulatory sandbox rules under Decree No. 16.734/2024 provide the necessary structure for controlled experimentation with technological innovations in urban environments. They address various safety and inclusion needs, providing an innovation space that promotes social responsibility and sustainability. However, for this experimental regulatory environment to fulfill its potential, public administration must be prepared to implement rigorous controls, guarantee transparency, and ensure technological development serves the population's interests without exclusion or marginalization.

Final considerations

This study has reviewed the concept and evolution of smart cities, considering their multiple interpretations and the challenges of implementing inclusive, effective urban technologies. Global innovation models and Brazilian legal frameworks were contextualized to identify legislation's essential role in promoting sustainable, technologically advanced urban environments. The analysis of Juiz de Fora's Innovation Law positions this legislative structure as a catalyst for

local economic and technological development, aligning the city with smart governance principles.

Analyzing Juiz de Fora's Innovation Law and its specific regulations reveals a coordinated effort to implement smart city principles 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 intended to create a favorable environment for technological and economic development. This ecosystem seeks to transform the city into an innovation center, promoting products and services that address contemporary urban needs.

The regulatory sandbox established by Decree No. 16.734/2024 is a significant innovation in this context. By allowing companies and institutions to test technologies in a controlled, supervised environment, it puts into practice the experimentalist principle fundamental to smart cities. This approach allows Juiz de Fora to explore technological innovations safely and in alignment with public interests, providing a basis for assessing new solutions' impacts before large-scale implementation. The sandbox thus advances efficient urban management and encourages responsible, ethical use of digital technologies.

However, the challenges are substantial. Rigorous selection criteria and inclusive governance highlight the complexity of managing the sandbox to promote collective benefits and avoid concentrating power. Continuous supervision of experimental projects and specific performance metrics are fundamental to ensuring tested technologies contribute to urban well-being and social justice. Without robust governance, these innovations risk favoring private interests at the expense of the inclusion and sustainability objectives that guide smart cities.

As an opportunity, the regulatory sandbox positions Juiz de Fora as a pioneering Brazilian city, creating a model for other localities seeking to integrate technology and urban governance responsibly. Through experimental practices, transparency, and citizen participation, the city can ensure that its innovation policies meet

the population's demands and reflect the principles of a truly smart city. The experimental regulatory environment also encourages a constant feedback cycle between the public and private sectors, allowing evidence-based regulatory adjustments and promoting economic development more closely aligned with local needs.

Finally, realizing the full potential of Juiz de Fora's regulatory framework and sandbox will require a continued commitment to regulatory adaptability and monitoring the social and environmental impacts of tested innovations. The Innovation Law and its regulations lay the foundations for a city that reconciles technological advances and social justice. However, success will depend on continuously improving these mechanisms and ensuring innovation serves inclusive and sustainable urban development.

References

ABNT NBR ISO 37122:2021. Cidades e comunidades sustentáveis – Indicadores para cidades inteligentes. Associação Brasileira de Normas Técnicas, 2021.

AGAR, Jon. The Government Machine: a Revolutionary History of the Computer. Cambridge, MA: MIT Press, 2003. viii + 554 pp. ISBN: 0-262-01202-2.

AMATO, Lucas Fucci; MISSAGIA, Caio Rezende. Ambientes regulatórios experimentais: O sandbox no sistema financeiro brasileiro. RBSD – Revista Brasileira de Sociologia do Direito, vol. 10, no. 3, pp. 143-171, September/December 2023.

ANTONIELLI, Dennys Marcelo; KIRA, Beatriz. Planejamento Urbano do Futuro, Dados do Presente: A Proteção da Privacidade no Contexto das Cidades Inteligentes. Revista Brasileira de Estudos Urbanos e Regionais (RBEUR), vol. 22, e202003, 2020. DOI: https://doi.org/10.22296/2317-1529.rbeur.202003.

DUARTE, Fábio; FIRMINO, Rodrigo José. *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, vol. 12, no. 3, pp. 303-320, 2008. DOI: 10.1080/13604810802479126.

JUIZ DE FORA. Lei nº 14.746, de 04 de dezembro de 2023. Establishes Juiz de Fora's Innovation System; defines the municipality's development hubs; provides for the responsibilities of the Municipal Council for Development, Technology and Innovation (Comdeti), and other measures. Diário Oficial do Município de Juiz de Fora, Juiz de Fora, MG, December 05, 2023.

JUIZ DE FORA. Decreto nº 16.372, de 30 de janeiro de 2024. Regulates Articles 39, 40, and 41 of Municipal Law No. 14.746 of December 04, 2023, concerning the composition and

responsibilities of the Municipal Council for Development, Technology and Innovation (COMDETI), and other measures. Diário Oficial do Município de Juiz de Fora, Juiz de Fora, MG, January 31, 2024.

JUIZ DE FORA. Decreto nº 16.448, de 11 de março de 2024. Regulates Articles 1, 2 (I), and 6 of Municipal Law No. 14.746 of December 04, 2023, concerning the creation, composition, and purposes of Juiz de Fora's Municipal Innovation System. Diário Oficial do Município de Juiz de Fora, Juiz de Fora, MG, March 12, 2024.

JUIZ DE FORA. Decreto nº 16.734, de 11 de setembro de 2024. Provides for the municipality's innovation system and other measures. Diário Oficial do Município de Juiz de Fora, Juiz de Fora, MG, September 12, 2024.

MINISTÉRIO DO DESENVOLVIMENTO REGIONAL. Carta Brasileira para Cidades Inteligentes. Brasília, 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. A cidade inteligente: tecnologias urbanas e democracia. Translated by Humberto do Amaral. São Paulo: Ubu Editora, 2019. 192 pp. ISBN: 978-85-7126-046-7.

OCDE. Smart Cities and Inclusive Growth. 2020. Available at: 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. Sandbox regulatório: instrumento experimentalista à disposição da Administração Pública local como suporte ao desenvolvimento econômico. R. de Dir. Público da Economia – RDPE, Belo Horizonte, vol. 21, no. 84, pp. 9-33, October/December 2023.

REIA, Jess; BELLI, Luca (eds.). Smart Cities no Brasil: Regulação, Tecnologia e Direitos. Belo Horizonte, MG: Casa do Direito, 2021. ISBN: 978-85-9530-274-7.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

13

From Legal Certainty to Technical Security: Topics for Decoding Technological Advances in Electronic Real Estate Registration

LUÍS HENRIQUE DE MENEZES ACIOLY

Contents: Introduction. 1. Development of Electronic Real Estate Registration in the Brazilian Legal Context. 2. First decoder: Electronic signatures and digital acts involving real estate in the public registry. 2.1. Electronic signatures: definition and relationship with the Brazilian legal system. 2.2. Acceptance of electronic signatures by the Real Estate Registry. 3. Second decoder: Secure digital document storage and the possible use of Blockchain Technology. 3.1. Blockchain: conceptual elements and applications. 3.2. Applicability of Blockchain to the Trusted Repository of Electronic Documents. Final Considerations.

Introduction

In the regulatory environment for new technologies, regulatory measures can be seen targeting new tools and changing social dynamics, as with the Internet of Things (IoT), the platformization of services, and generative artificial intelligence. However, technological evolution also affects sectors whose rules have been extensively systematized, raising questions about how to reconcile existing rules with the current context.

Professor Lyria Bennett Moses[2] expresses this concern clearly. In her view, technology-related regulation also involves the problem of regulatory disconnection: when new techniques emerge within a regulated space, they change the nature of the activity itself, creating a need to adapt the rules. This is the case with the real estate market and real estate registration.

Extrajudicial registry offices and the property folio system are vital to legal certainty and public notice of property rights, contributing to social peace. As such, they too have entered the digital age. This creates the challenge of making legal certainty—the objective of real estate registration—compatible with technical security in using new technologies.

Two topics therefore help decode technological advances in real estate registration: the acceptance of different types of electronic

1. Postgraduate student in Digital Law (Specialization) at the Instituto de Tecnologia e Sociedade (ITS) and UERJ's Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). Law graduate of Centro Universitário Ruy Barbosa – UniRuy. Research Coordinator of the Grupo de Estudos em Tecnologia, Informação e Sociedade – GETIS/CNPq. Attorney. Contact: 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, vol. 5, no. 1, pp. 1-20, 2013.

signatures to guarantee the authenticity of born-digital documents; and security parameters for electronically archived documents, particularly in the Trusted Repository of Electronic Documents (RCDE), with blockchain as a potentially relevant supporting technology. The research problem is to define the technical and legal requirements of authenticity and the points of convergence between electronic real estate registration and Blockchain.

This study therefore seeks to outline the current legal landscape of real estate registration's entry into the digital environment, emphasizing the Electronic Real Estate Registration System (SREI) through the topics that serve to decode these developments. This requires understanding the SREI's evolution, electronic signatures for acts involving real estate in public registries, and Blockchain's technical framework. The research combines two lines of reasoning: analyzing the first decoder through the existing regulatory structure and evaluating the second through its convergence with technological possibilities, namely Blockchain.

Methodologically, a critical review of the relevant literature informed descriptive, qualitative, exploratory bibliographic and documentary research emphasizing dialogue among authors from different social science fields. The literature review drew on books, dissertations, and articles in electronic databases—Scientific Electronic Library Online (Scielo), Index Law Journals, and Google Scholar—using the descriptors "electronic signature," "electronic registration," "electronic real estate registration system," "blockchain," and "smart contracts."

1. Development of Electronic Real Estate Registration in the Brazilian Legal Context

Unlike other activities, in which regulation follows development, Brazilian real estate registration has largely developed through regulatory advances responding to continual improvements in legal and archival techniques. This was the case with Federal Law No. 6.015 of 1973, which established the property folio system and gave the individual property record a central place in registration activity.[3]

3. RIBEIRO, Moacyr Petrocelli de Ávila. A Matrícula: Paradigmas para o Sistema do Registro Eletrônico de Imóveis. Revista de Direito Imobiliário, year 42, vol. 86, pp. 215-262, January/June 2019.

This technical and legal improvement responded to the transcription system, which, as Fioranelli[4] notes, required the registered property's description to be repeated each time ownership was transferred or the property was otherwise encumbered. Under the property record system, each property acquired a consolidated record containing its entire chain of title[5] and actual circumstances, with due attention to its objective identification and structural changes.[6]

The system's efficiency and effectiveness supported the expansion of real estate registration, giving registrars a leading role in protecting property rights through the quality of information linked to the property record.[7] In today's hyperinformation society,[8] however, the Internet has assumed a leading role in social relations, bringing cultural, economic, legal, and governmental changes.[9]

Without overlooking the depth of the subject of "Government as a Platform,"[10] the reshaping of public service delivery through the Internet has also reached real estate registration, particularly through Federal Law No. 11.977 of 2009. It made it possible to receive and issue electronic documents, provided the requirements of the Brazilian Public Key Infrastructure—ICP Brasil—and the e-PING architecture were observed.

Federal Law No. 11.977 of 2009 also established a duty for public registry services to institute an "electronic registration system" under specific regulations. Following this approach, the National Council of Justice issued Recommendation No. 14 of 2014 to guide the Inspectorates-General of Justice of the respective federative units

4. FIORANELLI, Ademar. Matrícula no registro de imóveis: questões práticas. In: YOSHIDA, Consuelo Yatsuda Moromizato Yoshida; FIGUEIREDO, Marcelo. AMADEI, Vicente de Abreu (coordinators). Direito notarial e registral avançado. São Paulo: Revista dos Tribunais, 2014.

5. CASTRO, Manuella Santos. Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro. 2021, 306 leaves. Doctoral dissertation – Faculdade de Direito, USP, São Paulo, 2021.

6. RIBEIRO, Moacyr Petrocelli de Ávila. A Matrícula: Paradigmas para o Sistema do Registro Eletrônico de Imóveis. Revista de Direito Imobiliário, year 42, vol. 86, pp. 215-262, January/June 2019.

7. RIBEIRO, Moacyr Petrocelli de Ávila. A Matrícula: Paradigmas para o Sistema do Registro Eletrônico de Imóveis. Revista de Direito Imobiliário, year 42, vol. 86, pp. 215-262, January/June 2019.

8. MADALENA, Juliano. Regulação das Fronteiras da Internet: um primeiro passo para uma Teoria Geral do Direito Digital. In: MARTINS, G. M.; LONGHI, J. V. R. (coordinators). Direito Digital: Direito Privado e Internet. 2nd edition. Indaiatuba: Foco, 2019. pp. 183-206.

9. CASTELLS, Manuel. A sociedade em rede. Translated by Roneide Venâncio Majer. 6th edition. São Paulo: Paz e Terra, 2002.

10. As Faleiros Júnior explains, the theory of "Government as a Platform" is grounded in a study by O'Reilly and refers to the "state's duty to encourage technological infrastructure that facilitates interaction among different actors for various purposes" (FALEIROS JÚNIOR, José Luiz de Moura. Inovação, desenvolvimento e a Lei do Governo Digital (Lei nº 14.129/2021): perspectivas quanto às estruturas de governo como plataforma. Inova Jur - Revista Jurídica da UEMG, Belo Horizonte, vol. 1, no. 1, pp. 1-29, January/June 2022, p. 6; O'REILLY, Tim. Government as platform. Innovations: Technology, Governance, Globalization, Cambridge, vol. 6, no. 1, pp. 13-40, 2011).

in implementing an “electronic real estate registration system.”[11] Recommendation No. 14 of 2014 required the parameters defined by the Associação do Laboratório de Sistemas Integráveis Tecnológicos to be observed when implementing the system, without providing further definitions.[12]

However, São Paulo’s Inspectorate-General of Justice (CGJ-SP) had already, in 2012, issued Administrative Order No. 42, providing guidelines for implementing the Electronic Real Estate Registration System (SREI) in that state. It established the Real Estate Registrars’ Shared Electronic Services Center as an Internet access point for real estate registration services.[13-14] Under this rule, the Associação de Registradores Imobiliários de São Paulo (ARISP) would develop, operate, and administer the SREI in São Paulo.[15-16]

Shortly thereafter, the National Council of Justice issued Administrative Order No. 47 of 2015, setting technical and legal guidelines for implementing the Electronic Real Estate Registration System (SREI) in each state and the Federal District.[17] The rule promoted shared electronic service centers administered locally under regulatory acts issued by each Inspectorate-General of Justice.[18] CNJ Administrative Order No. 47 of 2015 required uniform electronic centers in each of the

11. GRUBER, Rafael Ricardo. Registro Eletrônico de Imóveis, Cadastros e SINTER: Interconexão sem Submissão. Revista de Direito Imobiliário, year 39, vol. 81, pp. 253-287, July/December 2016. CASTRO, Manuella Santos. Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro. 2021, 306 leaves. Doctoral dissertation – Faculdade de Direito, USP, São Paulo, 2021.

12. ASSAD, Frederico Jorge Vaz de Figueiredo. Registro de imóveis eletrônico e governança fundiária. Revista de Direito Imobiliário, year 39, vol. 81, pp. 215-234, July/December 2016. TAVARES, Ramos André. O Operador Nacional do Sistema de Registro Eletrônico de Imóveis: Resposta à Exigência Constitucional de um Eficiente Sistema Registral. Jornal Eletrônico Migalhas, vol. 136, pp. 23-42, 2018.

13. Under this rule, the Registrars’ Center was to offer the following modules: I – Electronic Official Correspondence; II – Electronic Attachment of Real Estate (Online Attachment); III – Digital Certificate; IV – Online Property Folio; V – Electronic Search; VI – Electronic Filing of Instruments (e-Protocolo); VII – Trusted Repository of Electronic Documents (RCDE); VIII – Online Registration Tracking; IX – Registration Monitor; X – Online Inspection (monitoring, control, and oversight); and XI – Urban Land Regularization Register. This structure was maintained in the Shared Electronic Service (SAEC), with the appropriate improvements and additions, forming the backbone of the entire Electronic Real Estate Registry’s “front end.”

14. ASSAD, Frederico Jorge Vaz de Figueiredo. Registro de imóveis eletrônico e governança fundiária. Revista de Direito Imobiliário, year 39, vol. 81, pp. 215-234, July/December 2016. CASTRO, Manuella Santos. Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro. 2021, 306 leaves. Doctoral dissertation – Faculdade de Direito, USP, São Paulo, 2021.

15. Verbatim: “258. The Electronic Real Estate Registration Service (SREI) shall be provided to external users through a single Internet platform operating on the Electronic Portal of the Real Estate Registrars’ Shared Electronic Services Center (Real Estate Registrars’ Center), developed, operated, and administered by the Associação dos Registradores Imobiliários de São Paulo (ARISP) (...).”

16. ASSAD, Frederico Jorge Vaz de Figueiredo. Registro de imóveis eletrônico e governança fundiária. Revista de Direito Imobiliário, year 39, vol. 81, pp. 215-234, July/December 2016. CASTRO, Manuella Santos. Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro. 2021, 306 leaves. Doctoral dissertation – Faculdade de Direito, USP, São Paulo, 2021.

17. GRUBER, Rafael Ricardo. Registro Eletrônico de Imóveis, Cadastros e SINTER: Interconexão sem Submissão. Revista de Direito Imobiliário, year 39, vol. 81, pp. 253-287, July/December 2016.

18. Verbatim: “Art. 3. The exchange of electronic documents and information among real estate registry offices, the judiciary, public administration, and the general public shall be handled by shared electronic service centers to be established in each state and the Federal District. § 1. The respective real estate registrars shall create the shared electronic service centers pursuant to a regulatory act of the local Inspectorate-General of Justice.”

states and the Federal District, also requiring coordination among them to standardize registration services.[19]

The proliferation of state electronic service centers was countered by the need for a universal Internet access point and interoperability across the technical layers involved in nationwide real estate registration services. Together with the need to make land regularization policy effective, this led Federal Law No. 14.365 of 2017 to establish the National Operator of the Electronic Real Estate Registration System (ONR) as the body responsible for implementing and operating the SREI nationwide.[20]

The law provided the general structure for the ONR's formation,[21] financial support,[22] and regulation.[23] It was to be established as a private entity with mandatory affiliation for all real estate registrars.[24] It therefore does not form part of the federal public administration but has a sui generis legal nature.[25] The CNJ's General Inspectorate issued Administrative Order No. 89 of 2019, setting specific guidelines for the ONR's statutory purposes and operations and assigning it the implementation and operation of the Shared Electronic Service (SAEC).[26]

Under CNJ Administrative Order No. 89, the SREI comprises: (i) all real estate registrars in Brazil; (ii) the Shared Electronic Service (SAEC); and (iii) the shared electronic service centers. Gradually, state centers lost prominence relative to the SAEC, which brought together a broad range of real estate registration activities and integrated extrajudicial registry offices nationwide through a single Internet access point.[27]

19. Verbatim: "Art. 3 (...). § 2. There shall be a single shared electronic service center in each state and the Federal District. (...) § 5. The shared electronic service centers shall coordinate with one another to universalize access to electronic communication and provide the same services throughout the country."

20. TAVARES, Ramos André. O Operador Nacional do Sistema de Registro Eletrônico de Imóveis: Resposta à Exigência Constitucional de um Eficiente Sistema Registral. Jornal Eletrônico Migalhas, vol. 136, pp. 23-42, 2018.

21. Verbatim: "Art. 76. (...) 2. The ONR shall be organized as a nonprofit legal entity governed by private law."

22. Verbatim: "Art. 76 (...) § 9. A fund is hereby created for implementing and financing the SREI, to be managed by the ONR and funded by the state and Federal District real estate registration service units referred to in § 5 of this article."

23. Verbatim: "Art. 76. (...) § 4. The National Inspectorate of Justice of the National Council of Justice shall act as the ONR's regulator and ensure compliance with its bylaws."

24. Verbatim: "Art. 76. (...) § 5. The state and Federal District real estate registration service units shall form part of the SREI and be affiliated with the ONR."

25. CASTRO, Manuella Santos. Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro. 2021, 306 leaves. Doctoral dissertation – Faculdade de Direito, USP, São Paulo, 2021.

26. CASTRO, Manuella Santos. Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro. 2021, 306 leaves. Doctoral dissertation – Faculdade de Direito, USP, São Paulo, 2021.

27. VALERIO, Alexandre Scigliano; BONFATTI, Fabio Fernandes Neves. Possibilidade de Assinatura, Registro e Protesto Eletrônico dos Títulos de Crédito do Agronegócio. Revista Brasileira de Direito Empresarial, vol. 7, no. 2, pp. 17-38, July/December 2021.

Integrating all real estate registry offices into the SAEC[28] and prioritizing it over fragmented state centers reshaped the SREI. It encouraged essentially digital acts, such as issuing electronic certificates and receiving born-digital documents, linking a complex network of real estate registrars in a technological advance.[29] These converging efforts to promote electronic extrajudicial services were consolidated by Federal Law No. 14.382 of 2022, which addressed the Electronic Public Registry System (SERP), seeking to integrate other public registry offices through governance arrangements similar to those coordinating the SREI.[30]

Like the SREI for real estate registration, the SERP seeks to build an electronic system enabling interoperability and interconnection among registry office databases and universal user service through Internet-based technological structures. Technical parameters grounded in a solid regulatory framework are therefore essential to a secure environment for electronic real estate registration's development.

2. **First decoder**: Electronic signatures and digital acts involving real estate in the public registry

The validity of electronic registration depends on guaranteeing the authenticity of the people whose declarations of intent are documented. Electronic signatures are therefore a pillar of registry offices' digital age. Users' electronic filing of documents with extrajudicial services depends on compliance with specific technical and legal rules. The development of this regulatory framework, in turn, measures how smoothly reducing bureaucracy and ensuring security interact in the real estate market.

28. The integration of all real estate registry offices into the SAEC was regulated by the CNJ's National Inspectorate through Administrative Order No. 124 of 2021, which set February 15, 2022, as the deadline for completing the process.

29. MIRANDA, Caleb Matheus Ribeiro de. Comentários ao Sistema Eletrônico de Registros Públicos (SERP) – artigos 1º ao 9º. In: KÜMPEL, Vitor (coordinator). Breves comentários à Lei nª 14.382/2022. 2nd edition. São Paulo: YK, 2023, pp. 11-48.

30. Federal Law No. 14.382 of 2022 required a national operator to be established as a private entity administered by registrars under CNJ regulations. Through Administrative Order No. 139 of 2024, the CNJ created the National Operator of the Electronic Public Registry System (ONSERP), comprising the National Operator of the Civil Registry of Natural Persons (ON-RCPN), the National Operator of the Registry of Instruments and Documents and Civil Registry of Legal Persons (ON-RTDPJ), also created by that rule, and the ONR. The guidelines of Administrative Order No. 139 were incorporated into CNJ Administrative Order No. 149 of 2023. Article 212, § 2, of the latter consolidated the shared management structure: "Management of the ONSERP shall be the responsibility of the Executive Management Committee, comprising the presidents of the national public registry operators, which shall operate under the guidance and supervision of the National Inspectorate of Justice."

2.1 **Electronic signatures**: definition and relationship with the Brazilian legal system

Electronic contracts are not a new type of agreement but a particular way of concluding one, using information technology to create the document.[31] However, an electronic document's technical validity requires several elements: (i) authenticity, guaranteeing that its originator is who they claim to be; (ii) integrity, guaranteeing that the received document is identical to the original; (iii) confidentiality, guaranteeing that no unauthorized person can access its content; and (iv) non-repudiation, meaning the issuer cannot deny having produced it.[32]

In this context, electronic signatures[33] provide authenticity and integrity, while non-repudiation follows from a legal presumption validating the act according to the required signature level.[34] Brazil's legal system accepted electronic signatures through Provisional Measure No. 2.200-2 of 2001, incorporating guidelines from the Model Law of the United Nations Commission on International Trade Law—UNCITRAL.[35]

The UNCITRAL Model Law establishes two parties necessary for public-key identification: (i) the signatory, responsible for creating the electronic signature; and (ii) the relying party, responsible for verifying and deciding whether to accept that

31. MENKE, Fabiano. A forma dos contratos eletrônicos. Revista de Direito Civil Contemporâneo, São Paulo: Revista dos Tribunais, year 8, vol. 26, pp. 85-113, January/March 2021.

32. PINHEIRO, Patrícia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. Fundamentos dos Negócios e Contratos Digitais. 2nd edition. São Paulo: Revista dos Tribunais, 2021. SOTTANO, Augusto; LAGO, Ivan Jacopetti. As assinaturas eletrônicas e o registro de imóveis: estado atual da questão. In: GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; BRANDELLI, Leonardo (eds.). Direito Registral e Novas Tecnologias. Rio de Janeiro: Forense, 2021.

33. An electronic signature is understood as a mathematical digest calculated computationally using asymmetric-key technology. In asymmetric-key cryptography, a pair of keys works together: one encrypts and the other decrypts. The private key remains under the signatory's exclusive control, knowledge, and use, while the public key is freely distributed. Hashing transforms data of any size into a fixed-size block, so changing any information in the original document yields a completely different hash. The signer sends the original document and its hash encrypted with the private key. The recipient uses the public key to decrypt the hash, calculates the document's hash, and compares the two hashes. If they match, the electronic signature is valid, establishing the digital document's authenticity. This procedure authenticates the signature and ensures the born-digital document's integrity. An additional security layer can then be provided through a digital certificate verified by a Certification Authority, which attaches a Digital Certificate (PINHEIRO, Patrícia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. Fundamentos dos Negócios e Contratos Digitais. 2nd edition. São Paulo: Revista dos Tribunais, 2021).

34. LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. Revista de Processo, São Paulo: Revista dos Tribunais, year 48, vol. 345, pp. 79-121, November 2023.

35. MENKE, Fabiano. A forma dos contratos eletrônicos. Revista de Direito Civil Contemporâneo, São Paulo: Revista dos Tribunais, year 8, vol. 26, pp. 85-113, January/March 2021. SOTTANO, Augusto; LAGO, Ivan Jacopetti. As assinaturas eletrônicas e o registro de imóveis: estado atual da questão. In: GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; BRANDELLI, Leonardo (eds.). Direito Registral e Novas Tecnologias. Rio de Janeiro: Forense, 2021. LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. Revista de Processo, São Paulo: Revista dos Tribunais, year 48, vol. 345, pp. 79-121, November 2023.

signature. The rule also described an optional third party responsible for certifying the signature holder, who may or may not be a public agent: a "certification authority" or "certification services provider."[36]

In incorporating the UNCITRAL Model Law, Provisional Measure No. 2200-2 of 2001 provided for two coexisting models for recognizing signatures' validity.[37] The first, involving three parties,[38] concerns the Brazilian Public Key Infrastructure (ICP-Brasil), with the Instituto Nacional de Tecnologia da Informação (ITI) acting as Root Certification Authority. The second model,[39] involving only two parties, concerns certificates issued outside the Brazilian Public Key Infrastructure.[40]

However, the range of possibilities under this provision created doubts and uncertainty for citizens using electronic signatures, particularly when submitting electronic documents to public authorities.[41] Addressing this gap, Federal Law No. 14.063 of 2020 consolidated three types of electronic signature: (i) simple;[42] (ii) advanced;[43] and (iii) qualified.[44]

36. SOTTANO, Augusto; LAGO, Ivan Jacopetti. As assinaturas eletrônicas e o registro de imóveis: estado atual da questão. In: GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; BRANDELLI, Leonardo (eds.). Direito Registral e Novas Tecnologias. Rio de Janeiro: Forense, 2021.

37. ALVIM, Arruda; CUNHA, Igor Martins da. As assinaturas eletrônicas no ordenamento jurídico brasileiro e a relevância da autonomia privada: uma breve análise da validade dos documentos eletrônicos à luz da MP 2.200-2/2001 e da Lei 14.063/2020. Revista de Processo, São Paulo: Revista dos Tribunais, year 48, vol. 337, pp. 83-114, São Paulo: RT, March 2023.

38. Verbatim: "Art. 10. The electronic documents addressed by this Provisional Measure shall be considered public or private documents for all legal purposes. § 1. Statements contained in electronic documents produced using a certification process provided by ICP-Brasil shall be presumed true in relation to the signatories, pursuant to Article 131 of Law No. 3.071 of January 1, 1916—the Civil Code."

39. Verbatim: "Art. 10. (...) § 2. This Provisional Measure does not preclude other means of proving authorship and integrity of electronic documents, including certificates not issued by ICP-Brasil, provided they are recognized as valid by the parties or accepted by the person against whom the document is invoked."

40. PINHEIRO, Patrícia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. Fundamentos dos Negócios e Contratos Digitais. 2nd edition. São Paulo: Revista dos Tribunais, 2021.

41. ALVIM, Arruda; CUNHA, Igor Martins da. As assinaturas eletrônicas no ordenamento jurídico brasileiro e a relevância da autonomia privada: uma breve análise da validade dos documentos eletrônicos à luz da MP 2.200-2/2001 e da Lei 14.063/2020. Revista de Processo, São Paulo: Revista dos Tribunais, year 48, vol. 337, pp. 83-114, São Paulo: RT, March 2023. LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. Revista de Processo, São Paulo: Revista dos Tribunais, year 48, vol. 345, pp. 79-121, November 2023.

42. Verbatim: "Art. 4. For the purposes of this Law, electronic signatures are classified as follows: I – simple electronic signature: a) one that identifies its signatory; b) one that attaches or associates data with other electronic data of the signatory."

43. Verbatim: "Art. 4. (...) II – advanced electronic signature: one using certificates not issued by ICP-Brasil or other means of proving authorship and integrity of electronic documents, provided it is recognized as valid by the parties or accepted by the person against whom the document is invoked, with the following characteristics: a) it is uniquely linked to the signatory; b) it uses electronic signature creation data that the signatory can operate under their exclusive control with a high level of confidence; c) it is linked to the associated data so that any subsequent modification is detectable."

44. Verbatim: "Art. 4. (...) III – qualified electronic signature: one using a digital certificate pursuant to § 1 of Article 10 of Provisional Measure No. 2.200-2 of August 24, 2001."

2.2 Acceptance of electronic signatures by the Real Estate Registry

In regulating when public authorities could accept signatures based on certificates outside ICP-Brasil, Federal Law No. 14.063 of 2020 also specified when that infrastructure would be required.[45] It required qualified signatures for real estate transfers and registrations, subject to statutory exceptions.[46-47] Federal Law No. 14.382 of 2022 revised this by amending the Public Registries Law to permit advanced signatures in public registry acts involving real estate, subject to CNJ National Inspectorate regulations.[48-49]

The restriction imposed by Federal Law No. 14.063 of 2020 is overcome not only because its provisions are incompatible with Federal Law No. 14.382 of 2022, but also, particularly, through the rule for resolving apparent conflicts between norms of equal hierarchical status. Under this rule, a later norm implicitly repeals an incompatible earlier one, as provided by the Introductory Law to the Norms of Brazilian Law (Decree-Law No. 4.657 of 1942).[50]

Accordingly, the CNJ's National Inspectorate introduced extensive regulations on electronic signatures under the responsibility of the National Operator of the Civil Registry of Natural Persons (ON-RCPN), through Administrative Order No. 157 of 2023. It amended the National Code of Rules for Extrajudicial Services to include: (i) the Electronic Authentication System using biographical and biometric data to identify internal users

45. ALVIM, Arruda; CUNHA, Igor Martins da. As assinaturas eletrônicas no ordenamento jurídico brasileiro e a relevância da autonomia privada: uma breve análise da validade dos documentos eletrônicos à luz da MP 2.200-2/2001 e da Lei 14.063/2020. Revista de Processo, São Paulo: Revista dos Tribunais, year 48, vol. 337, pp. 83-114, São Paulo: RT, March 2023.

46. The exceptions in Federal Law No. 14.063 of 2020 concerned registration of acts with commercial registries (Article 5, § 1, II, "c") and acts performed by financial institutions providing real estate credit that are authorized to execute private instruments having the status of public deeds (Article 17-A).

47. SOTTANO, Augusto; LAGO, Ivan Jacopetti. As assinaturas eletrônicas e o registro de imóveis: estado atual da questão. In: GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; BRANDELLI, Leonardo (eds.). Direito Registral e Novas Tecnologias. Rio de Janeiro: Forense, 2021.

48. Verbatim: "Art. 17. Anyone may request a registry certificate without informing the registrar or employee of the reason for or interest in the request. § 1. Information accessed from or sent to public registries through the Internet must be signed using an advanced or qualified signature under Article 4 of Law No. 14.063 of September 23, 2020, pursuant to the terms established by the National Inspectorate of Justice of the National Council of Justice. § 2. An act of the National Inspectorate of Justice of the National Council of Justice may establish circumstances in which advanced signatures may be used in acts involving real estate."

49. LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. Revista de Processo, São Paulo: Revista dos Tribunais, year 48, vol. 345, pp. 79-121, November 2023.

50. Verbatim: "Art. 2. Unless intended to operate temporarily, a law shall remain in force until another law amends or repeals it. § 1. A later law repeals an earlier one when it expressly declares so, is incompatible with it, or entirely regulates the subject addressed by the earlier law."

and external users across all SERP registry branches;[51] and (ii) a Civil Registry Public Key Infrastructure (ICP-RC), based on advanced electronic signatures.[52]

A Brazilian Civil Registry Trusted Electronic Services List (LSEC-RCPN)[53] was consolidated, including the ICP-RC. It recognizes the validity of advanced electronic signatures for acts concerning electronic documents submitted to public registry services, acts involving real estate, and private instruments having the status of public deeds executed by financial institutions providing real estate credit.

However, filing documents with the Real Estate Registry and conducting specific registration procedures[54] may depend on statutory formalities. Where a public deed is required,[55] a civil-law notary's involvement is indispensable. Electronic notarial acts are subject to specific guidelines validating documents signed using a notarized certificate—a type of advanced signature—or ICP-Brasil certification for the other signatories.[56]

Reducing bureaucracy in real estate registration by accepting electronic signatures based on digital certificates outside ICP-Brasil ultimately encourages wider use of extrajudicial services.[57] This stems from the lower cost of non-ICP-Brasil digital certificates and the greater

51. Verbatim: "Art. 228-C. The IdRC shall be considered valid for user identification and authentication across all Serp platforms and services, including the other registry branches (...)."

52. Verbatim: "Art. 228-E. The ICP-RC shall manage the life cycle of public keys for advanced electronic signatures pursuant to Article 38 of Law No. 11.977 of July 7, 2009, and Article 4, II, of Law No. 14.063 of September 23, 2020. § 1. The ICP-RC does not form part of ICP-Brasil's hierarchical chain."

53. Verbatim: "Art. 228-F. The LSEC-RCPN shall contain data describing the services accepted as trusted by the ON-RCPN. (...) § 3. The ICP-RC forms part of the LSEC-RCPN. § 4. Electronic signatures whose roots are registered in the LSEC-RCPN may validly be used for the acts described in Article 38 of Law No. 11.977 of July 7, 2009, Article 17 of Law No. 6.015 of December 31, 1973, and Article 17-A of Law No. 14.063 of July 14, 2023."

54. In addition to registering the documents listed in Article 167, I, of Federal Law No. 6.015 of 1973, there are the annotations listed in II of the same article and special procedures such as adverse possession (Article 216-A), correction of a property's area (Article 213), and notice to regularize payments under a purchase and sale commitment (Article 251-A).

55. Under Article 108 of the Civil Code, acts intended to establish, transfer, modify, or waive property rights over real estate valued at more than thirty times the highest minimum wage in the country must be executed by public deed. However, this rule is relaxed for transactions conducted by entities linked to the Housing Finance System (SFH), pursuant to Article 61 of Federal Law No. 4.380 of 1964, and the Real Estate Finance System (SFI), pursuant to Article 38 of Federal Law No. 9.514 of 1997.

56. ALVARES, Luís Ramon. O Papel dos Cartórios Extrajudiciais na Dinâmica da Desjudicialização no Brasil. 2022, 61 leaves. Master's dissertation – Programa de Pós-graduação em Direito, Curso de Mestrado Profissional, Universidade de Araraquara (UNIARA), Araraquara, 2022.

57. FARIA, Bianca Castellar de; LACERDA, Naurican Ludovico. A eficiência do Registro Imobiliário brasileiro e os impactos da Medida Provisória 1.085/2021. *In*: FIUZA, César Augusto de Castro; MARTOS, Frederido Thales; BORGES, Maria Creusa de Araújo. *Direito Civil Contemporâneo*. Florianópolis: CONPEDI, 2022.

diversity of authentication factors, which provides multiple security layers and prevents obsolescence.[58]

This is a key to decoding advances in electronic real estate registration. It reduces bureaucracy while guaranteeing legal certainty grounded in a regulatory framework that recognizes the inherent reliability of this type of electronic signature under the applicable rules.

3. **Second Decoder**: Secure Digital Document Storage and the Possible Use of Blockchain Technology

A second pillar of registry offices' entry into the digital age is secure storage of born-digital documents. This involves not only preventing unauthorized access and accidental or unlawful destruction, loss, alteration, communication, or dissemination, as provided by Federal Law No. 13.709 of 2018, but also developing a specific technical framework promoting the confidentiality, integrity, and availability of registered information.[59]

These rules were developed primarily through National Council of Justice Administrative Order No. 74 of 2018, addressing extrajudicial offices divided into three classes according to revenue. There is thus a regulatory gap concerning security rules for activities within the SREI and the Trusted Repository of Electronic Documents (RCDE).

However, this approach is associated with the ONR's governance system, which is responsible for technical guidelines for implementing and coordinating the SREI.[60] The study therefore turns to the possible use of Blockchain technology to support technical security in archiving born-digital documents in the Electronic Real Estate Registry.

58. PINHEIRO, Patrícia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. Fundamentos dos Negócios e Contratos Digitais. 2nd edition. São Paulo: Revista dos Tribunais, 2021.

59. HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018.

60. The ONR is responsible for submitting "suggestions to the National Inspectorate of Justice for technical standardization instructions applicable to the SREI, enabling secure system operation, data and document interoperability, and the longevity of electronic files, as well as electronic adaptation of the legal and formal requirements of services to guarantee the authenticity and security of operations conducted with electronic documents" (Article 31, II, "d," of CNJ Administrative Order No. 89 of 2019).

3.1 **Blockchain**: Conceptual Elements and Applications

Commonly associated with “cryptocurrencies” and “Non-Fungible Tokens,” Blockchain technology represents an undeniable advance in information security and integrity, particularly in a sociotechnical context where high information flows shape society’s different dimensions.[61] Blockchain is enabled by decentralized data recording in a linked network, also called decentralized ledger technology,[62] as opposed to the centralized information recording common to data flows.

Barbosa[63] defines Blockchain as a continually growing list of blocks linked securely through cryptography in a peer-to-peer network. Faleiros Júnior and Roth[64] present Tapscott and Tapscott’s concept,[65] explaining that Blockchain relies on rules in the form of distributed calculations that ensure the integrity of data flows, maintaining a shared record in agreement across numerous validators. Depending on its configuration, each unit stores information such as credits, debits, or ownership, verified through consensus with other points.[66]

Decentralized recording relies on a ledger that receives information and replicates it across a complex network of key points,[67] without a centralized or unified record.[68] There is no hierarchy among the chain’s units or management from a central node, but rather a spatial distribution of linear convergence.[69] Each node constitutes a participant, increasing trust through

61. O’SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. North Carolina Banking Institute, vol. 21, pp. 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 e responsabilidade civil. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coordinators). Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa. Indaiatuba: Foco, 2021, pp. 797-824.

64. FALEIROS JÚNIOR, José Luiz de Moura; ROTH, Gabriela. Como a utilização do Blockchain pode afetar Institutos Jurídicos Tradicionais?. Revista Jurídica do Ministério Público Catarinense, Florianópolis, vol. 14, no. 30, pp. 39-59, June/November 2019.

65. TAPSCOTT, Don; TAPSCOTT, Alex. Blockchain Revolution: como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: SENAI-SP, 2016.

66. RASKIN, Max. The Law and Legality of Smart Contracts. Georgetown Law Technology Review, vol. 1, no. 2, pp. 305-341, 2017.

67. The idea of a complex network composed of specific units shapes the concept of Blockchain. This study therefore uses “block,” “points,” and “key points” interchangeably, since they can convey the same understanding in the context presented here.

68. BARBOSA, Mafalda Miranda. Blockchain e responsabilidade civil. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coordinators). Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa. Indaiatuba: Foco, 2021, pp. 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 the same data. Adding participants also adds validators for information recorded in the ledger.[70] Blockchain thus combines decentralized information with the need for consensus.

The literature identifies five attributes of Blockchain technology: (i) distribution, since each network member can ascertain all circulating data and their history; (ii) irreversibility, since records cannot be altered and remain immutably linked to every previously recorded transaction; (iii) peer-to-peer operation, allowing direct interaction among key points without an intermediary; (iv) programmed logic, through processing based on computer code; and (v) transparency, since each block is available to any network member even when data are anonymized.[71] Irreversibility enables the authenticity of ledger contents because of the technical cost of modifying them.[72]

In relational terms, Blockchain is associated with transactions that attach a hash to the information concerned, with each key point recording the data flow by reference to the preceding point.[73] Synchronization between information recorded at preceding and subsequent points maintains data integrity and enables the transaction.[74] For cryptoassets specifically, linked blocks record each transaction's date and time alongside the associated ownership, consolidating a chain of ownership.[75]

Information in the ledger is validated through the convergence and consensus of all key points in the chain, rather than through a centralized ledger held by a trusted intermediary, as in banking transactions.[76] This means that, for an unauthorized

70. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. North Carolina Banking Institute, vol. 21, pp. 177-194, 2017.

71. CHITTENDEN, Tara. Blockchain: The Legal Implications of Distribuited Systems. The Law Society: London, 2017. BARBOSA, Mafalda Miranda. Blockchain e responsabilidade civil. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coordinators). Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa. Indaiatuba: Foco, 2021, pp. 797-824.

72. NALIN, Paulo; NAGAROLI, Rafaella. Inteligência artificial, blockchain e smart contracts: breves reflexões sobre o novo desenho jurídico do contrato na sociedade da informação. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coordinators). Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa. Indaiatuba: Foco, 2021, pp. 753-773.

73. DIVINO, Sthéfano Bruno Santos. Smart Contracts: Conceitos, Limitações, Aplicabilidade e Desafios. Revista Jurídico Luso-Brasileira, year 4, no. 6, pp. 2771-2808, November/December 2018.

74. WRIGHT, Aaron; DE FILIPPI, Primavera. Decentralized Blockchain Technology and the Rise of Lex Cryptographia, SSRN, March 10, 2015. CANTALI, Rodrigo Ustárroz. Smart Contracts e Direito Contratual: Primeiras Impressões sobre suas Vantagens e Limites. Revista Jurídico Luso-Brasileira, year 8, no. 3, pp. 1529-1599, May/June 2022.

75. RASKIN, Max. The Law and Legality of Smart Contracts. Georgetown Law Technology Review, vol. 1, no. 2, pp. 305-341, 2017.

76. 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.

modification to occur, the action must be coordinated across all blocks simultaneously, making the procedure more difficult.[77]

This picture expands when public and private Blockchains are distinguished. In a public blockchain, any user may join without permission, becoming part of the validation network and contributing to convergence.[78] This model, also known as permissionless Blockchain, allows user anonymity and leaves the number of key points undefined.[79] A private blockchain, in turn, predetermines who may join, the number of users, and who may contribute to consensus.[80] In this system, described by Zetzsche et al.[81] as permissioned, there is no anonymity: each user's permissions and authenticity can be defined through a digital certificate.[82]

Applying Blockchain to "Smart Contracts" has driven their expansion by providing the technical basis for robust security in self-executing programming.[83] Smart Contracts are not a specific legal form in contract law, but a way of automatically performing an agreement's terms through computer engineering or software.[84-85] They are a computer program, written

77. GUIMARÃES, Luíza Resende; CASTRO, Maria Clara Versiani de. Afinal, smart contracts são contratos? Natureza jurídica a partir de uma leitura sociológica. In: CHAVES, N. C.; COLOMBI, H. (eds.). Direito e Tecnologia: novos modelos e tendências. Porto Alegre: Fi, 2021, pp. 36-64.

78. 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. ALEXANDRE, Marcos Gaspar. Sharing Economy e Blockchain: Problemas e Possíveis Soluções, 2018, 105 leaves. Master's dissertation in Management – Faculdade de Economia da Universidade de Coimbra, Coimbra, 2018.

79. VUKOLIC, Marko. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 9591, pp. 112-126, 2016. ALEXANDRE, Marcos Gaspar. Sharing Economy e Blockchain: Problemas e Possíveis Soluções, 2018, 105 leaves. Master's dissertation in Management – Faculdade de Economia da Universidade de Coimbra, Coimbra, 2018.

80. PILKINGTON, Marc. Blockchain Technology: Principles and Applications. In: OLLEROS, F. X.; ZHEGU, M. (eds.). Research Handbook on Digital Transformations, Cheltenham: Edward Edgar Publishing, 2016.

81. 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.

82. ALEXANDRE, Marcos Gaspar. Sharing Economy e Blockchain: Problemas e Possíveis Soluções, 2018, 105 leaves. Master's dissertation in Management – Faculdade de Economia da Universidade de Coimbra, Coimbra, 2018.

83. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. North Carolina Banking Institute, vol. 21, pp. 177-194, 2017. CANTALI, Rodrigo Ustárroz. Smart Contracts e Direito Contratual: Primeiras Impressões sobre suas Vantagens e Limites. Revista Jurídico Luso-Brasileira, year 8, no. 3, pp. 1529-1599, 2022.

84. According to Florani, Smart Contracts constitute a third phase of digital contracting. The first concerns electronic contracts, where only the medium recording the agreement changes. The second involves data-driven contracts, a hybrid of traditional agreements and automatic digital completion of information (FLORANI, Lara Bonemer Rocha. Smart contracts nos contratos empresariais: um estudo sobre possibilidade e viabilidade econômica de sua utilização. 2020. 163 leaves. Doctoral dissertation – Pontifícia Universidade Católica do Paraná, 2020).

85. CANTALI, Rodrigo Ustárroz. Smart Contracts e Direito Contratual: Primeiras Impressões sobre suas Vantagens e Limites. Revista Jurídico Luso-Brasileira, year 8, no. 3, pp. 1529-1599, May/June 2022.

in code and structured through algorithms[86] to produce a predetermined result. Nick Szabó[87] devised the concept to make contractual obligations self-executing when a triggering event occurs.[88] It responds quickly to the conditions for which the software was programmed, bringing greater rationality to transactions.

Blockchain is not essential to conceiving a Smart Contract, but it provides sufficient security for contractual obligations to be performed as previously planned.[89] Recording transactions in a decentralized ledger ensures coherent validation of data flows and prevents predetermined obligations from being changed.[90] Programming contractual obligations transforms a static ledger into a dynamic system capable of executing a contract's business logic.[91] This logic underpins cryptocurrency transactions by recording assets' incoming and outgoing flows in wallets protected through asymmetric-key cryptography.[92] The operation's inherent security meets the main demands of information flows in the digital age.

86. Although "algorithm" is readily associated with artificial intelligence systems, it is a different concept. Algorithms can be defined as sequentially organized instructions determining a command or order to be executed (MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. Revista de Direito Público, vol. 16, no. 90, pp. 39-64, November/December 2019). They are the programming of commands to be executed by a mechanical or computational entity (ACIOLY, Luis Henrique de Menezes. Reflexões sobre a Utilização da Inteligência Artificial e Algoritmos nas Relações Consumeristas à Luz da Lei Geral de Proteção de Dados. Revista Brasileira de Direito Comercial, Concorrência, Empresarial e do Consumidor. Porto Alegre: Lex Magister. vol. 48, pp. 165-187, August/September 2022). Artificial Intelligence, in turn, can be understood as the field devoted to building systems capable of exhibiting human behavior through learning (BIGONHA, Carolina. Inteligência Artificial em Perspectiva. Panorama Setorial da Internet, year 10, no. 2, pp. 1-9, July/October 2018). Within AI, the algorithm structures the logic for machine learning (ACIOLY, Luis Henrique de Menezes. Reflexões sobre a Utilização da Inteligência Artificial e Algoritmos nas Relações Consumeristas à Luz da Lei Geral de Proteção de Dados. Revista Brasileira de Direito Comercial, Concorrência, Empresarial e do Consumidor. Porto Alegre: Lex Magister. vol. 48, pp. 165-187, August/September 2022).

87. SZABO, Nick. Formalizing and Securing Relationships on Public Networks. First Monday, vol. 2, no. 9, 1997.

88. An example given by Szabó (SZABO, Nick. Formalizing and Securing Relationships on Public Networks. First Monday, vol. 2, no. 9, 1997) and discussed in the literature is a vending machine, which simply receives payment and delivers the selected product (RASKIN, Max. The Law and Legality of Smart Contracts. Georgetown Law Technology Review, vol. 1, no. 2, pp. 305-341, 2017; FLORANI, Lara Bonemer Rocha. Smart contracts nos contratos empresariais: um estudo sobre possibilidade e viabilidade econômica de sua utilização. 2020. 163 leaves. Doctoral dissertation – Pontifícia Universidade Católica do Paraná, 2020; CANTALI, Rodrigo Ustárroz. Smart Contracts e Direito Contratual: Primeiras Impressões sobre suas Vantagens e Limites. Revista Jurídico Luso-Brasileira, year 8, no. 3, pp. 1529-1599, May/June 2022).

89. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. North Carolina Banking Institute, vol. 21, pp. 177-194, 2017. ACIOLY, Luis Henrique de Menezes; OLIVEIRA, Micael Araújo de Souza. Espectro de Aplicação dos Smart Contracts à Luz do Direito Contratual Brasileiro: Breves considerações no contexto da boa-fé objetiva. Revista Conversas Civilísticas, Salvador, vol. 2, no. 2, pp. 98-121, 2022.

90. ACIOLY, Luis Henrique de Menezes; OLIVEIRA, Micael Araújo de Souza. Espectro de Aplicação dos Smart Contracts à Luz do Direito Contratual Brasileiro: Breves considerações no contexto da boa-fé objetiva. Revista Conversas Civilísticas, Salvador, vol. 2, no. 2, pp. 98-121, 2022.

91. FLORANI, Lara Bonemer Rocha. Smart contracts nos contratos empresariais: um estudo sobre possibilidade e viabilidade econômica de sua utilização. 2020. 163 leaves. Doctoral dissertation – Pontifícia Universidade Católica do Paraná, 2020.

92. NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available at: https://bitcoin.org/bitcoin.pdf. Accessed July 01, 2024; FOLLADOR, Guilherme Broto. Criptomoedas e competência tributária. Revista Brasileira de Políticas Públicas, Brasília, vol. 7, no. 3, pp. 79-104, 2017.

3.2 Trusted Repository of Electronic Documents and Digital Storage

Turning to a related issue, Blockchain's incorporation into Brazil's public sector gained prominence through Notarchain, within the e-Notariado platform for Internet delivery of notarial services, associated with National Council of Justice Administrative Order No. 100 of 2020. Developed with IBM using "Hyperledger Fabric" technology (Santos, 2022), Notarchain is a private Blockchain. It enables different access levels according to user permissions, using digital certificates to guarantee authenticity.[93] Access is restricted to previously authorized users, with key points limited to notaries.

These coherent technical parameters sustain delegated notaries' digital operations, promoting security shared by all blocks in a restricted chain of actors. The Trusted Repository of Electronic Documents (RCDE), a specific SAEC module, has a similar function: storing electronic documents—born-digital or digitized files of powers of attorney, certificates, contracts, mortgage cancellations, and public deeds—to support registration acts.[94] These files would be accessible to any Real Estate Registrar, avoiding repeated document requests when users indicate they have submitted them to the platform.

The RCDE emerged within the Shared Electronic Service as an initiative associated with Article 10 of Ministry of Cities Ordinance No. 1.248 of 2023. This concerns declarations of full payment for contracts financed by the Residential Leasing Fund (FAR) and Social Development Fund (FDS) under the National Urban Housing Program (PNHU), administered by Caixa Econômica Federal.[95] The RCDE stores these contracts' Statements of Full Payment and Powers of Attorney, facilitating registrars' access.

93. SANTOS, Gabriel Gonçalves. Smart Contracts: Conceitos, limitações e potencialidades. 2022, 138 leaves, illustrated. Master's dissertation – Universidade Federal de Minas Gerais, Faculdade de Direito, Belo Horizonte, 2022.

94. OPERADOR NACIONAL DO SISTEMA DO REGISTRO ELETRÔNICO DE IMÓVEIS - ONR. Comunicado nº 2, de 2024. Declaração de Quitação. Available at: https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN_334%5B1%5D.pdf. Accessed July 01, 2024.

95. OPERADOR NACIONAL DO SISTEMA DO REGISTRO ELETRÔNICO DE IMÓVEIS - ONR. Comunicado nº 2, de 2024. Declaração de Quitação. Available at: https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN_334%5B1%5D.pdf. Accessed July 01, 2024.

However, consolidating a means of archiving born-digital documents reframes the tool, giving it particular importance for file storage and free registrar access as broad support for electronic registration acts. A private Blockchain could therefore serve as an archiving technology combining unalterable content with validation distributed among registrars as key points in a complex chain.

Final Considerations

This article has presented issues concerning technological advances arising from the regulatory landscape. Examining the regulatory environment was necessary to understand the technical context of Electronic Real Estate Registration's development. The topics analyzed provided keys to understanding the dynamics of digital real estate registration.

Examining the Electronic Real Estate Registration System's (SREI) regulatory development showed that its design was not uniform, predictable, and systematic from its conception in Federal Law No. 11.977 of 2009. Rather, successive rules structured and shaped the activity. In its current form, the SREI has solid governance and sustainability structures enabling nationwide operations, interconnecting real estate registry offices and concentrating digital services at a single Internet access point, the Shared Electronic Service (SAEC).

The analysis then turned to the topics that decode these advances. The acceptance of electronic signatures as a means of ensuring born-digital documents' authenticity and integrity developed similarly to the SREI itself: through a complex set of rules shaping their use in public registry acts involving real estate. The predominance of qualified signatures based on the Brazilian Public Key Infrastructure has given way to the coexistence of that model and accepted advanced electronic signatures. This reduces bureaucracy and democratizes real estate registration, since advanced signature models offer diverse authentication factors while ensuring operational security.

Digital document archiving, in turn, is only lightly grounded in regulatory rules, whether because technical regulation would be inappropriate given the clear risk of legal obsolescence or because information security already has technical standards and good practices. Improving digital archiving therefore involves incorporating Blockchain technology, particularly within the Trusted Repository of Electronic Documents under the SAEC, shared by registrars and users.

Bibliographic References

ACIOLY, Luis Henrique de Menezes. Reflexões sobre a Utilização da Inteligência Artificial e Algoritmos nas Relações Consumeristas à Luz da Lei Geral de Proteção de Dados. Revista Brasileira de Direito Comercial, Concorrência, Empresarial e do Consumidor. Porto Alegre: Lex Magister. vol. 48, pp. 165-187, August/September 2022.

ACIOLY, Luis Henrique de Menezes; OLIVEIRA, Micael Araújo de Souza. Espectro de Aplicação dos Smart Contracts à Luz do Direito Contratual Brasileiro: Breves considerações no contexto da boa-fé objetiva. Revista Conversas Civilísticas, Salvador, vol. 2, no. 2, pp. 98-121, 2022.

ALEXANDRE, Marcos Gaspar. Sharing Economy e Blockchain: Problemas e Possíveis Soluções, 2018, 105 leaves. Master's dissertation in Management – Faculdade de Economia da Universidade de Coimbra, Coimbra, 2018.

ALVARES, Luís Ramon. O Papel dos Cartórios Extrajudiciais na Dinâmica da Desjudicialização no Brasil. 2022, 61 leaves. Master's dissertation – Programa de Pós-graduação em Direito, Curso de Mestrado Profissional, Universidade de Araraquara (UNIARA), Araraquara, 2022.

ALVIM, Arruda; CUNHA, Igor Martins da. As assinaturas eletrônicas no ordenamento jurídico brasileiro e a relevância da autonomia privada: uma breve análise da validade dos documentos eletrônicos à luz da MP 2.200-2/2001 e da Lei 14.063/2020. Revista de Processo, São Paulo: Revista dos Tribunais, year 48, vol. 337, pp. 83-114, São Paulo: RT, March 2023.

ASSAD, Frederico Jorge Vaz de Figueiredo. Registro de imóveis eletrônico e governança fundiária. Revista de Direito Imobiliário, year 39, vol. 81, pp. 215-234, July/December 2016.

BARBOSA, Mafalda Miranda. Blockchain e responsabilidade civil. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coordinators). Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa. Indaiatuba: Foco, 2021, pp. 797-824.

BIGONHA, Carolina. Inteligência Artificial em Perspectiva. Panorama Setorial da Internet, year 10, no. 2, pp. 1-9, July/October 2018.

CANTALI, Rodrigo Ustárroz. Smart Contracts e Direito Contratual: Primeiras Impressões sobre suas Vantagens e Limites. Revista Jurídico Luso-Brasileira, year 8, no. 3, pp. 1529-1599, May/June 2022.

CASTELLS, Manuel. A sociedade em rede. Translated by Roneide Venâncio Majer. 6th edition. São Paulo: Paz e Terra, 2002.

CASTRO, Manuella Santos. Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro. 2021, 306 leaves. Doctoral dissertation – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.

CHITTENDEN, Tara. *Blockchain*: The Legal Implications of Distribuited Systems. The Law Society: London, 2017.

DIVINO, Sthéfano Bruno Santos. Smart Contracts: Conceitos, Limitações, Aplicabilidade e Desafios. Revista Jurídico Luso-Brasileira, year 4, no. 6, pp. 2771-2808, November/December 2018.

FALEIROS JÚNIOR, José Luiz de Moura. Inovação, desenvolvimento e a Lei do Governo Digital (Lei nº 14.129/2021): perspectivas quanto às estruturas de governo como plataforma. Inova Jur – Revista Jurídica da UEMG, Belo Horizonte, vol. 1, no. 1, pp. 1-29, January/June 2022.

FALEIROS JÚNIOR, José Luiz de Moura; ROTH, Gabriela. Como a utilização do Blockchain pode afetar Institutos Jurídicos Tradicionais?. Revista Jurídica do Ministério Público Catarinense, Florianópolis, vol. 14, no. 30, pp. 39-59, June/November 2019.

FARIA, Bianca Castellar de; LACERDA, Naurican Ludovico. A eficiência do Registro Imobiliário brasileiro e os impactos da Medida Provisória 1.085/2021. In: FIUZA, César Augusto de Castro; MARTOS, Frederido Thales de Araújo; BORGES, Maria Creusa de Araújo. Direito Civil Contemporâneo. Florianópolis: CONPEDI, 2022.

FIORANELLI, Ademar. Matrícula no registro de imóveis: questões práticas. In: YOSHIDA, Consuelo Yatsuda Moromizato Yoshida; FIGUEIREDO, Marcelo. AMADEI, Vicente de Abreu (coordinators). Direito notarial e registral avançado. São Paulo: Revista dos Tribunais, 2014.

FLORANI, Lara Bonemer Rocha. Smart contracts nos contratos empresariais: um estudo sobre possibilidade e viabilidade econômica de sua utilização. 2020. 163 leaves. Doctoral dissertation – Pontifícia Universidade Católica do Paraná, 2020.

FOLLADOR, Guilherme Broto. Criptomoedas e competência tributária. Revista Brasileira de Políticas Públicas, Brasília, vol. 7, no. 3, pp. 79-104, 2017. Available at: https://www.publicacoes.uniceub.br/RBPP/article/view/4925/0. Accessed July 01, 2024.

GRUBER, Rafael Ricardo. Registro Eletrônico de Imóveis, Cadastros e SINTER: Interconexão sem Submissão. Revista de Direito Imobiliário, year 39, vol. 81, pp. 253-287, July/December 2016.

GUIMARÃES, Luíza Resende; CASTRO, Maria Clara Versiani de. Afinal, smart contracts são contratos? Natureza jurídica a partir de uma leitura sociológica. In: CHAVES, N. C.; COLOMBI, H. (eds.). Direito e Tecnologia: novos modelos e tendências. Porto Alegre: Fi, 2021, pp. 36-64.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. *Fundamentos de Segurança da Informação*: Com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018.

LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. Revista de Processo, São Paulo: Revista dos Tribunais, year 48, vol. 345, pp. 79-121, November 2023.

MADALENA, Juliano. Regulação das Fronteiras da Internet: um primeiro passo para uma Teoria Geral do Direito Digital. In: MARTINS, G. M.; LONGHI, J. V. R. (coordinators). Direito Digital: Direito Privado e Internet. 2nd edition. Indaiatuba: Foco, 2019. pp. 183-206.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. Revista de Direito Público, vol. 16, no. 90, pp. 39-64, November/December 2019.

MENKE, Fabiano. A forma dos contratos eletrônicos. Revista de Direito Civil Contemporâneo, São Paulo: Revista dos Tribunais, year 8, vol. 26, pp. 85-113, January/March 2021.

MIRANDA, Caleb Matheus Ribeiro de. Comentários ao Sistema Eletrônico de Registros Públicos (SERP) – artigos 1º ao 9º. In: KÜMPEL, Vitor (coordinator). Breves comentários à Lei nª 14.382/2022. 2nd edition. São Paulo: YK, 2023, pp. 11-48.

MOSES, Lyria Bennett. How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target. Law, Innovation and Technology, vol. 5, no. 1, pp. 1-20, 2013. Available at: http://ssrn.com/abstract=2464750. Accessed June 11, 2023.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available at: https://bitcoin.org/bitcoin.pdf. Accessed July 01, 2024.

NALIN, Paulo; NAGAROLI, Rafaella. Inteligência artificial, blockchain e smart contracts: breves reflexões sobre o novo desenho jurídico do contrato na sociedade da informação. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coordinators). Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa. Indaiatuba: Foco, 2021, pp. 753-773.

OPERADOR NACIONAL DO SISTEMA DO REGISTRO ELETRÔNICO DE IMÓVEIS - ONR. Comunicado nº 2, de 2024. Declaração de Quitação. Available at: https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN_334%5B1%5D.pdf. Accessed July 01, 2024.

O'REILLY, Tim. Government as platform. Innovations: Technology, Governance, Globalization, Cambridge, vol. 6, no. 1, pp. 13-40, 2011. Available at: https://direct.mit.edu/itgg/article/6/1/13/9649/Government-as-a-Platform. Accessed June 15, 2024.

O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. North Carolina Banking Institute, vol. 21, pp. 177-194, 2017.

PILKINGTON, Marc. Blockchain Technology: Principles and Applications. In: OLLEROS, F. X.; ZHEGU, M. (eds.). Research Handbook on Digital Transformations, Cheltenham: Edward Edgar Publishing, 2016.

PINHEIRO, Patrícia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. Fundamentos dos Negócios e Contratos Digitais. 2nd edition. São Paulo: Revista dos Tribunais, 2021.

RASKIN, Max. The Law and Legality of Smart Contracts. Georgetown Law Technology Review, vol. 1, no. 2, pp. 305-341, 2017.

RIBEIRO, Moacyr Petrocelli de Ávila. A Matrícula: Paradigmas para o Sistema do Registro Eletrônico de Imóveis. Revista de Direito Imobiliário, year 42, vol. 86, pp. 215-262, January/June 2019.

SANTOS, Gabriel Gonçalves. Smart Contracts: Conceitos, limitações e potencialidades. 2022, 138 leaves, illustrated. Master's dissertation – Universidade Federal de Minas Gerais, Faculdade de Direito, Belo Horizonte, 2022. Available at: http://hdl.handle.net/1843/57345. Accessed July 01, 2024.

SOTTANO, Augusto; LAGO, Ivan Jacopetti. As assinaturas eletrônicas e o registro de imóveis: estado atual da questão. In: GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; BRANDELLI, Leonardo (eds.). Direito Registral e Novas Tecnologias. Rio de Janeiro: Forense, 2021.

SZABO, Nick. Formalizing and Securing Relationships on Public Networks. First Monday, vol. 2, no. 9, 1997. Available at: https://doi.org/10.5210/fm.v2i9.548. Accessed July 01, 2024.

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution*: como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: SENAI-SP, 2016.

TAVARES, Ramos André. O Operador Nacional do Sistema de Registro Eletrônico de Imóveis: Resposta à Exigência Constitucional de um Eficiente Sistema Registral. Jornal Eletrônico Migalhas, vol. 136, pp. 23-42, 2018. Available at: https://www.migalhas.com.br/arquivos/2018/8/art20180821-03.pdf. Accessed July 01, 2024.

VALERIO, Alexandre Scigliano; BONFATTI, Fabio Fernandes Neves. Possibilidade de Assinatura, Registro e Protesto Eletrônico dos Títulos de Crédito do Agronegócio. Revista Brasileira de Direito Empresarial, vol. 7, no. 2, pp. 17-38, July/December 2021.

VUKOLIC, Marko. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 9591, pp. 112-126, 2016.

WRIGHT, Aaron; DE FILIPPI, Primavera. Decentralized Blockchain Technology and the Rise of Lex Cryptographia, SSRN, March 10, 2015. Available at: http://dx.doi.org/10.2139/ssrn.2580664. Accessed July 01, 2024.

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. Available at: http://dx.doi.org/10.2139/ssrn.3018214. Accessed July 01, 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

14

The Role of the Central Bank of Brazil in Regulating Payment Fintechs

VICTOR CHAME ALVIM

Contents: 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 Rules 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 innovative technology. By disrupting established paradigms, these companies have not only redefined how financial services are accessed and used but also brought economic inclusion to previously marginalized groups. This context highlights the importance of understanding not only fintechs' exponential growth but also the regulatory challenges and opportunities for innovation facing this emerging sector.

This study is justified by the urgent need to explore fintechs' impact on Brazil's financial environment. In a country characterized by significant banking penetration and rapid adoption of digital technologies, understanding how fintechs shape and are shaped by the regulatory and economic context is crucial. This work seeks to deepen understanding of the dynamics among technological innovation, financial regulation, and financial inclusion, offering relevant contributions to policymakers, academics, and financial sector professionals.

The central research question is: how are payment fintechs regulated in Brazil, and how do those regulations influence their ability to promote financial inclusion and technological innovation? This question examines not only the challenges fintechs face in Brazil's regulatory context but also the opportunities created by effective, adaptable regulation. By defining this problem, the study seeks clear, objective answers contributing to an informed, well-grounded debate on fintechs' future in the country.

1. Bachelor's degree in Law from the Universidade Federal Fluminense – UFF; postgraduate student in Digital Law at ITS Rio in partnership with the Universidade do Estado do Rio de Janeiro – UERJ. Legal Counsel at dLocal Instituição de Pagamento.

This study's objectives include investigating payment fintechs' evolution in Brazil and the economic, technological, and regulatory factors driving their growth. It will examine different stages of that evolution and how these companies have influenced the national financial landscape. It also seeks to analyze regulatory challenges by exploring the rules and regulations affecting fintech operations in the country. Compliance requirements and the dilemmas fintechs face in adapting to a constantly changing regulatory environment will be highlighted to understand their impact on the sector's development and innovation.

The methodology will consist of a comprehensive, analytical literature review. Academic sources, financial institution reports, regulatory documents, and specialized journal articles will be consulted to map and critically analyze current knowledge. This approach will integrate the available information and provide a solid basis for the analyses and conclusions presented in this scholarly article.

1. The Evolution of Payment Fintechs in Brazil

Fintech refers to companies that use innovative technology to offer financial products and services more efficiently and accessibly, adapting them to consumers' and businesses' needs.[2] These companies operate in financial market segments such as electronic payments, peer-to-peer lending, personal financial management, automated investment, and digital insurance. Fintech is distinguished by its disruptive potential in the traditional financial sector, usually characterized by more bureaucratic and less agile structures. Fintechs seek to transform users' financial experiences through innovative technological solutions, using 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 mark a significant milestone in the global financial sector's evolution. Arising from the convergence of technology and finance, fintechs emerged as disruptive alternatives to traditional financial service models. In the

2. WÓJCIK, D. Financial Geography I: Exploring FinTech – Maps and concepts. Progress in Human Geography, 45(3), 566-576. 2021.

Brazilian and international contexts, this growth had various drivers, particularly economic, technological, and regulatory factors.[3]

The emergence and evolution of fintechs in Brazil form a fascinating chapter in the financial sector's recent history. Fintechs first gained prominence in the country in the early 2000s as internet penetration and mobile technologies advanced. Companies such as PagSeguro and Moip, currently part of the Wirecard group, pioneered electronic payment and online transaction processing solutions, making financial market access easier for small merchants and digital entrepreneurs.[4]

From the mid-2010s, Brazil's fintech landscape expanded significantly. Financial service startups emerged in personal financial management, online credit, automated investment, and digital insurance. Demand for more accessible, efficient solutions drove this growth, particularly among consumers seeking alternatives to traditional banks.[5]

The regulatory environment also played a crucial role in Brazilian fintechs' evolution.[6] The Central Bank of Brazil introduced measures such as Resolution No. 4.282 of 2013, establishing requirements for payment institutions' operations, and, more recently, the PIX instant payment system in 2020. PIX revolutionized financial transactions in the country and opened new opportunities for fintechs.

Today, Brazilian fintechs are increasingly integrated into the national financial ecosystem and compete on equal terms with traditional banks in many respects. They have democratized access to financial services while promoting greater market efficiency and innovation, contributing to a more dynamic and inclusive financial system for all Brazilians.[7]

3. SILVA, Lucas Leão. LISBOA, Erika Farias. FERREIRA, Luciene Braz. VERSIANI, Ângela França. SOUSA, Paulo Renato. CORDEIRO, Marcelo Lisboa. As instituições financeiras e sua relação com as fintechs no Brasil. Revista Economia & Gestão, vol. 20, no. 55, 2020.

4. BASTOS, Luiz Felipe Pereira. Cronologia das fintechs no brasil: um olhar sobre a transformação do setor financeiro, 2023. Final project for a higher education technology program in Business Management. 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. Análise do cenário regulatório das fintechs no Brasil. Universidade Federal Rural do Semi-árido, Centro de Ciências Sociais Aplicadas e Humanas, Law Program, 2020. Available at: https://repositorio.ufersa.edu.br/server/api/core/bitstreams/754509b9-d274-415f-be7d-c84861ac2bb2/content. Accessed July 18, 2024.

7. BASTOS, Luiz Felipe Pereira. Cronologia das fintechs no brasil: um olhar sobre a transformação do setor financeiro, 2023. Final project for a higher education technology program in Business Management. Fatec São Carlos, São Carlos, 2023.

Economically, fintechs emerged from the need for efficient, accessible financial services, particularly among populations previously excluded from traditional banking. Technologically, advances in digital platforms, cloud computing, big data analysis, and artificial intelligence enabled agile, personalized, accessible financial solutions. These technologies made new business models possible and transformed the user experience, allowing faster, safer transactions.[8]

The regulatory environment also played a crucial role in shaping fintechs. Innovative regulations, such as regulatory sandboxes providing controlled environments to test products and services, have often been fundamental to developing and validating fintech solutions. Traditional regulations, however, frequently present challenges, requiring significant adaptations to meet security, consumer protection, and anti-money laundering requirements.[9]

Across fintechs' main development phases, a progression from emerging startups to established financial ecosystem participants is evident. Initially focused on niches such as mobile payments and international transfers, fintechs expanded into peer-to-peer lending, personal financial management, automated investment, and digital insurance. This diversification reflects their adaptability in responding to market demands and exploring 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 Law No. 4.595, with the mission of ensuring the national currency's purchasing-power stability, maintaining a sound and efficient financial system, and promoting the population's economic well-being. Over time, the BCB's mission expanded to include controlling inflation,

8. LIMA, Talison Layala Praxedes de. Análise do cenário regulatório das fintechs no Brasil. Universidade Federal Rural do Semi-árido, Centro de Ciências Sociais Aplicadas e Humanas, Law Program, 2020. Available at: https://repositorio.ufersa.edu.br/server/api/core/bitstreams/754509b9-d274-415f-be7d-c84861ac2bb2/content. Accessed July 18, 2024.

9. DINIZ, Bruno. O fenômeno Fintech: tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo. Rio de Janeiro: Alta Books, 2019, p. 31.

regulating the financial system, and implementing effective monetary policies.[10]

The Central Bank of Brazil comprises several areas and departments, each with specific functions contributing to its overall mission. The BCB's internal organization is described as follows: the National Monetary Council (CMN), the national financial system's highest body, formulates monetary and credit policy. It comprises the Minister of Finance, the Minister of Planning, Development and Management, and the Central Bank President. The Board of Directors, comprising the Central Bank President and directors responsible for specific areas, defines and implements policies to achieve the CMN's objectives.[11]

The BCB's departments and functional areas include the Banking Operations and Payments System Department (Deban), which manages banking operations and the payment system; the Banking Supervision Department (Desup), which supervises financial institutions to ensure soundness and regulatory compliance; the Economics Department (Depec), which conducts economic analyses and monitors macroeconomic indicators; and the Open Market Operations Department (Demab), which conducts open market operations and controls financial system liquidity.[12]

The Central Bank of Brazil uses several monetary policy instruments to achieve its objectives. The Selic rate, the economy's benchmark interest rate, influences all other interest rates and is used to control inflation and stabilize the currency. Open market operations involve buying and selling government securities to control money in circulation and maintain adequate financial system liquidity. Reserve requirements—the percentage of deposits commercial banks must hold at the Central Bank—regulate credit supply and banking system liquidity. Foreign exchange market interventions also seek to

10. BANCO CENTRAL DO BRASIL. Estabilidade financeira: fintechs. Brasília, DF: Banco Central do Brasil, 2020a. Available at: https://www.bcb.gov.br/estabilidadefinanceira/fintechs. Accessed July 15, 2024.

11. MENDONÇA, Saulo Bichara; DE PAULA IVO, Felipe. Conselho Administrativo de Defesa Econômica e Banco Central do Brasil: análise do conflito de competência. Revista de Direito, vol. 12, no. 1, p. 4, 2020.

12. MISSAGIA, Caio Rezende; AMATO, Lucas Fucci. Ambientes regulatórios experimentais: o sandbox no sistema financeiro brasileiro. Revista Brasileira de Sociologia do Direito, vol. 10, no. 3, pp. 143-171, 2023.

influence the exchange rate and stabilize the currency, protecting the economy from external shocks and exchange rate fluctuations.[13]

The Central Bank of Brazil plays a vital role in the national economy, ensuring economic and financial stability through a defined organizational structure and effective monetary policy instruments. The BCB's mission and functions are essential to a stable economic environment conducive to Brazil's sustainable development.

2.1 Main Regulations and Rules for Payment Fintechs

The Central Bank of Brazil has adopted several regulatory initiatives crucial to supervising payment fintechs. One is Resolution No. 4.282 of 2013 [14], establishing criteria for authorizing and operating payment institutions. It defines minimum capital, corporate governance, internal control, and risk management requirements that fintechs must observe to obtain and retain authorization to operate.[15]

The Central Bank also issued Circular No. 3.682 of 2013 [16], regulating payment services and establishing specific guidelines for payment institutions. It addresses user information, protection of customer funds, transparent fees, and prevention of money laundering and terrorist financing. Circular No. 3.682, by promoting

13. SILVA, Christian Feliciano da. Disque 100 – Implementação de políticas regulatórias: o caso do Open Finance a partir do Banco Central do Brasil. 2023. 42 leaves, illustrated. Final project for a bachelor's degree in Public Policy Management – Universidade de Brasília, Brasília, 2023.

14. BRASIL. Ministério da Fazenda. Banco Central do Brasil. Resolução nº 4.282, de 4 de novembro de 2013. Establishes guidelines for regulating, overseeing, and supervising payment institutions and payment arrangements within the Brazilian Payments System (SPB) under Law No. 12.865 of October 9, 2013. Diário Oficial da União: 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 July 18, 2024.

15. OIOLI, Erik Frederico; SILVA, Rafael Toni; ZILIOTI, Matheus. Fintechs e a regulação do sistema financeiro nacional. In: OIOLI, Erik Frederico (coordinator). Manual de direito para startups. 2nd edition. São Paulo: Thomson Reuters Brasil, 2020, pp. 187-210.

16. BRASIL. Ministério da Fazenda. Banco Central do Brasil. Circular nº 3.682, de 4 de novembro de 2013. Approves regulations governing payment services within payment arrangements belonging to the Brazilian Payments System (SPB), establishes criteria for excluding payment arrangements from the SPB, and provides other measures. Diário Oficial da União: section 1, Brasília, DF, year 150, no. 216, pp. 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 July 18, 2024.

greater transparency and security in operations, strengthens users' trust in payment fintech services.[17]

Another important regulatory milestone is the Brazilian Payments System (SPB), established by Law No. 12.865 of 2013 [18]. The SPB provides the infrastructure for financial transactions in the country, including electronic payments and fund transfers. Joining the SPB places payment fintechs within a secure, efficient system that facilitates interoperability among financial institutions and promotes financial inclusion.

The Central Bank also implemented the regulatory sandbox concept under Resolution No. 29 of 2020 [19]. It allows payment fintechs to test technological innovations in a controlled environment under BCB supervision and monitoring. This initiative encourages financial sector innovation while ensuring consumer protection and financial system stability. The sandbox provides space to test and evaluate technologies and business models before full market implementation.

The general term "sandbox" is used in software development strategies to describe an environment isolated from other systems, allowing a new system to operate without interference from the external environment. Introduced into finance by fintechs, a sandbox

17. "Art. 18. Financial institutions may operate in the country only with prior authorization from the Central Bank of the Republic of Brazil or, for foreign institutions, an Executive Branch decree." (BRASIL. Lei nº 4.595, de 31 de dezembro de 1964. Provides for monetary, banking, and credit policy and institutions, creates the National Monetary Council, and provides other measures. Brasília, DF: Presidência da República, [2017], Article 18. Available at: http://www.planalto.gov.br/ccivil_03/leis/L4595compilado.htm. Accessed July 18, 2024).

18. "Art. 6. For the purposes of the rules applicable to payment arrangements and institutions joining the Brazilian Payments System (SPB) under this Law, the following definition applies: I – payment arrangement: a set of rules and procedures governing a particular payment service offered to the public and accepted by more than one payee, with direct access by end users, payers, and payees;" (BRASIL. Lei nº 12.865, de 9 de outubro de 2013. Provides for payment arrangements and institutions within the Brazilian Payments System (SPB), among other matters. Brasília, DF: Presidência da República, [2020]. Available at: http://www.planalto.gov.br/ccivil_03/_ato20112014/2013/lei/l12865.htm. Accessed July 18, 2024.)

19. In Brazil, the principal regulatory framework enabling fintech sandboxes was Joint Resolution No. 1 of February 4, 2021, jointly issued by the National Monetary Council (CMN), Central Bank of Brazil (Bacen), Comissão de Valores Mobiliários (CVM), and Superintendência de Seguros Privados (Susep). It establishes guidelines for implementing the experimental regulatory environment known as the regulatory sandbox.

Joint Resolution No. 1/2021 defines criteria and procedures for selecting and monitoring sandbox participants, as well as requirements for entering and exiting this controlled regulatory environment. It seeks to promote financial sector innovation by allowing fintechs to test products and services under regulatory supervision while protecting consumers and financial system integrity.
The Central Bank of Brazil also issued BCB Resolution No. 29 of October 26, 2020, establishing specific conditions for creating and operating the regulatory sandbox within Bacen's remit. It details fintech admission criteria, participants' obligations, and supervision and control mechanisms.

> describes a testing environment where financial products and services are tested in isolation and assessed for safety and effectiveness before being offered to the public.[20]

Regarding security and compliance, the Central Bank sets strict rules to protect customer data and prevent unlawful activities. The General Personal Data Protection Law (LGPD), enacted in 2018, and the BCB's cybersecurity and risk management guidelines under Resolution No. 4.658 of 2018 [21], impose obligations on payment fintechs to ensure users' information remains confidential, intact, and available. These security rules are essential to mitigating risks and maintaining consumers' trust in fintech services.

3. Challenges and Opportunities in Regulating Payment Fintechs

Payment fintechs face substantial, multifaceted regulatory and compliance challenges. In a constantly evolving financial environment, they must adapt to a regulatory framework that seeks financial system security and stability but may also create significant barriers to innovation and growth. Meeting strict legal and regulatory requirements imposes a considerable burden on companies that often have more agile but less robust structures than traditional financial institutions.[22]

One major regulatory challenge is complying with current legislation, including complex, detailed rules on money laundering prevention, data protection, and cybersecurity. Payment fintechs must implement robust policies and procedures to comply with Law No. 9.613/1998, concerning crimes of "laundering" or concealment of assets,

20. SQUASSONI, Christian. O Sandbox Regulatório e o novo papel do regulador financeiro. In: EROLES, Pedro (coordinator). Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas Tecnologias Financeiras. São Paulo: Quartier Latin, 2019. pp. 157-178.

21. RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018. Provides for cybersecurity policy and requirements for contracting data processing, data storage, and cloud computing services applicable to financial institutions and other institutions authorized to operate by the Central Bank of Brazil.

22. PELLEGRINO, Maria Beatriz. A evolução dos subcredenciadores no Sistema de Pagamentos Brasileiro (SPB). In: EROLES, Pedro (coordinator). Fintechs, bancos digitais e meios de pagamento: aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p. 109.

rights, and valuables, as well as the General Personal Data Protection Law (LGPD), which establishes personal data processing guidelines. These requirements demand significant investment in technology and human resources and continuous monitoring and updating of internal processes.[23]

Regulation also presents transparency and accountability challenges. Payment fintechs must keep detailed operational records and be prepared to provide accurate, timely information to regulators. Central Bank Circular No. 3.682 of 2013, for example, requires periodic reporting, demanding efficient, reliable management systems. Failure to meet these obligations may result in severe sanctions, including substantial fines and, in extreme cases, revoked operating authorization.[24]

Another challenge is managing risks and implementing adequate internal controls. Payment fintechs operate in a dynamic environment exposed to operational, credit, and market risks. National Monetary Council Resolution No. 4.658 of 2018, concerning cybersecurity policy and requirements for contracting data processing and storage services, requires fintechs to mitigate risks and protect customer information's integrity and confidentiality. An effective compliance program, including regular internal audits and continuous employee training, is essential to mitigating these risks.[25]

The regulatory environment can also create uncertainty for payment fintechs. Financial technologies and consumer expectations often evolve before regulatory rules are updated. This gap may create legal and operational uncertainties, hindering predictability and strategic planning. A flexible, adaptable framework allowing experimentation and testing of business models in a controlled environment, such as the regulatory sandbox implemented

23. SQUASSONI, Christian. O Sandbox Regulatório e o novo papel do regulador financeiro. In: EROLES, Pedro (coordinator). Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas Tecnologias Financeiras. São Paulo: Quartier Latin, 2019. pp. 157-178.

24. OIOLI, Erik Frederico; SILVA, Rafael Toni; ZILIOTI, Matheus. Fintechs e a regulação do sistema financeiro nacional. In: OIOLI, Erik Frederico (coordinator). Manual de direito para startups. 2nd edition. São Paulo: Thomson Reuters Brasil, 2020, pp. 187-210.

25. DINIZ, Bruno. O fenômeno Fintech: tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo. Rio de Janeiro: Alta Books, 2019.

by the Central Bank, is a positive response, although its effective implementation and reach are still developing.[26]

Final considerations

Payment fintechs present numerous opportunities to drive innovation and promote financial inclusion in Brazil. Appropriate regulation, although challenging, also opens the way to a safer, more trustworthy environment where innovation can flourish and business models can be tested and implemented, benefiting both companies and consumers.

Technological innovation is one of payment fintech growth's greatest opportunities. Digitizing financial services allows more efficient, accessible, and convenient solutions. Artificial intelligence, machine learning, and blockchain enable innovative products and services addressing specific consumer needs, improving user experience and increasing financial market competitiveness. Digital wallets, contactless payments, and integrated payment platforms illustrate how fintechs are revolutionizing the sector.

Fintechs also play a crucial role in financial inclusion. A significant proportion of Brazil's population remains unbanked or underbanked, facing difficulties accessing traditional financial services. Digital payment fintech solutions can reach these marginalized populations and provide basic services such as payment accounts, fund transfers, and microcredit. This inclusion is essential to economic and social development, giving people greater autonomy and ability to manage their finances.

The regulatory environment also creates significant opportunities. Open banking in Brazil, for example, seeks to encourage innovation and competition in finance. It allows secure sharing of financial data among different

26. SQUASSONI, Christian. O Sandbox Regulatório e o novo papel do regulador financeiro. In: EROLES, Pedro (coordinator). Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas Tecnologias Financeiras. São Paulo: Quartier Latin, 2019. pp. 157-178.

institutions with customer consent, promoting personalized, integrated services. Fintechs can use this infrastructure to develop more competitive solutions adapted to consumer needs, improving market efficiency and transparency.

Another important opportunity is the Central Bank's regulatory sandbox, which allows fintechs to test technological innovations in a controlled, supervised environment. Ideas can be evaluated and adjusted before full market implementation, reducing risks and improving their chances of success. The sandbox encourages innovation and helps fintechs adapt to regulatory requirements through constructive dialogue between regulators and innovators.

Growing demand for sustainable, socially responsible solutions also creates opportunities for payment fintechs. They can develop financial products promoting environmental sustainability and positive social impacts, aligned with modern consumers' and investors' expectations. Examples include platforms for investment in sustainable projects, microcredit for small businesses, and financial education initiatives. Incorporating social responsibility criteria into operations can earn consumer trust and contribute to more equitable, sustainable development.

Payment fintechs in Brazil thus face a wide range of opportunities to drive innovation and financial inclusion. Digitizing financial services, promoting open banking, using regulatory sandboxes, and developing sustainable solutions are among the ways fintechs can transform financial markets. Appropriate regulation can catalyze innovation and growth rather than obstruct them, creating an environment where fintechs thrive and provide significant benefits to society.

References

BANCO CENTRAL DO BRASIL. Estabilidade financeira: fintechs. Brasília, DF: Banco Central do Brasil, 2020a. Available at: https://www.bcb.gov.br/estabilidadefinanceira/fintechs. Accessed July 15, 2024.

BASTOS, Luiz Felipe Pereira. Cronologia das fintechs no brasil: um olhar sobre a transformação do setor financeiro. Final project for a higher education technology program in Business Management. Fatec São Carlos, São Carlos, 2023.

BRASIL. Lei nº 12.865, de 9 de outubro de 2013. Provides for payment arrangements and payment institutions belonging to the Brazilian Payments System (SPB), among other matters. Brasília, DF: Presidency of the Republic, [2020]. Available at: http://www.planalto.gov.br/ccivil_03/_ato20112014/2013/lei/l12865.htm. Accessed July 18, 2024.)

BRASIL. Lei nº 4.595, de 31 de dezembro de 1964. Provides for monetary, banking, and credit policy and institutions, establishes 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. Accessed July 18, 2024).

BRASIL. Ministério da Fazenda. Banco Central do Brasil. Circular nº 3.682, de 4 de novembro de 2013. Approves regulations governing payment services within payment arrangements belonging to the Brazilian Payments System (SPB), establishes criteria for excluding payment arrangements from the SPB, and provides other measures. Diário Oficial da União: section 1, Brasília, DF, year 150, no. 216, pp. 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 July 18, 2024.

BRASIL. Ministério da Fazenda. Banco Central do Brasil. Resolução nº 4.282, de 4 de novembro de 2013. Establishes guidelines for regulating, overseeing, and supervising payment institutions and payment arrangements within the Brazilian Payments System (SPB) under Law No. 12.865 of October 9, 2013. Diário Oficial da União: 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 July 18, 2024.

LIMA, Talison Layala Praxedes de. Análise do cenário regulatório das fintechs no Brasil. Universidade Federal Rural do Semiárido. Centro de Ciências Sociais Aplicadas e Humanas, Law Program, 2020. Available at: https://repositorio.ufersa.edu.br/server/api/core/bitstreams/754509b9-d274-415f-be7d-c84861ac2bb2/content. Accessed July 18, 2024.

MISSAGIA, Caio Rezende; AMATO, Lucas Fucci. Ambientes regulatórios experimentais: o sandbox no sistema financeiro brasileiro. Revista Brasileira de Sociologia do Direito, vol. 10, no. 3, pp. 143-171, 2023.

MENDONÇA, Saulo Bichara; DE PAULA IVO, Felipe. Conselho Administrativo de Defesa Econômica e Banco Central do Brasil: análise do conflito de competência. Revista de Direito, vol. 12, no. 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 e a regulação do sistema financeiro nacional. In: OIOLI, Erik Frederico (coordinator). Manual de direito para startups. 2nd edition. São Paulo: Thomson Reuters Brasil, 2020, pp. 187-210.

PELLEGRINO, Maria Beatriz. A evolução dos subcredenciadores no Sistema de Pagamentos Brasileiro (SPB). In: EROLES, Pedro (coordinator). Fintechs, bancos digitais e meios de pagamento: aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p. 109.

RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018. Provides for cybersecurity policy and requirements for contracting services for processing and storing

data and for cloud computing to be observed by financial institutions and other institutions authorized to operate by the Central Bank of Brazil.

SILVA, Lucas Leão. LISBOA, Erika Farias. FERREIRA, Luciene Braz. VERSIANI, Ângela França. SOUSA, Paulo Renato. CORDEIRO, Marcelo Lisboa. As instituições financeiras e sua relação com as fintechs no Brasil. Revista Economia & Gestão, vol. 20, no. 55, 2020.

SILVA, Christian Feliciano da. Disque 100 – Implementação de políticas regulatórias: o caso do Open Finance a partir do Banco Central do Brasil. 2023. 42 leaves, illustrated. Final project for a bachelor's degree in Public Policy Management – Universidade de Brasília, Brasília, 2023.

SQUASSONI, Christian. O Sandbox Regulatório e o novo papel do regulador financeiro. In: EROLES, Pedro (coordinator). Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas Tecnologias Financeiras. São Paulo: Quartier Latin, 2019. pp. 157-178.

WÓJCIK, D. Financial Geography I: Exploring FinTech – Maps and concepts. Progress in Human Geography, 45(3), 566-576. 2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

15

Blockchain as a Feminine Noun: A Gender Analysis of the Growing Use of Blockchain Technology

CAROLINA FREITAS GOMIDE DE ARAUJO

Contents: Introduction. 1. What Are the Values of the Technology of Value? 2. How Distributed Is the Distributed Financial System? 3. Can We Entrust Women's Future to the Technology of Trust? Final Considerations. References.

Introduction

According to the Dicionário Priberam da Língua Portuguesa (DPLP), blockchain, a masculine noun, is a "technology that uses a decentralized database, with information from a large network, linked by encryption algorithms, generally used for cryptocurrency transactions."[2]

The choice of a masculine translation in the dictionary, although an interesting grammatical question, serves as a starting point for a deeper question: how masculine is blockchain technology?

As it appears, the grammatical choice confirms a reality: blockchain is a system that, to date, has been built from a masculine perspective. This article, however, seeks to highlight potential applications through which the technology could reduce gender inequalities rather than contribute to their intensification.

Thus, this article aims to analyze how this emerging technology interacts with gender inequalities in various contexts. In addressing these issues, the article seeks to broaden understanding of the intersection between gender and technology in the digital age, bringing potential applications of the technology to light. To do so, it will use an approach that includes a literature review, documentary analysis, and the study of previously documented cases.

Blockchain technology emerged as a revolutionary innovation, promising to transform various 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 review by FGV researchers on blockchain applications from a gender perspective found only 21 articles in the Scopus, Web of Science, Scielo, Ebsco, and Google Scholar databases through August 2023, with only one focused on the Brazilian case.[3]

1. Master's degree in Public Law from the Faculdade de Direito da Universidade de São Paulo (USP). Postgraduate student in Digital Law at UERJ/ITS. Visiting researcher at Queen's University, Canada. Author of the books "Cortes Constitucionais Digitais" and "Poder Constituinte Originário das Mulheres no Brasil."

2. DICIONÁRIO PRIBERAM. Blockchain. Available at: https://dicionario.priberam.org/blockchain. Accessed July 20, 2024.

3. SANTOS, Vanessa Martins dos; DINIZ, Eduardo Henrique; MORAES, Tricia Karla Lacerda; CERNEV, Adrian Kemmer; LOURENÇO, Carlos Eduardo. Blockchain e (des)igualdade de gênero: uma revisão sistemática da literatura. AMCIS 2024 Proceedings, 2024. Available at: https://aisel.aisnet.org/amcis2024/span_lacais/span_lacais/5. Accessed July 7, 2024.

Thus, the choice of topic is justified by the still limited academic literature on the subject. In other words, although blockchain technology is increasingly important and has the potential to transform various sectors of society, analyses that consider its gender implications remain rare.

The article is structured into three sections. The first discusses how masculine power structures have shaped access to technologies since their origins, and the potential impact of the absence of a gender perspective in applying new technologies such as blockchain. The second presents examples of initiatives that use blockchain to promote gender equality in access to property and financial resources, aiming to explore how this technology can affect gender inequalities in global economic systems. Finally, the last section presents blockchain-based solutions for addressing gender inequalities on a global scale and in different social contexts.

1. What Are the Values of the Technology of Value?

The internet as we know it today reflects a world historically shaped by patriarchal structures. The internet's initial architecture was built in a cultural environment in which masculine 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 women's voices. This creates a digital space that, in many cases, is neither safe nor inclusive for women.

The advent of blockchain promises a revolution in online exchanges of value and property. However, the promise of a fairer and more inclusive system faces significant challenges related to reproducing the same gender inequalities observed in society and replicated and intensified during the development of the internet.

If the internet grew rapidly and brought the social problems of physical reality into the digital space, blockchain technology is likely to follow a similar path, but at a faster pace. This is concerning, given that the dynamics of gender exclusion may intensify in an environment where the distribution of value and property is central.

As this section will discuss, although blockchain is often promoted as a neutral technology, the reality is that its implementation and development take place in a social context that still carries

deep gender disparities. Moreover, the blockchain and cryptocurrency industry is still predominantly male, with significantly low female representation in leadership and technological development positions. This inequality can result in products and solutions that fail to adequately consider women's needs and perspectives.

The blockchain world is widely recognized for its male dominance, often characterized by the term "Bitcoin bros." This reality is evident at industry events, which often end up discouraging women's participation.

One notorious example occurred in 2018 at the North American Bitcoin Conference, where 85 speakers were men and only three were women. The event was widely criticized after organizers invited the 5,000 participants to an official evening networking opportunity at a large strip club in Miami. Until 23h, when the event technically ended, guests were served by women wearing lingerie. Women who attended the conference said they left the club when the strippers appeared and criticized the event online. Jeff Scott, a New York cryptocurrency trader attending the conference, commented: "We're a group 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."[4]

In 2022, at the Bitcoin Conference in Miami, which attracted more than 25,000 participants, Rachel Siegel, known online as @CryptoFinally, experienced an incident of harassment that highlighted the persistent sexism in the community. During the event, Siegel, who was interacting with other participants, had her photo taken without permission by a participant identified as @bitcoin_fuckboi. The image, posted on social media, showed Siegel from an unflattering angle and was accompanied by sexually aggressive comments and insults about her body. When Siegel tried to report the incident to conference organizers, she encountered resistance and an inadequate response. Even after identifying the harasser on social media and discovering that he had taken selfies with other prominent participants, the organizers took no significant action. One organizer, who used the pseudonym @Chairforce, even liked some of the offensive tweets.[5]

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 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 August 6, 2024.

To try to overcome this situation, initiatives focused on education and the creation of women's networks in blockchain have been developed. In 2022, Gwyneth Paltrow and Mila Kunis promoted an event to introduce a new cryptocurrency club called BFF. Initiatives such as Women in Blockchain and the Black Women Blockchain Council also aim to support women throughout the broad cryptocurrency ecosystem. Another example is Ladies in Bitcoin, which organizes events and workshops to educate women interested in Bitcoin.[6]

Analyzing 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 blockchain's potential, the literature highlights at least four specific areas of risk related to applying the technology from a gender perspective. They are: (i) the lack of gender analysis in the planning stages 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 protecting human rights, including gender-based violence.[7]

First, 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. Thus, a gender impact analysis would be needed for any proposed use of blockchain technology to anticipate some of the main areas of concern and risks that need to be addressed before its introduction.

Regarding unequal access to technology, disparities in access to smartphones and connectivity are a problem strongly influenced by gender. Women often face greater difficulties accessing information and means of communication, and the digital gender gap makes women in low- and middle-income countries 10% less likely to own a mobile phone and 23% less likely to use mobile internet. In places such as the Kakuma refugee camp in Kenya, although smartphone ownership and internet access are growing, only 12% of women own smartphones, compared with 37% of men. This means

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 August 6, 2024.

7. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. Gender & Development, pp. 317-336. 2019.

that women often depend on men's smartphones instead of having their own, limiting women's access to online services and applications.[8]

Regarding the lack of representation and participation of women and girls in the design and implementation of the technology, it is essential to hear 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 the technology, but can also exercise their autonomy and use blockchain technology in ways that empower them. The data, however, demonstrate the disparity affecting women in this market.

Regarding who owns startups related to blockchain use, research by the brokerage Bitget identified that only 8% of startups are led by women.[9]

A study conducted by Forex reveals concerning data on the gender disparity in the crypto and blockchain sector, showing men's predominance 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 male dominance in the industry.[10]

In addition to examining CEOs, the Forex study examined leadership positions in general, finding that, of the 259 leadership positions identified, 201 were held by men and 58 by women. This represents 78% of positions held by men and only 22% by women. Another noteworthy point is the analysis of the top 50 crypto influencers on Twitter, in which Forex found that only 14% were women.[11]

Finally, regarding the fourth aspect and potential gender-based violence caused by the technology, Thylin and Duarte point out that any humanitarian application of blockchain technology must comply with international humanitarian law, which can be challenging when private companies' interests conflict with humanitarian interests. A central concern with new technologies is the issue

8. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. Gender & Development, pp. 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 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 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 July 11, 2024.

of data protection and privacy, which can lead to severe human rights violations. Although the full range of possible violations is not yet clear, keeping information on the blockchain private and secure against potential attacks is one of the most concerning issues about blockchain technology, and the gender dimensions of these data protection and privacy risks need to be explored.[12]

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 exchanges of value, have gender equality as one of its fundamental principles. It is therefore imperative for academia to analyze blockchain's potential risks and applications as its reach expands. Beginning this research agenda, the following sections highlight some potential applications already recorded in the literature.

2. How Distributed Is the Distributed Financial System?

"Women, consider cryptocurrencies. Otherwise, men will get all the wealth again." This famous warning was issued by investor Alexia Bonatsos on Twitter.[13]

Indeed, in the offline world, women have historically faced significant barriers regarding property and access to financial resources. For centuries, the laws of many countries denied women the right to own property, restricting their economic and social autonomy. Even after legal achievements guaranteeing women the right to own assets, substantial inequalities persist that hinder women's access to financing and investments.

Blockchain technology promises to democratize access to property and value, but data show that there is no gender distribution in the distributed financial system. This can be analyzed through aspects such as the number of women investing in cryptocurrencies or the number of women able to increase their wealth using blockchain-related technologies.

According to data provided by Brazil's Federal Revenue Service, between 2021 and 2023, cryptoasset transactions carried out by women fluctuated on average

12. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. Gender & Development, pp. 317-336. 2019.

13. ÉPOCA NEGÓCIOS. Mulheres buscam seu espaço na indústria do Blockchain. Available at: <https://epocanegocios.globo.com/Carreira/noticia/2018/02/mulheres-buscam-seu-espaco-na-industria-do-blockchain.html> Accessed July 6, 2024.

between 10% and 20%. In the best scenario, recorded in December 2022, men still accounted for more than 70% of transactions.[14]

Regarding investment received, a study by the brokerage Bitget demonstrates a clear correlation between the founder's gender and investment volumes, as statistics indicate that women-led blockchain startups raised only 6% of the total value of market investments, confirming the existence of gender bias.[15]

This unequal history reinforces the importance of studying blockchain technology from a gender perspective so that it develops in a way that includes and empowers women and gender minorities. This chapter discusses the potential application of blockchain as a financial instrument capable of mitigating gender inequalities in the financial market.

A Brazilian example of a blockchain technology application with a gender impact is the Moeda Seeds platform. This platform facilitates access to microfinance for women entrepreneurs with projects that have a social impact. Using blockchain and its own digital tokens, Moeda Seeds creates an ecosystem in which investors worldwide can contribute quickly and transparently to sustainable growth. The platform is designed to support financial inclusion and gender equality, especially for women who have difficulty accessing credit from traditional banks. In addition to financial support, selected projects receive management assistance to optimize their operations and promote sustainable practices over the long term.[16]

Another example is 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, independently of male family members. Olivier Mukuta and his team developed this solution and won an award at the first blockchain hackathon co-organized by UN Women and Innovation Norway in July 2017, which aimed to empower women in humanitarian crises.[17]

14. RECEITA FEDERAL. Criptoativos: Relatório de Dados abertos e informações gerais. Available at: https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos/arquivos/criptoativos_dados_abertos_25092023.pdf Accessed 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 August 3, 2024.

16. KANEGAE, L. C.; CERNEV, A. K.; DINIZ, E. Moeda Seeds: E-Commerce and Crypto Solutions for Development. Revista de Administração Contemporânea, vol. 25, special issue, p. e200224, 2021.

17. 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 July 6, 2024.

For women in humanitarian crises, lack of access to financial systems and the inability to transfer assets are critical issues. This problem is often associated with the absence of identification documents, as in low-income countries, for example, more than 45% of women lack basic identification, compared with 30% of men. Moreover, most adults without access to banking are women, accounting for 56% of the unbanked, compared with 44% for men. In countries affected by humanitarian crises, women are 30% less likely than men to have an individual financial account, as in Lebanon, where 62% of men and 33% of women have a bank account.[18]

When a crisis occurs, 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.[19]

One example is Building Blocks, a World Food Programme (WFP) project considered the humanitarian sector's largest blockchain-based cash distribution system, used to provide efficient and secure assistance to refugees and vulnerable people. Operating in countries such as Bangladesh, Jordan, Lebanon, and Ukraine, the project enables financial assistance to be distributed through a collaborative network bringing together various humanitarian organizations. Since its inception, the project has processed more than 555 million dollars in cash transfers, saving 3.5 million dollars in bank fees that can be redirected to assist more people in need.[20]

Through blockchain hubs operated by multiple organizations, the platform enables the coordination of aid distribution, meeting needs such as food and reproductive health simultaneously. Families receive vouchers that can be used at local points of sale, simplifying the process and eliminating the need to visit different locations for assistance. This frees up resources for other needs, such as education, and provides protection against diseases common in environments without adequate sanitation.[21]

18. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. Gender & Development, pp. 317-336. 2019.

19. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. Gender & Development, pp. 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 Accessed 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 July 4, 2024.

UN Women also partnered with the WFP to innovate in the use of blockchain to support Syrian refugee women participating in cash-for-work programs in the Za'atari and Azraq refugee camps in Jordan. In the joint initiative, women beneficiaries who previously received their monthly benefit in cash on a specific date at UN Women's Oasis centers can now withdraw money at their convenience from various supermarkets as cash back at checkout.

In the program, a virtual wallet is created for each beneficiary, showing the amount owed to her for her work, and, once a purchase is made, the blockchain records the amount to be debited. Moreover, instead of requiring any additional identification documents, women can do this using an iris scan that validates their identity at the supermarket. This makes transactions for women in the refugee camps much faster and safer to monitor.[22]

In addition, UN Women is strengthening its programming to improve the digital and financial literacy of refugee women beneficiaries. At its four Oasis centers, the UN is offering additional training and seminars on expense tracking and budgeting so beneficiaries can view their Building Blocks accounts and history online.[23]

It must be emphasized, however, that there are caveats regarding adoption of the program. First, critics have argued that, because it is a private blockchain, its transformative potential would be limited. In fact, before the partnership with UN Women, the WFP managed all the system's nodes, reducing its credibility. UN Women began operating an independent node, enabling mutual validation of transactions. The expectation is that, by demonstrating effective collaboration around a neutral blockchain network, other humanitarian organizations will recognize the benefits and join the common network, bringing the system closer to the characteristics of a public network.[24]

Moreover, 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, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. Gender & Development, pp. 317-336. 2019.

23. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. Gender & Development, pp. 317-336. 2019.

24. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. Gender & Development, pp. 317-336. 2019.

resources, which can be problematic in humanitarian contexts. In addition, countries less involved in exploring the technology and smaller humanitarian actors may not benefit fully from blockchain, exacerbating global inequalities.[25]

Thus, some initiatives that use blockchain technology in different ways to encourage women's access to the banking and financial system can already be identified. However, the technology also has the potential to influence other social relationships, as the following discussion highlights.

3. Can We Entrust Women's Future to the Technology of Trust?

Blockchain is known as the technology of trust because the transfers recorded on it can be considered reliable and immutable. Using this analogy, this section seeks to explore whether we can trust that blockchain technology will have beneficial applications regarding women's access to services and policies. This section presents some potential applications of the technology.

Regarding career advancement, the shortage of women in leadership positions at blockchain startups, as already noted, calls for strategies to promote gender equality in technological spaces. Blockchain platforms themselves present viable instruments for increasing women's participation in the market, from the hiring process, eliminating biases and enabling impartial assessments based on candidates' qualifications, to career management, promoting women's participation and advancement.[26]

The literature, for example, already advocates the possibility of creating a recruitment platform on which each candidate has a unique identity, eliminating the possibility of prejudice and allowing candidates to be assessed solely on their qualifications. In the study by Obu et al., a hiring platform was practically designed based

25. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. Gender & Development, pp. 317-336. 2019.

26. SANTOS, Vanessa Martins dos; DINIZ, Eduardo Henrique; MORAES, Tricia Karla Lacerda; CERNEV, Adrian Kemmer; LOURENÇO, Carlos Eduardo. Blockchain e (des)igualdade de gênero: uma revisão sistemática da literatura. AMCIS 2024 Proceedings, 2024.

on blockchain and intentionally adjusted to prevent hiring based on gender and other discriminatory factors.[27]

Beyond encouraging women's career advancement, blockchain can play a vital role in protecting women against violence and abuse, offering 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 securely and immutably.

Blockchain technology is being used in mobile applications to record and report cases of sexual harassment anonymously. These applications ensure that reports are handled confidentially and that digital evidence is preserved securely.

The French application Hehop, short for Help for Hope, uses blockchain to enable victims of domestic violence to collect and store digital evidence of abuse that can be used in legal proceedings. The technology ensures that the evidence is secure and tamperproof, providing a powerful tool for victims to access the judiciary.[28]

In Brazil, one example is Projeto Glória, in which blockchain is integrated with artificial intelligence and analytics to improve the collection, analysis, and availability of data on violence against women. These data are intended to support the development of educational content, implementation of public policies, and establishment of a support network equipped with the tools needed to achieve social improvements.[29]

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 digital art to be promoted. With NFTs' potential to transform the art world, the lack of female representation in the NFT and blockchain space began to enter the agenda of artists pursuing social missions, leading some women 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), pp. 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 July 5, 2024.

29. VICENTE, Beatriz de Freitas Alves. A tecnologia blockchain a favor da mulher. 2022. Available at: https://www.conjur.com.br/2022-abr-04/beatriz-vicente-blockchain-favor-mulher/ Accessed July 3, 2024.

a market dominated by men, through various initiatives and projects.[30]

One 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 launched in 2022 called WoW Galaxy. WoW aims to create an inclusive and diverse Web 3.0, promoting equal participation in the NFT space. The project team supports causes related to women's empowerment, initially donating 7.5% of sales from its first collection to organizations such as She's The First, Too Young to Wed, and Strange Cintia.[31]

Similarly, Women Rise is an NFT art project created by visual artist Maliha Abidi and launched in 2021. The Women Rise collection consists of 10,000 unique, randomly generated digital tokens. To help pursue gender equality, 2.5% of sales are donated to the Malala Fund and 7.5% to organizations supporting gender equality, women's education, and mental health in marginalized communities. Moreover, Women Rise is one of the first NFT projects to commit to the 2030 Agenda for Sustainable Development, incorporating the Sustainable Development Goals (SDGs) into its artwork and donations.[32]

Another use of NFTs is proposed in the literature to change safety in sexting and the unauthorized sharing of intimate photos, which primarily affects girls and women. Franco et al. explore the use of blockchain technology, and specifically NFTs, to combat the nonconsensual dissemination of user-generated intimate images, highlighting that traditional messaging applications used for sexting are insecure because they allow personal content to be shared easily. By implementing decentralized blockchain-based solutions, the authors aim to create a safer and more reliable environment in which the presence of malicious nodes is mitigated, ensuring better performance, scalability, and privacy compared with centralized systems.[33]

A risk concerning gender-related data and its inclusion in blockchain technology, in turn, is raised by Shahaab et al., who argue that although

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.; MICHIENZI, A.; PALAZZI, C. E. A decentralised messaging system robust against the unauthorised forwarding of private content. Future Generation Computer Systems, vol. 145, pp. 211-222, 2023.

blockchain can play a crucial role in constructing digital identity and protecting personal data online, personal data must not be considered “static” and must never be stored immutably, as this could have serious consequences for trans people.[34]

Thus, this section sought to highlight that, beyond typical applications related to the financial market, the literature already discusses potential applications and risks of blockchain technology in various social contexts.

Final Considerations

This article explored the various ways in which blockchain technology can be used to address issues of gender inequality, considering the scarcity of academic works addressing the topic, especially in Portuguese.

The first section highlighted how blockchain technology’s promise of democratization still faces significant challenges in fully realizing its transformative potential for gender equality.

The second section discussed gender distribution in the distributed financial system. Analysis of the data revealed that women still face significant barriers in accessing and using cryptoassets and investments, demonstrated by the gender disparity in blockchain startups and women’s lower participation in cryptocurrency transactions. However, examples such as Moeda Seeds and VipiCash demonstrated that the technology can provide women with greater control over their financial resources and facilitate access to microfinance. Moreover, initiatives such as Building Blocks demonstrate how blockchain can be used to offer innovative solutions in humanitarian contexts.

The last section presented blockchain solutions for impartial recruitment, NFTs in the art market, and applications for reporting violence that offer a glimpse of how the technology can be used innovatively to address social issues.

Although there is potential to use the technology from a gender perspective, it is crucial to ensure that these solutions are implemented with attention to ethical considerations and women’s needs, 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, pp. 1-8, 2020.

that technology alone will not resolve systemic inequalities. The conclusion is that technological developments must be accompanied by a holistic approach that includes public policies, education, and awareness to create a more inclusive environment.

Only through collaboration among governments, the private sector, and civil society will it be possible to maximize blockchain technology's positive impact on women's lives, ensuring that it becomes a truly 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 August 3, 2024.

DICIONÁRIO PRIBERAM. Blockchain. Available at: https://dicionario.priberam.org/blockchain. Accessed July 20, 2024.

ÉPOCA NEGÓCIOS. Mulheres buscam seu espaço na indústria do Blockchain. Available at: https://epocanegocios.globo.com/Carreira/noticia/2018/02/mulheres-buscam-seu-espaco-na-industria-do-blockchain.html. Accessed 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 July 11, 2024.

FRANCO, M.; GAGGI, O.; GUIDI, B.; MICHIENZI, A.; PALAZZI, C. E. A decentralised messaging system robust against the unauthorised forwarding of private content. Future Generation Computer Systems, vol. 145, pp. 211-222, 2023.

KANEGAE, L. C.; CERNEV, A. K.; DINIZ, E. Moeda Seeds: E-Commerce and Crypto Solutions for Development. Revista de Administração Contemporânea, vol. 25, special issue, 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 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 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), pp. 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 August 6, 2024.

RECEITA FEDERAL. Criptoativos: Relatório de Dados abertos e informações gerais. Available at: https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos/arquivos/criptoativos_dados_abertos_25092023.pdf Accessed July 25, 2024.

SANTOS, Vanessa Martins dos; DINIZ, Eduardo Henrique; MORAES, Tricia Karla Lacerda; CERNEV, Adrian Kemmer; LOURENÇO, Carlos Eduardo. Blockchain e (des)igualdade de gênero: uma revisão sistemática da literatura. AMCIS 2024 Proceedings, 2024. Available at: https://aisel.aisnet.org/amcis2024/span_lacais/span_lacais/5. Accessed 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, pp. 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, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. Gender & Development, pp. 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 July 6, 2024.

VICENTE, Beatriz de Freitas Alves. A tecnologia blockchain a favor da mulher. 2022. Available at: https://www.conjur.com.br/2022-abr-04/beatriz-vicente-blockchain-favor-mulher/ Accessed 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 July 5, 2024.

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 Accessed August 4, 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Theme III

Data Protection and Digital Security

AUTHORS

Giovana Sant'Anna

Lígia Maria de Souza Lopes Reis

Maíra Lima de Souza

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

16

Risk and Cybersecurity in Brazil: A Regulatory Analysis Aimed at Data Protection

GIOVANA SANT'ANNA

Contents: Introduction. 1. Risk Society and the Information Society. 2. Cyber Vulnerabilities and Cybersecurity. 3. Current Legislative Landscape. Final Considerations. Bibliographic References.

Introduction

Concern about internet use cannot be described as something new to the current generation. Since the 1980s and the steady, gradual democratization of computers, the term virus[2] was already becoming popular among users, system administrators, and organizations in general. Risks arising from internet use already existed then, but cyberattacks are now increasingly sophisticated and difficult to detect, leaving us to find a wide variety of ways to mitigate them, primarily through predictive approaches.[3]

Social evolution resulting from the growing use of technologies brought a dimension linked to digital structures into personal relationships, which, in turn, requires the constant use of large amounts of personal and sensitive data.[4] This drew attention to Information Security[5] and digital security,[6] topics that became frequent subjects of debate and discussion fueled by media coverage, especially after incidents

1. Attorney who graduated in Law from the Faculdade de Direito de São Bernardo do Campo in 2018. Postgraduate student at the Instituto de Tecnologia do Rio de Janeiro (ITS Rio).

2. A computer virus is malware, that is, intrusive software or code created to infect, damage, or access computer files, replicating itself and infecting other files and documents. For more details, see: LATTO, Nica. O que é e como funciona um vírus de computador? Avast Academy, 2020. Available at: https://www.avast.com/pt-br/c-computer-virus#:~:text=Um%20v%C3%ADrus%20de%20computador%20%C3%A9,a%20outros%20arquivos%20ou%20documentos. Accessed July 17, 2024.

3. ALMEIDA, João Emílio de. Cibersegurança: da prevenção do risco à gestão de incidentes. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, Porto, issue 43, pp. 1-4, September 30, 2021. pp. 1-4. Available at: https://scielo.pt/pdf/rist/n43/1646-9895-rist-43-1.pdf. Accessed May 2, 2024.

4. In short, under Law 13.709/2018, personal data means any information related to a person that makes that person identified or identifiable, and sensitive personal data means any data concerning ethnic or racial origin, religion, political opinions, membership in unions or religious, philosophical, or political organizations, health or sex life, or genetic or biometric data. For more details, see: BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Brasília: Presidency of the Republic. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.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. Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. 1st edition. Rio de Janeiro: Rio de Janeiro: FGV Direito Rio, August 2023. Available at: https://direitorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil. Accessed June 24, 2024.

6. SHIRA, Fer; JANCZ, Carla. Barricadas estratégias e coletividade: uma cartilha de segurança digital para organizações. Marialab, São Paulo, December 1, 2022. p. 3. Available at: https://www.marialab.org/wp-content/uploads/2020/12/Barricas-estrategias-coletividade.pdf. Accessed July 13, 2024.

involving major information leaks, putting the rights of thousands of users worldwide at risk.[7]

Today, targets are not limited to private companies or individuals. Cyberattacks target government organizations and even countries directly, one example being the controversial United States presidential election in 2016, which brought the terms “cyberterrorism” and “military attack” through cyber means to the fore. In other words, technological progress brought an enormous burden: information’s monetary valuation and its use as an influential weapon of social, political, and economic control.[8]

Beck[9] emphasizes that globalization brings new risks to light. Risk is not restricted to physical threats, but includes social and environmental dangers arising from technological progress, which may range from nuclear accidents to data privacy and security. These are global and transcendent risks capable of affecting individuals and societies and challenging traditional structures, which will necessarily have to seek new methods for managing digital risks.

Thus, the intense transformation resulting from recent decades of unchecked technological progress culminated in the emergence of a new era for humanity, characterized by attractive technology.[10] Legal Theory was therefore forced to rethink its foundations to incorporate technological impacts, shaping boundaries and rules capable of curbing the previously unknown technological development and keeping pace with changes in human and social meaning, ensuring protection of the rights of users who are data subjects.[11]

Teffé[12] understands that the law must act preventively to protect data while still reflecting individuals’ autonomy and imposing duties on the relevant actors. Thus originates the term “Digital Law,” arising from the law itself, encompassing its most varied areas, the dilemmas of the so-called

7. FICHTNER, Laura. What kind of cyber security? Theorising cyber security and mapping approaches. Internet Policy Review, Germany, vol. 7, pp. 1-19, May 15, 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 June 3, 2024.

8. ALMEIDA, João Emílio de. Cibersegurança: da prevenção do risco à gestão de incidentes. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, Porto, issue 43, pp. 1-4, September 30, 2021. pp. 1-4. Available at: https://scielo.pt/pdf/rist/n43/1646-9895-rist-43-1.pdf. Accessed May 2, 2024.

9. BECK, Ulrich. Sociedade de Risco rumo a uma outra modernidade. São Paulo: Editora 34, 2014, pp. 25-28.

10. LUCCA, Newton de. Dignidade da pessoa humana e os riscos eletrônicos. Galileu – Revista de Economia e Direito, vol. XVII, no. 1. 2012. p. 283.

11. BITTAR, Eduardo C.B. A Teoria do Direito, a Era Digital e o Pós-Humano: o novo estatuto do corpo sob um regime tecnológico e a emergência do Sujeito Pós-Humano de Direito. Direito e Praxis, vol. 10, no. 2, 2019, p. 935.

12. TEFFÉ, Chiara de. Dados pessoais sensíveis: Qualificação, tratamento e boas práticas. Indaiatuba, São Paulo, 2022. unpaginated. Available at: https://www.google.com.br/books/edition/Dados_Pessoais_Sens%C3%ADveis/atCLEAAAQBAJ?hl=ptBR&gbpv=1. Accessed June 28, 2024.

information society and today's technological expansion.[13] The issue of regulation for the virtual world and the advent of digital law can be seen as expressing a political vision much more than a legal one, since the internet represents a direct domain for economic and social development.[14]

Domestically, we find some legislative frameworks seeking to protect internet users' individual rights and data, notably the Cybercrime Law (Law 12.737/2012), the Brazilian Civil Rights Framework for the Internet (Law 12.965/2014), and the General Data Protection Law (Law 13.709/2018).[15] However, regulation of cybersecurity measures remains unclear and fragmented. This is the field in which this article develops, seeking to elucidate the concept of risk in digital society, the importance of preventive action through governance measures, and the current regulations applicable to cybersecurity and data protection in Brazil through the publication of the unprecedented—and recent—National Information Security Policy, enacted by Decree No. 11.856 in December 2023.

1. Risk Society and the Information Society

The digital age poses unprecedented challenges to Legal Science because of intense social transformations, the imposition of "algorithms," and digital operations, that is, the introduction of a new social (technological) dynamic that established necessary processes for adapting legal subject matter to ensure effective protection of data subjects' rights.[16] Digital law arises from the very need for regulation prompted by the technological obstacles and dilemmas characteristic of the Information Society.[17] In today's society, information is regarded as a valuable product, a financial asset, and must be understood as such; therefore, it must be processed, cared for, and protected. Information systems are essential for organizing these data and play an important role in risk analysis and mitigating potential information leaks.[18]

13. PIMENTEL, José E. S. Introdução ao Direito Digital. Revista Jurídica ESMP-SP, vol. 13, 2018, p. 18.

14. LUCCA, Newton. Dignidade da pessoa humana e os riscos eletrônicos. Galileu – Revista de Economia e Direito, vol. XVII, no. 1. 2012. p. 283.

15. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. Brasil contemporâneo. São Paulo, vol. 29., 2024. p. 4.

16. BITTAR, Eduardo C.B. A Teoria do Direito, a Era Digital e o Pós-Humano: o novo estatuto do corpo sob um regime tecnológico e a emergência do Sujeito Pós-Humano de Direito. Direito e Praxis, vol. 10, no. 2, 2019, p. 935.

17. PIMENTEL, José E. S. Introdução ao Direito Digital. Revista Jurídica ESMP-SP, vol. 13, 2018, p. 18.

18. SAMPAIO, Dhiêgo R.L. Um estudo sobre riscos de segurança da informação no campus da UFC em Quixadá com base na norma ISO/IEC 27005. 2014. 45 leaves. Monograph (Bachelor's degree in Information Sciences) – Universidade Federal do Ceará, Quixadá, 2014.

Broadly speaking, Digital Law emerges to regulate the virtual environment, interactions arising from that environment, and the storage and processing of digital data, to actively protect society against violations of its individual rights. De Lucca[19] conceptualizes that, if a parallel between the two eras (the Industrial Revolution and the Digital Revolution) were plausible, the difference would lie in the speed of the transformations caused by the digital age. Whereas the Industrial Revolution is based on the amount of labor invested in products and services, the Digital Revolution is based on the amount of information and knowledge about products and services. The large quantity and rapid transmission of this information are hallmarks of the digital age, whose production model is based on the mass generation of information, its rapid dissemination, and the decentralization of its sources.[20]

Information in a dangerous or uncertain environment creates risks[21] and therefore insecurity. Digital insecurity must be combated by implementing controls that can be put in place to ensure risks are reduced to an acceptable level.[22] We must also consider that the state's processing of data through digital technologies can cause institutional violence against communities. Users are considered the weak party in any digital system, so educating society is undoubtedly considered essential, as it is one of the effective means of curbing these new forms of social violence and the vulnerability of individual rights.[23] It should be emphasized that the large volume of data resulting from internet use has become an extremely valuable currency in today's society, highlighting a severe risk to data subjects' privacy.[24]

The German sociologist Ulrich Beck[25] proposes, through the "Theory of (Industrial) Risk Society," a rupture at the heart of society as a consequence of

19. LUCCA, Newton. Dignidade da pessoa humana e os riscos eletrônicos. Galileu – Revista de Economia e Direito, vol. XVII, no. 1. 2012. pp. 283-285.

20. PIMENTEL, José E. S. Introdução ao Direito Digital. Revista Jurídica ESMP-SP, vol. 13, 2018, pp. 19-20.

21. According to ISO/IEC 27005, information security risk is assessed as a function of the likelihood of an incident and its consequences, and managing it makes it possible to alter its likelihood and consequences.

22. SAMPAIO, Dhiêgo R.L. Um estudo sobre riscos de segurança da informação no campus da UFC em Quixadá com base na norma ISSO/IEC 27005. 2014. 45 leaves. Monograph (Bachelor's degree in Information Sciences) – Universidade Federal do Ceará, Quixadá, 2014.

23. BELLI, Lucca; Bakonyi Erica; Chen Larissa, et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. Rio de Janeiro: FGV Direito Rio, 2023, pp. 15-16.

24. LORENZON, Laila N. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia,* 2021, p. 40.

25. BECK, Ulrich. *Sociedade de Risco rumo a uma outra modernidade.* São Paulo: Editora 34, 2014, p. 17.

industrial and scientific development and, inherent in them, risks. The author holds that Risk Society is intrinsically catastrophic, since in it the exceptional state of insecurity and threat is normalized. He further defines current risks as direct impacts of modernization and distinguishes them from the industrial risks of the nineteenth and twentieth centuries, since those were limited to certain areas and specific groups, whereas the risks arising from modernization are transnational and will inevitably cross border barriers and even reach those who produced them or profit from them.

Beck[26] mentions that these risks have a boomerang effect, that is, not even the most powerful social stratum is effectively safe and shielded from them. The sociologist further proposes that risks, like wealth, are objects of distribution, and that this distribution does not occur equally. While wealth appears as products, risks or threats qualify as the byproduct of modernization.[27] It is therefore 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[28] highlights the asymmetry among the state, processing agents, and data subjects in the distribution of risks, underscoring the need to rethink this distribution in order 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[29] teaches that the concept of risk was already present as early as the mid-sixteenth century. Its emergence would have come from the invention of maritime insurance, being seen as a probability of losses and gains over the course of voyages. Thus, it would involve the interaction among systems, society, and the uncertainties arising from that relationship, and is therefore inherent in a complex social construction. Luhmann[30] further establishes that, depending on the social sphere involved, risk will differ and will entail different challenges and outcomes. For example, the political aspect will demand a risk and outcomes different from those of the economic and legal spheres of society. As for technological risk, we can understand it as the result of the very

26. BECK, Ulrich. Sociedade de Risco rumo a uma outra modernidade. São Paulo: Editora 34, 2014, pp. 25-30.

27. Ibid.

28. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: *Thomson Reuters Brasil*, 2020, p. 255.

29. LUHMANN, Niklas. A Sociological Theory. New York: Routledge, 2017, pp. 8-9.

30. Ibid., pp. 30-35.

systemic development, capable of involving risks of technical failures, cyberattacks, and even social and environmental consequences not yet mapped. However, risks must be assessed and mitigated, that is, managed, in order to ensure the safety of society at large in its use of the internet.

Luhmann[31] distinguishes the concepts of risk, security, and danger. He sees the first two as antagonistic, with risk associated with the decisions made in everyday life and security with the state we constantly seek socially, even though in the contemporary world scene it is practically impossible to fully mitigate every type of risk. As for danger, the author relates this concept to a situation of harm that is not caused by the agent who bears 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. After the Renaissance, however, there was a significant shift with the rationalization of decision-making, when we gradually began to assume responsibility for the outcomes of those decisions.[32] Hence, digital risks will be present as long as social and technological changes produce unforeseen consequences. We can therefore regard risks as the uncertain side of modernity. This does not mean that life today is riskier than in earlier eras, but that for today's society, both laypeople and experts must carry out the daily and permanent task of weighing and managing risks.[33]

Over the years, society has gradually advanced in establishing rational risk calculations. Initially, risk calculation took a dualistic view of failure versus success, but this calculation was later better developed with robust metrics drawn from mathematics and probability, yielding greater control over the outcomes of risks. Yet when addressing the subject of risk, we must always remember that we are facing a vast range of human experiences, which places us before an eternal unknown and means that, even with the most robust methods developed to date, it is impossible to predict or control all risks.[34] Moreover, science and technology bring with them several

31. Ibid., p. 19.

32. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: *Thomson Reuters Brasil*, 2020, p. 252.

33. GIDDENS, Anthony. *Modernidade e Identidade*. Rio de Janeiro: Jorge Zahar, 2002, p. 32.

34. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: *Thomson Reuters Brasil*, 2020, p. 252.

benefits and conveniences, even as they force us to confront risks and dangers. It is therefore advantageous to assess and manage risks rationally so that we can reap the benefits of postmodern society.[35]

In the early 2000s, cases of data intrusion and violations of users' privacy became more frequent owing to the emergence of spam[36] from website databases, which sold and shared users' information.[37] This rapid social transformation brought about by high levels of digitalization, with a focus on data as a model of wealth, brought to light the need for greater investment in cybersecurity. As the technology market expands, with qualified professionals in the field, there is also a growing criminal sector that demands constant updating on the subject. Thus, the demand for legal protection of data stems from the economic importance that data play in today's reality, and the high volume of data stored by public and private entities highlights the elevated risk to users' privacy, making clear the need for legislative updating to guarantee the protection of civil society's fundamental rights.[38]

2. Cyber Vulnerabilities and Cybersecurity

As already mentioned, the large number of connected people has culminated in a significant increase in cybercrime and in greater societal attention to the pressing need to draw up rules of conduct and to limit state and private action in controlling the information they process and store.[39] At first analysis, cybersecurity is a multifaceted ecosystem that requires implementing a governance mechanism and a competent body of norms that interact with each other and with the different sectors of society in order to ensure efficient and effective application. This calls for a formalized national alignment by means

35. GIDDENS, Anthony. *Modernidade e Identidade*. Rio de Janeiro: Jorge Zahar, 2002, p. 32.

36. Spam derives from the English term "Sending and Posting Advertisement in Mass," that is, it can be interpreted as the mass sending and posting of advertisements. For more details, see: LINKNACIONAL. O que é spam? Link Nacional, October 20, 2023. Available at: https://www.linknacional.com.br/blog/o-que-e-spam/. Accessed June 24, 2024.

37. BRAGA, Noelson Araújo. Ciberegurança e o Direito à Privacidade: Um estudo sobre a construção cibernética no Brasil e na União Europeia na ótica realista. 2021. 35 leaves. Monograph (Bachelor's degree in International Relations) – Universidade de Brasília UNB, Brasília, 2021.

38. LORENZON, Laila N. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia,* 2021, p. 40.

39. BRAGA, Noelson Araújo. Ciberegurança e o Direito à Privacidade: Um estudo sobre a construção cibernética no Brasil e na União Europeia na ótica realista. 2021. 35 leaves. Monograph (Bachelor's degree in International Relations) – Universidade de Brasília UNB, Brasília, 2021.

of a regulation capable of establishing minimum operational standards, principles, and a governance system with risk mitigation.[40]

Cybersecurity must be considered a real concern in drawing up a plan to confront challenges and prevent risks and threats from materializing. Reactive action—decision-making after accidents—can cause substantial losses and enormous financial, legal, and reputational damage to companies and to public authorities.[41] In the setting of private organizations, it is inevitable to strengthen defense systems and anticipate frequent digital attacks. These attacks generally consist of theft or hijacking of information,[42] as occurs with ransomware.[43] We can therefore understand cybersecurity as a body of norms that establishes procedures and practices aimed at the security of systems, information, and digital risks, with information security being only one of the layers of cybersecurity.

Cybersecurity incidents, although often linked to failures or direct attacks, also refer to unsafe behavior by developers or users of technologies, which can compromise the foundational principles of confidentiality, integrity, authenticity, authentication, and access.[44] There are recent and striking cases that directly affected the provision of public services in Brazil, notably the incident involving the vaccination records of the Brazilian population and attacks on court systems that force the extension of deadlines and the paralysis of public service delivery to citizens.[45]

In 2021, two emblematic cases marked Brazil's reality at the cybersecurity level: the intrusion into the ConectSUS app[46] and the sale of data from the Controladoria Geral da União (Office of the Comptroller General, CGU) on internet forums. The ConectSUS app was breached 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; GASPAR, Walter B. Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. 1st ed. Rio de Janeiro: Rio de Janeiro: FGV Direito Rio, August 2023. p. 22. Available at: https://direitorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil. Accessed June 24, 2024.

41. Ibid.

42. ALMEIDA, João E. de. Cibersegurança: da prevenção do risco à gestão de incidentes. *RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação.* Porto, 2021, p.2.

43. A form of attack that consists of blocking or hijacking organizations' information or systems, where release occurs only upon payment of a ransom. For more details, see: ibid., p. 19.

44. BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B. Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. 1st ed. Rio de Janeiro: Rio de Janeiro: FGV Direito Rio, August 2023. pp. 24-25. Available at: https://direitorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil. Accessed June 24, 2024.

45. Ibid., p. 19.

46. Problemas no ConecteSUS: antes de ataque hacker, sistema teve polêmica com alteração de dados e falhas. 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 alteration of the data of several users. Some vaccine doses simply disappeared from the system, and users reported that their data (name, mother's name, and nationality) had been modified. The Ministry of Health stated at the time that it had taken the appropriate measures and even took down access to the ConectSUS app.[47] Also in 2021, there was a widespread intrusion into Brazilian government public services: Federal Administration credentials were found for sale on dark web forums, and logins and passwords of the CGU and the Ministry of Health were leaked.[48]

In addition, in November 2020 the Superior Court of Justice (STJ) suffered a cyberattack[49] that the Court itself described as the worst cyberattack ever carried out against a Brazilian public institution.[50] The attack prevented millions of people from accessing the STJ platform, including the Justices themselves, causing genuine chaos in the judiciary and the suspension of procedural deadlines for almost an entire week. The years 2020 and 2021 were thus marked by major data leaks in Brazil, leaks capable of affecting a number larger than the national population itself, since they exposed the data of more than 220 million people.[51] This fact reflects an important current characteristic: the dependence of public and private organizations on the internet.[52]

This shows that, in the current scenario, in which being connected has become an essential act across various social strata, cyber insecurity threatens society as a whole, calling into question even the democratic outlook.[53] Private companies and public bodies and entities remain the main targets of attacks; nevertheless, society in general must always be concerned and contribute to protecting its rights. It is worth noting that

47. Problemas no ConecteSUS: antes de ataque hacker, sistema teve polêmica com alteração de dados e falhas. 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. CRIMINOSOS vendem dados do CGU e Ministério da Saúde na dark web. [S. l.], December 21, 2021. Available at: https://canaltech.com.br/seguranca/criminosos-vendem-dados-do-cgu-e-ministerio-da-saude-na-dark-web-204985/. Accessed June 27, 2024.

49. G1. STJ aciona PF para apurar possível ataque de hackers ao sistema do tribunal. G1, November 4, 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 July 2, 2024.

50. MARCON, Daniele Verza. Seguro contra Riscos Cibernéticos: desafios para delimitar a garantia e promover a cibersegurança na era digital. 2023. Master's dissertation (Master's 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 July 3, 2024.

51. Ibid.

52. Ibid.

53. BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B. Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. 1st ed. Rio de Janeiro: Rio de Janeiro: FGV Direito Rio, August 2023. p. 19. Available at: https://direitorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil. Accessed June 24, 2024.

cyberattacks do not occur only as a result of active attacks, but also occur passively, owing to the fragility or absence of basic security measures and users' lack of training.[54]

In 2023, Brazil topped the ranking of countries with the largest volume of leaked data, surpassing India, the United States, and Indonesia in the volume of compromised information. Among the leaked information, names, emails, addresses, and passwords stored by the cookies[55] saved in Brazilian users' browsers stand out.[56] Such incidents show that Brazilian society still suffers from a lack of control over its own information, which can be read as an affront to the privacy right of the data subject, who is unable to exercise his or her power of decision, processing, and transmission over his or her information.[57]

In view of the high risk faced by federal public organizations, in 2022 the Tribunal de Contas da União (Federal Court of Accounts, TCU) published a booklet highlighting five cybersecurity control measures that would need to be urgently implemented by the Brazilian public administration, namely: inventory and control of enterprise information technology assets; inventory and control of software assets; continuous vulnerability management; security awareness and skills training; and incident response management.[58]

This was part of a series of measures taken in response to the episodes highlighted here, since they brought to light the high-risk vulnerability of the national public administration. In addition to the booklet published by the TCU, these events also prompted the publication of a new framework on cybersecurity in December 2023, the National Cybersecurity Policy (PNCiber)—Presidential Decree No. 11.856. This Decree, which functions as an immediate response to the worrying current scenario,[59] will be analyzed in the next chapter.

54. SHIRA, Fer; JANCZ, Carla. BARRICADAS ESTRATÉGIAS E COLETIVIDADE: Uma cartilha de segurança digital para organizações. Marialab, São Paulo, December 1, 2022. Available at: https://www.marialab.org/wp-content/uploads/2020/12/Barricas-estrategias-coletividade.pdf. Accessed July 13, 2024.

55. Cookies are files created by websites in order to collect information about users' browsing on the internet; they can be used for users' convenience, storing logins and passwords and items added to virtual shopping carts, for example. For more details, see: G1. O que são cookies na internet e como eles funcionam. G1, June 09, 2024. Available at: https://g1.globo.com/tecnologia/noticia/2024/06/09/o-que-sao-cookies-na-internet-e-como-eles-funcionam.ghtml. Accessed June 24, 2024.

56. CRIMINOSOS vendem dados do CGU e Ministério da Saúde na dark web. [S. l.], December 21, 2021. Available at: https://canaltech.com.br/seguranca/criminosos-vendem-dados-do-cgu-e-ministerio-da-saude-na-dark-web-204985/. Accessed June 27, 2024.

57. TEFFÉ, Chiara de. Dados pessoais sensíveis: Qualificação, tratamento e boas práticas. Indaiatuba, São Paulo, 2022. unpaginated.

58. Tribunal de Contas da União. Cinco controles de segurança cibernética para ontem / Tribunal de Contas da União. – Brasília: TCU, 2022. 36 p. p.1. Available at: https://portal.tcu.gov.br/5-controles-de-seguranca-cibernetica.htm. Accessed July 06, 2024.

59. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. Brasil contemporâneo. São Paulo, vol. 29., 2024. pp. 8-10.

3. Current Legislative Landscape

Cyber policies are indispensable in a governance approach that demands institutional structures aimed at solving public problems in a context of undefined roles and responsibilities. In this scenario of multiple actors, the role of public administration must be to direct and guide actions. These mechanisms must operate by defining clear objectives, assigning responsibilities, and developing improvements in performance and in policies that promote information security. In other words, what is needed is guiding standardization by the Federal Government, the promotion of public policies, and the assignment of responsibilities to the competent bodies and entities.[60]

The National Cybersecurity Policy (PNCiber) was implemented precisely to respond reactively to the current scenario of insecurity through the development of regulation and oversight mechanisms, international cooperation strategies, and the development of training and education in cybersecurity, among others.[61] However, it is essential to stress that other measures were adopted before the publication of the PNCiber, and it is necessary to clarify them to enable a more precise analysis of this scenario in Brazil.

First, it should be noted that, in the context of data protection in Brazil, the following stand out: Article 5 of the Federal Constitution, which provides for the inviolability of people's private life, privacy, honor, and image;[62] the Civil Code, which provides for the inviolability of private life;[63] and the Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet)—Law 12.965/2014—a pioneer in codifying rights and duties for internet use.[64] The latter already established the protection of personal data as a principle of internet use in Article 3, items II and III.[65] However, even after its enactment, Brazil still faced the need for specific and consolidated regulation on the processing of personal data.[66]

60. Ibid., pp. 2-3.

61. Ibid., pp. 10-11.

62. BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 2016. 496 p. Available at: planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed June 01, 2024.

63. BRASIL. Lei 10.406, de 10 de janeiro de 2002. Establishes the Brazilian Civil Code. Diário Oficial da União. Brasília: Presidency of the Republic. Available at: planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Accessed January 05, 2024.

64. LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. Revista do Programa de Direito da União Europeia, [S. l.], pp. 1-14, March 15, 2021. pp. 41-42.

65. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Establishes principles, guarantees, rights, and duties for the use of the Internet in Brazil. Diário Oficial da União. Brasília: Presidency of the Republic. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed June 07, 2023.

66. MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. Panorama Setorial da Internet, [S. l.], year 11, no. 2, pp. 1-20, June 2019. pp. 2-4. Available at: https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Accessed July 2024.

It was for this reason that the General Data Protection Law (LGPD) came about 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 precursor instrument in the Brazilian landscape by establishing a standard of conduct to be adopted by processors of personal data in favor of protecting fundamental rights, human dignity, and data subjects' right to privacy (Lóssio, 2020). It came as the instrument capable of ensuring the protection of personal data, which until then was not effectively secured by other instruments. In addition, the LGPD supported the development of public policies to control the processing of these data, since an insecure digital environment becomes more unacceptable by the day, nationally or internationally. The aforementioned legislation also brought as a characteristic novelty the protection of users' privacy against companies with excessive stored 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 twenty-first century culminated in a lag that still has not kept pace with exponential technological growth (Braga, 2021). Nevertheless, when one conducts a practical analysis of risk analysis under the LGPD, what one finds is far more a practice of regulatory compliance aimed at achieving accountability[67] and reducing the likelihood of sanctions than an effective concern with possible harm to users' rights. Hence, the overlap that occurs during risk analysis—in which a search for technical and regulatory compliance takes the place of protecting users' fundamental rights—is a valid concern.[68]

Because of this, several Decrees originated in the Brazilian landscape, among them the E-Digital (Decree 9.319/2018);[69] Decree No. 10.046/2019 [70], which provides for governance in data sharing within the federal public administration; the Digital Government Strategy for the years

67. A set of practices aimed at holding the entire data processing chain accountable. For more details, see: MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. Panorama Setorial da Internet, [S. l.], year 11, no. 2, pp. 1-20, June 2019. Available at: https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Accessed July 2024.

68. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: *Thomson Reuters Brasil,* 2020, pp 245-271. p. 258.

69. BRASIL. Decreto nº 9.319, de 14 de março de 2018. Amends Decree No. 8.777 of May 11, 2016, which establishes the National Consumer Protection and Defense Policy. Diário Oficial da União, Brasília, March 15, 2018. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.htm. Accessed June 01, 2024.

70. BRASIL. Decreto nº 10.046, de 30 de setembro de 2019. Amends Decree No. 9.203 of November 22, 2017, which regulates Law No. 13.334 of September 13, 2016. Diário Oficial da União, Brasília, October 1, 2019. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Accessed June 01, 2024.

2020 to 2022 (Decree No. 10.332/2020);[71] the publication of the National Cybersecurity Strategy, or E-Ciber (Decree 10.222/2020);[72] and the approval of the National Critical Infrastructure Security Plan, through Decree No. 11.200 [73]. The E-Digital is notable on the subject of cybersecurity because it proposes significant improvements to Brazil's cyber infrastructure.[74] It promotes adequate access to technology and digital inclusion throughout the national territory, in urban and rural areas, proposes development and innovation initiatives, and also determines the protection of users' rights and privacy and fosters the need for security in the digital environment, encouraging education and professional training.[75]

The PNCiber was also preceded by the publication of Decree 9.637/2018, which established the National Information Security Policy (PNSI), updated in 2021 through Decree No. 10.641. The PNSI was an important nationwide policy whose scope was to strengthen the culture of information security in society and to encourage professional qualification in the field of information security.[76] We can interpret it as the foundation of cyber governance in Brazil, since it established information security on a large scale and incorporated the principles of integrity, confidentiality, and guaranteed availability of information. Furthermore, it stimulated the creation of a national cybersecurity policy with the participation of the public and private sectors.[77]

In this sense, the PNSI provides for the importance of creating a national information security strategy (E-Ciber) [78] . The national strategy, together with the national plans, constituted the instruments of the PNSI that established the participation of society and of public bodies and entities and assigned

71. BRASIL. Decreto nº 10.332, de 28 de abril de 2020. Provides for the creation of the National Program to Support Job and Income Generation. Diário Oficial da União, Brasília, Apr. 29, 2020. Available at: https://www.planalto.gov.br/cci- vil_03/ _ato2019-2022/2020/decreto/d10332.htm#:~:text=DECRETO%20N%C2%BA%2010.332%2C%20DE%2028,funda- cional%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Accessed: June 07, 2024.

72. BRASIL. Decreto nº 10.222, de 05 de fevereiro de 2020. Approves the National Cybersecurity Strategy. Diário Oficial da União, Brasília,. 2020. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222. htm. Accessed: June 07, 2024.

73. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. Bra- sil contemporâneo . São Paulo, v. 29., 2024. pp. 4-8.

74. Ibid.

75. Decreto n. 9.319, de 21 de março de 2018. (2018). Establishes the National System for Digital Transformation and sets out the governance structure for implementing the Brazilian Digital Transformation Strategy. Brasília, DF.

76. Ibid.

77. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. *Bra- sil contemporâneo*. 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. Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digital- mente soberano. 1st ed. Rio de Janeiro: Rio de Janeiro: FGV Direito Rio , Aug. 2023. Available at: https://direitorio.fgv.br/publi- cacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil. Accessed: June 24, 2024. p. 12.

as the competence and responsibility of the Institutional Security Cabinet of the Presidency of the Republic for its preparation and publication [79] . Article 6 of the PNSI determines the structure of the National Information Security Strategy, divided into the following modules: cyber defense; security of critical infrastructure; security of classified information; and protection against data leakage. The PNSI was also concerned with guaranteeing the protection of users' fundamental rights against possible data leaks, establishing the protection of personal data and privacy as one of its principles throughout Article 3, item II [80] .

The National Critical Infrastructure Security Plan (Decree No. 11.200/2022) [81] addresses the indispensability of risk management for the security of critical infrastructure, with the determination of a systemic methodology to identify, assess, and treat risks. Because of the quantity of information, it establishes the need for constant monitoring and timely action in crisis scenarios so that appropriate measures can be adopted. It also promoted the need for integration and cooperation between the public and private sectors and established an Integrated Security and Critical Infrastructure Data System, through which the Security of Brazil's Critical Infrastructure will be permanently followed and monitored, using specific methodologies for identifying, tracking, and providing data on alerts and risk analyses [82] .

However, Belli et al. [83] emphasizes that for Brazil to become a digitally sovereign nation it is indispensable to create a digital sovereignty strategy based on cybersecurity and strategic investments. For this reason, in May 2023 a draft was published by the Institutional Security Cabinet providing for the creation of the PNCiber. This draft was extensive, more so than the Decree that was published, and its content addressed the need to unify the "patchwork quilt" of the Brazilian reality of cybersecurity regulation [84] .

79. Decreto n. 9.319, de 21 de março de 2018. (2018). Establishes the National System for Digital Transformation and sets out the governance structure for implementing the Brazilian Digital Transformation Strategy. Brasília, DF.

80. Ibid.

81. BRASIL. Decreto nº 11.200, de 30 de setembro de 2022. Provides for the regulation of public policies. Diário Oficial da União: Brasília, DF. Available at: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm#:~:text=DECRETO%20N%C2%BA%2011.200%2C%20DE%2015,de%20Seguran%C3%A7a%20de%20Infraestruturas%20Cr%C3%ADticas. Accessed: June 01, 2024.

82. Ibid.

83. BELLI, Lucca; Bakonyi Erica; Chen Larissa, et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. Rio de Janeiro: *FGV Direito Rio,* 2023, p. 13.

84. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. *Brasil contemporâneo*. São Paulo, v. 29., 2024. p. 9.

Therefore, the PNCiber emerged with the aim of guiding national cybersecurity activities through the establishment of governance methods, guidelines, and actions directed at cybersecurity in Brazil [85] . The principle-based part of the 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 [86] .

As already stated, the LGPD itself previously corroborated the protection of civil society's fundamental rights in the use of the internet by establishing practices to be adopted by all those who process users' data [87] . Thus, the policy under discussion reaffirmed the importance of protecting users' fundamental rights, while also being concerned with the need to maintain national sovereignty, technological education, and cooperation across all layers of society [88] .

Among the Policy's own objectives, the following stand out: preventive actions focused on training and educating society in general; fostering scientific research, technological development, and innovation on the theme of cybersecurity; the need for coordinated action and the exchange of cybersecurity information among the three branches of government (Legislative, Executive, and Judiciary), among the federative entities (States, the Union, Municipalities, and the Federal District), between the public and private sectors, and among society in general [89] . In other words, the PNCiber has a strong focus on incident prevention actions, not only for training public officials and private organizations but for society in general, promoting education and technical training as ways of equipping society with knowledge of cybersecurity [90] .

Thus, the PNCiber establishes principles and objectives and also institutes, in its Article 5, the National Cybersecurity Committee (CNCiber) to promote

85. PINHEIRO, Patricia P.G. Cibersegurança, Sociedade e Futuro . Computação Brasil, [S. l.], pp. 67-70, June 1, 2024. p. 69.

86. Decreto n. 11.856, de 26 de dezembro de 2023. (2023). Establishes the National Cybersecurity Policy and the National Cybersecurity Committee . Brasília, DF.

87. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD) . Diário Oficial da União. Brasília: Presidency of the Republic. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709. htm. Accessed: Nov. 07, 2023.

88. Decreto n. 11.856, de 26 de dezembro de 2023. (2023). Establishes the National Cybersecurity Policy and the National Cybersecurity Committee. Brasília, DF.

89. Ibid..

90. Ibid..

the unification of measures in this field [91] . Pinheiro [92] highlights that the influence 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 the CNCiber. This committee aims to implement, foster, and update the measures provided for in the National Policy, since cybersecurity needs to be continuously adapted and readapted through the application of ethical principles of development and the adoption of preventive measures [93] . The Committee, therefore, has the competence to evaluate and propose measures on the subject of cybersecurity in Brazil, to formulate proposals for the prevention of cyber incidents, to foster education and dialogue on cybersecurity, and to pursue international cooperation in this field [94] .

However, it is important to point out that the draft that provided for the creation of the PNCiber did not address the main instruments that already existed, such as the PNSI and the E-Ciber, and proved to be silent on vital points for implementing governance measures for Brazilian cybersecurity. This is a symptom of the current Brazilian legislative reality in cybersecurity, which is numerous and awash with scattered laws and decrees, but not necessarily guiding, clear, and objective [95] .

In other words, this shows that current legislation is still not able to expressly relate the regulatory contents to one another in pursuit of a common objective [96] , evidencing the importance of the advent of the PNCiber, which brought with it a new direction for rapid and coordinated action among all those responsible, with a guiding bias toward cybersecurity in Brazil, based on guidelines and methods of governance and risk management [97] . It is certain that any diagnosis of the National Cybersecurity Policy is still immature, given its recent publication, but it can already be observed that it seeks to achieve a standardization of action in the Brazilian cybersecurity scenario, assigns responsibilities to competent bodies and entities, and fosters social education and preventive actions against cyber incidents.

91. Ibid..

92. PINHEIRO, Patrícia P.G. Cibersegurança, Sociedade e Futuro . Computação Brasil, [S. l.], pp. 67-70, June 1, 2024. p. 68.

93. Ibid. p. 69.

94. Decreto n. 11.856, de 26 de dezembro de 2023. (2023). Establishes the National Cybersecurity Policy and the National Cybersecurity Committee . Brasília, DF.

95. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. *Brasil contemporâneo*. São Paulo, v. 29., 2024. p. 11.

96. Ibid.

97. PINHEIRO, Patrícia P.G. Cibersegurança, Sociedade e Futuro. Computação Brasil, [S. l.], pp. 67-70, June 1, 2024. pp. 69-70.

Final Considerations

From all that has been set out, it is possible to understand that there is no ready-made recipe to follow in the scope of cybersecurity and data protection that can be applied indiscriminately and that will ensure a scenario of full digital security, not least because, given constant technological development, the assessment and management of digital risks has become an almost uninterrupted practice. However, general action must start from making the layers of society aware of the need to follow basic cybersecurity precepts, knowing how to properly identify what a risk is, how to mitigate it, and which fundamentals must be observed, as well as legislative mandates, when handling and storing data, so that we do not fall into a high-risk scenario, with greater vulnerability of the 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. It runs from the enactment of the Brazilian Internet Civil Rights Framework (Marco Civil da Internet)—which this year completes its first decade in force—to the LGPD, which acted as a true milestone in data protection nationally, and on to the publication of the Decrees in the field of cybersecurity, as already mentioned throughout the third chapter, which culminated in the publication of the PNCiber. That is, measures that seek, broadly speaking, to standardize procedures, to raise awareness in the public and private spheres of the need for professional training, of the importance of joining the efforts of all those involved in the subject, and of the urgency of adopting predictive measures, in addition to bringing to civil society the idea of a pressing acculturation and education about everyday internet use, including with preventive actions for cybersecurity and the protection of their data, but which must be put into practice with a focus on the true protection of rights rather than on mere procedural and regulatory compliance.

For us to reach a more comfortable scenario in terms of cybersecurity, it is essential that the public itself be aware that a real and imminent threat exists, since it falls 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 containment of existing risks. It is no accident that the entire Brazilian regulatory framework mentioned throughout this work contains provisions on promoting user education and training. In addition, evident

is the continuing need for the development of legal mechanisms, since they actively contribute to preventing digital security incidents, as well as concern with the real application of risk analysis by those responsible, going beyond the sphere of mere regulatory compliance.

Today we are able to see cybersecurity as an international agenda, which seeks to mitigate the risks inherent in its use and which, as a result of technology, cross borders and reach a range of disciplines, with serious economic, political, legal, and social impacts in the mitigation of fundamental rights. Thus, cybersecurity is only one of the layers of internet governance, which is concerned with technological, political, and legal norms and rules; moreover, it is a continuous, multidisciplinary process. In short, the significant changes brought about by the sharp increase in internet use in the twenty-first century produced important transformations in human interactions and implied the need to adapt the concept of risk and global regulation for the protection of users' data, guaranteeing support in case of incidents, attribution of responsible parties, and measures to be adopted continuously to mitigate digital risks capable of causing serious harm to civil society and to the public sector and private organizations.

Undeniable is 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 ensure the application of good practices and preventive actions against possible incidents and to provide effective protection of fundamental rights. Finally, we cannot forget the need for risk assessment to be carried out in a manner faithful to the protection of those who are inherently most vulnerable, the data subjects, preventing a fall into an unfair distribution of these risks to society, which can cause social disasters and injury to users' basic rights.

References

ALMEIDA, João Emílio de. Cibersegurança: da prevenção do risco à gestão de incidentes. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação , Porto, no. 43, pp. 1-4, Sept. 30, 2021. DOI 10.17013/risti.43.1-4. Available at: https://scielo.pt/pdf/rist/n43/1646-9895-rist-43-1.pdf. Accessed: May 2, 2024.

BECK, Ulrich; SEBASTIÃO NASCIMENTO. *Sociedade de risco: rumo a uma outra modernidade*. São Paulo: Editora 34, 2011.

BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B. Cibersegurança : Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. 1st ed. Rio de Janeiro: Rio de Janeiro: FGV Direito Rio, Aug. 2023. Available at: https://direitorio.fgv.br/publicacao/ciberseguranca-u- ma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil. Accessed: June 24, 2024.

BITTAR, E. C. B. A Teoria do Direito, a Era Digital e o Pós-Humano: o novo estatuto do corpo sob um regime tecnológico e a emergência do Sujeito Pós-Humano de Direito. Revista Direito e Práxis , v. 10, no. 2, pp. 933–961, June 2019.

BRAGA, Noelson Araújo. CIBERSEGURANÇA E O DIREITO À PRIVACIDADE : Um Estudo sobre a construção cibernética no Brasil e União Europeia na ótica realista. 2021. Monograph (Bachelor's in International Relations) - UNIVERSIDADE DE BRASÍLIA INSTITUTO DE RELAÇÕES INTERNA- CIONAIS, [S. l.], 2021. Available at: https://bdm.unb.br/bitstream/10483/30829/3/2021_Noelso- nAraujoBraga_tcc.pdf. Accessed: July 3, 2024.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 2016. 496 pp. Available at: planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed June 01, 2024.

BRASIL. Lei 10.406, de 10 de janeiro de 2002. Establishes the Brazilian Civil Code. Diário Oficial da União . Brasília: Presidency of the Republic. Available at: planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Accessed Jan. 05, 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Establishes principles, guarantees, rights, and duties for the use of the Internet in Brazil. Diário Oficial da União . Brasília: Presidency of the Republic. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed: June 07, 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Brasília: Presidency of the Republic. Available at: https://www.planalto. gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed: Nov. 07, 2023.

CRIMINOSOS vendem dados do CGU e Ministério da Saúde na dark web. [S. l.], Dec. 21, 2021. Available at: https://canaltech.com.br/seguranca/criminosos-vendem-dados-do-cgu-e-minis- terio-da-saude-na-dark-web-204985/. Accessed: June 27, 2024.

Decreto n. 9.319, de 21 de março de 2018. (2018). Establishes the National System for Digital Transformation and sets out the governance structure for implementing the Brazilian Digital Transformation Strategy . Brasília, DF.

Decreto n. 10.222, de 5 de fevereiro de 2020. (2020). Approves the National Cybersecurity Strategy . Brasília, DF.

Decreto n. 10.046, de 30 de setembro de 2019. Amends Decree No. 9.203 of November 22, 2017, which regulates Law No. 13.334 of September 13, 2016 . Diário Oficial da União, Brasília, Oct. 1, 2019. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/ d10046.htm. Accessed: June 01, 2024.

Decreto n. 10.641, de 2 de março de 2021. (2021). Amends Decree No. 9.637 of December 26, 2018, which establishes the National Information Security Policy and provides for information security governance, and amends the, 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.

Decreto n. 11.200, de 15 de setembro de 2022. (2022). Approves the National Critical Infrastructure Security Plan . Brasília, DF.

Decreto n. 11.856, de 26 de dezembro de 2023. (2023). Establishes the National Cybersecurity Policy and the National Cybersecurity Committee . Brasília, DF.

FICHTNER, Laura. What kind of cyber security? Theorising cyber security and mapping approaches. Internet Policy Review , Germany, v. 7, pp. 1-19, May 15, 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: June 3, 2024.

G1. STJ aciona PF para apurar possível ataque de hackers ao sistema do tribunal. G1 , Nov. 4, 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: July 2, 2024.

G1. O que são cookies na internet e como eles funcionam. G1, June 09, 2024. Available at: https://g1.globo.com/tecnologia/noticia/2024/06/09/o-que-sao-cookies-na-internet-e-como- -eles-funcionam.ghtml. Accessed: June 24, 2024.

GIDDENS, A.; PLÍNIO DENTZIEN. *Modernidade e identidade*. Rio De Janeiro, Rj: Jorge Zahar, 2002.

GOLDONI, L. R. F.; RODRIGUES, K. F.; MEDEIROS, B. P. Qual é o futuro da governança de cibersegurança no Brasil? Cadernos Gestão Pública e Cidadania , v. 29, p. e90972–e90972, Apr. 17, 2024.

GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados . PALHARES, Felipe (Ed.). São Paulo: Thomson Reuters Brasil, 2020, pp. 245-271.

LATTO, Nica. O que é um vírus de computador? [S. l.], Feb. 12, 2020. Available at: https://www.avast.com/pt-br/c-computer-virus#:~:text=Um%20v%C3%ADrus%20de%20computador%20%C3%A9,a%20outros%20arquivos%20ou%20documentos. Accessed: July 17, 2024.

LHUMANN, Niklas. Risk: A sociological Theory. 1st ed. New York: [s. n.], 2017. Available at: https://www.researchgate.net/publication/345677301_Risk_A_Sociological_Theory. Accessed: June 8, 2024.

LINKNACIONAL. O que é spam? Link Nacional, Oct. 20, 2023. Available at: https://www.linknacional.com.br/blog/o-que-e-spam/. Accessed: June 24, 2024.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement. Revista do Programa de Direito da União Europeia, [S. l.], pp. 1-14, Mar. 15, 2021.

LÓSSIO, Cláudio Joel Brito. O compliance digital e a proteção de dados: preservando direitos na sociedade da informação. Dissertation (Master's in Law) - Universidade Autônoma de Lisboa

Luís de Camões, Lisboa, 2020. Available at: https://repositorio.ual.pt/handle/11144/4621. Accessed: July 10, 2024.

LUCCA, Newton de. Dignidade da pessoa humana e os riscos eletrónicos. Galileu - Revista de Direito e Economia , [s. l.], v. 7, pp. 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: July 17, 2024.

MARCON, Daniele Verza. Seguro contra Riscos Cibernéticos : desafios para delimitar a garantia e promover a cibersegurança na era digital. 2023. Dissertation (Master's 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: July 3, 2024.

MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. Panorama Setorial da Internet , [S. l.], year 11, no. 2, pp. 1-20, June 2019. Available at: https:// www.nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_priva- cidade_e_dados_pessoais.pdf. Accessed: July 2024.

PIMENTEL, José Eduardo de Souza. Introdução ao Direito Digital. Revista Jurídica da Escola Superior do Ministério Público de São Paulo, v. 13, no. 1, pp. 16–39, Sept. 17, 2018.

PINHEIRO, Patricia Peck Garrido. CIBERSEGURANÇA, SOCIEDADE E FUTURO. Computação Brasil, [S. l.], pp. 67-70, June 1, 2024.

Problemas no ConecteSUS: antes de ataque hacker, sistema teve polêmica com alteração de dados e falhas. Available at: <https://g1.globo.com/saude/noticia/2021/12/10/problemas-no-conecte-sus-antes-de-ataque-hacker-sistema-teve-polemica-com-alteracao-de-dados-e-falhas.ghtml>.

SAMPAIO, Dhiêgo Rhubens Lima. UM ESTUDO SOBRE RISCOS DE SEGURANÇA DA INFORMAÇÃO NO CAMPUS DA UFC EM QUIXADÁ COM BASE NA NORMA ISO/IEC 27005 . 2014. Monograph (Bachelor's in Information Systems) - Universidade Federal do Ceará, Quixadá, CE, 2014. Available at: https://repositorio.ufc.br/handle/riufc/25039. Accessed: June 7, 2024.

SHIRA, Fer; JANCZ, Carla. BARRICADAS ESTRATÉGIAS E COLETIVIDADE: Uma cartilha de segurança digital para organizações. Marialab , São Paulo, Dec. 1, 2022. Available at: https://www.marialab.org/wp-content/uploads/2020/12/Barricas-estrategias-coletividade.pdf. Accessed: July 13, 2024.

Tribunal de Contas da União. Cinco controles de segurança cibernética para ontem / Tribunal de Contas da União. – Brasília: TCU, 2022. 36 pp. Available at: https://portal.tcu.gov.br/5-controles- - de-seguranca-cibernetica.htm. Accessed: July 06, 2024.

TEFFÉ, Chiara de. Dados Pessoais Sensíveis: Qualificação, Tratamento e Boas Práticas. Indaiatuba, SP: Foco, 2022. 304 pp. Available at: https://www.google.com.br/books/edition/Dados_Pes- soais_Sens%C3%ADveis/atCLEAAAQBAJ?hl=ptBR&gbpv=1&dq=inauthor: %22Chiara+Spadac- cini+de+Teff%C3%A9%22&printsec=frontcover. Accessed: June 28, 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

17

Cyberchildhood and social cybersecurity: in search of better protection for children and adolescents on the internet

LÍGIA MARIA DE SOUZA LOPES REIS

Contents: Introduction. 1. General overview: context and data. 2. Regulatory framework. 2.1. Differentiated data collection. 2.2. Excessive exposure. 3. Future outlook. 3.1. Digital cybersecurity and the regulatory future. Final considerations. References

Introduction

This article aims to analyze how Brazil has advanced in building a regulatory framework intended to protect children and adolescents in digital environments, seeking to shed light on possible normative contributions to improving social cybersecurity. Drawing on a study of Laws 12.965/2014 (Brazilian Internet Civil Rights Framework) and 13.709/2018 (General Personal Data Protection Law), it presents the advances, gaps, and impacts of these regulations on the use of digital platforms by these groups. In addition, it seeks to understand the Brazilian Bill 2628/2022 and the American legislative proposal Kids Online Safety Act (Kosa) , analyzing whether they really 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. General overview: context and data

Brazilian children and adolescents have been accessing the internet at ever younger ages. According to TIC Kids Online Brasil 2023 [2] , 24% of the country's children and adolescents report having started to use the World Wide Web in early childhood, that is, by the age of six [3] . Added to this is another alarming finding. A study conducted by Nielsen [4] , at the request

1. Communications specialist with a master's degree in Communication Regulatory Policies from the Universidade de Brasília (UnB). Specialist in International Relations from UnB and in Public Administration from the Escola Nacional de Administração Pública (Enap). Federal civil servant at the Conselho Nacional do Ministério Público da União (CNMP) since 2011, seconded to the Supremo Tribunal Federal (STF). Currently pursuing a postgraduate degree in Digital Law (a partnership between the Instituto de Tecnologia e Sociedade do Rio and the Centro de Estudos e Pesquisas em Direito da Universidade do Estado do Rio de Janeiro) and an undergraduate degree in law.

2. Conducted by the Regional Center for Studies on the Development of the Information Society (Cetic.br), of the Brazilian Network Information Center (NIC.br), linked to the Brazilian Internet Steering Committee (CGI.br), since 2012. For the 2023 edition, the survey interviewed, in person, 2,704 children and adolescents aged 9 to 17, in addition to their parents or guardians, across the entire national territory in 2022.

3. NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2023 [e-book]. ed. São Paulo: Comitê Gestor da Internet do Brasil, 2024.

4. American company that carries out global audience measurement, data collection, and analysis of traditional and digital media to assess trends and behaviors.

from Google, reveals low adoption of parental controls [5] by parents and guardians in Brazil, where they have been guaranteed under the country's regulatory framework since the enactment of Law No. 12.965/2014. In 2023 [6], only 17% of the adults surveyed knew about and used technological means of access control.

Unsupervised online browsing, low literacy, and scant awareness among these users involve countless risks, some of which have already been mapped by specialists, such as excessive data collection, overexposure of one's image, and encouragement of consumption. These actions affect users who lack the necessary digital skills, such as knowledge of rights and cybersecurity tools [7], something essential for conscious and defensive use of networks. After all, children and adolescents are people in formation and, for that reason, are afforded specific constitutional protection in Brazil, set out in Article 227 of the CRFB. The text reads:

> It is the duty of the family, society, and the State to ensure to children, adolescents, and young people, with absolute priority, the right to life, health, food, education, leisure, professional training, culture, dignity, respect, freedom, and family and community life, in addition to protecting them from all forms of negligence, discrimination, exploitation, violence, cruelty, and oppression [8].

In an attempt to address the effects caused by the acceleration of contemporary changes, the public authorities have issued regulations aimed specifically at the digital environment, such as Law No. 12.965/2014, better known as the Brazilian Civil Rights Framework for the Internet (MCI), and Law No. 13.709/2018, dubbed the General Data Protection Law (LGPD), to cite just a few [9]. To these measures is added the work 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 bases that authorize the processing of data of children and adolescents. Despite these efforts, inconsistencies and paradoxes can be observed.

5. Parental control is a mechanism used by adults to control the access that children may have to different websites, operating systems, or computers. Through it, 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. BRASIL. Constituição Federal, art. 227, *caput*.

9. In January 2024, Law No. 14.811/2024 was enacted, whose purpose is to protect children and adolescents against violence, especially in educational or similar settings. The law includes specific measures aimed at increasing the safety of younger people in virtual environments, inasmuch as it adds new provisions on digital crimes against these groups to the Penal Code.

According to the Global Digital Report 2024 [10], Brazil ranks second among countries in the share of users over 16 who spend the most time online and fifth worldwide in Instagram use. The behavior of older users is reproduced by younger ones: in addition to starting their digital lives ever earlier, Brazilian children under 13 prefer TikTok [11].

The finding is surprising, since this social network is rated 12+ years in the stores that provide the app for download. And that limit is by no means an arbitrary cutoff. Under the Child and Adolescent Statute (ECA), a child is any person under twelve years of age, and from that age up to 18 completed years, the person is considered an adolescent.

The use of social networks by children and adolescents has grown notably 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 networks, an increase of ten percentage points compared with 2019, when 68% was recorded. By way of comparison, a study conducted in the United Kingdom in 2021 by Ofcom—an acronym for The Office of Communications [12]—indicated that 33% of children aged 5 to 7 have their own social media profiles. That figure 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

Saying that the internet is not regulated in Brazil is an untruth and reflects ignorance. The fact is that different rules apply to the digital environment, such as the LGPD and the MCI. Depending on the subject matter, other rules may reach the digital environment, such as the one dealing with copyright. In the case of the rights of children and adolescents, an important set of regulations can be invoked to protect them.

2.1 Differentiated data collection

The advance of the twenty-first century and of new communication technologies 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 TIC Kids Online Brasil 2023, this is the preferred social network of 46% of respondents aged 11 to 12 (CETIC.BR, 2023).

12. This is the communications regulatory agency of the United Kingdom, whose cited content can be found at https://bit.ly/Ofcom2024.

but also altered people's behavior, including that of children.

Living in an increasingly digital world, younger people have found in digital networks, online games, and streaming platforms other ways of entertaining, informing, and amusing themselves, different from those sought by their parents. Also according to TIC Kids Online Brasil 2023, 95% of the population aged 9 to 17 declared themselves internet users 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 [13].

With regard to data collection on the internet, the General Data Protection Law can be understood as a general and cross-cutting norm, which runs across different processing agents and affects various categories of data subjects, among them those who require special regulation and protection—children and adolescents. The combination of Articles 5, items X and LXXIX, and 227 of the CRFB with Article 17 of the ECA gave rise to a chapter of the LGPD devoted entirely to these groups.

Law No. 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 calls for reflection on the vulnerability of children and adolescents and the need for care on the part of the family, society, and the State (Art. 227, caput, of the 1988 Federal Constitution, combined with Art. 4 of the ECA). This general law also establishes that the controller [14], when collecting data from these groups, shall act

> only through practices that promote and protect their rights, as provided in the national and international legal system, with absolute priority, refraining from practices that exploit the vulnerability of children and youth, including commercial ones [15].

The best interest must be respected in the context of personal data protection, since this guarantee relates to personality rights. Thus, "its indiscriminate use [data collection] is capable of objectifying people, affecting the development of personality, promoting manipulation

13. NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2023 [e-book]. ed. São Paulo: Comitê Gestor da Internet do Brasil, 2024.

14. A natural or legal person, governed by public or private law, who is responsible for decisions concerning the processing of personal data, as stated in Article 5, item VI, of the LGPD.

15. HENRIQUES, I.; PITA, M.; HARTUNG, P. Proteção de dados pessoais e a vulnerabilidade infantil. São Paulo: Editora ABC, 2022, p. 213.

and generating discrimination” [16]. And, when the risks involve the foundational stages of human development,

> the issue must also be addressed taking into account the special legal protection afforded to children and adolescents, whose rights must, by constitutional mandate, be ensured with absolute priority [17].

The LGPD further requires that the processing of children’s personal data be carried out with the specific and prominent consent given by at least one of the parents or the legal guardian (Art. 14, § 1). Legal scholars explain that parental consent must be given as a free, informed, and unambiguous expression and must also meet the principle of purpose, as established in Art. 5, XII, of the law, “regardless of whether it is given by mothers, fathers, or legal guardians” [18].

There are only two situations in which the personal data of children and adolescents may be processed without the consent of at least one of the parents or the 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 a matter of protecting 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).

That same general law also establishes that the controller has the duty to make all reasonable efforts to verify that consent was given by the person responsible for the child, taking into account available technologies (Art. 14, § 5). In addition, this processing agent must keep public the information on the types of data collected, the way they are used, and the procedures for the full exercise of these data subjects’ rights (Art. 14, § 2), which meets the principles of transparency and purpose, since it gives them full awareness of the procedures and uses of what belongs to them, namely, their data.

Because these are people in formation, information on data processing must be provided in a simple, clear, and accessible manner, taking into account the physical-motor, perceptual, sensory, intellectual, and mental characteristics of the user. Audiovisual resources must be used when

16. MENDES, SARLET, RODRIGUES JR. Tratado de Proteção de Dados Pessoais. 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 be suited to the child's understanding (Art. 14, § 6). Moreover, controllers must not condition the participation of children and adolescents in games, internet applications, or other activities on the provision of personal information beyond what is strictly necessary for the activity (Art. 14, § 4).

With regard to the rights of data subjects, set out in Article 18 of the LGPD and which also extend to this group, five of the nine items listed in the norm stand out: 1) confirmation of the existence of processing, for the complete and unambiguous awareness of at least one of the parents or the legal guardian; 2) correction of incomplete, inaccurate, or outdated data, especially considering the development of the data subject; 3) anonymization, blocking, or deletion of unnecessary or excessive data or data processed in noncompliance with the LGPD, in view of the transitory nature of the relationship; 4) deletion of personal data processed with the consent of the data subject; and 5) information about the possibility of not giving consent and about the consequences of refusal.

The exercise of these rights must be aligned with the principles of the LGPD, of which five of the ten set out in the law are listed here, 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 at legitimate, specific, and explicit purposes informed to the data subject, with no possibility of further processing in a manner incompatible with those purposes; 3) necessity, which refers to limiting processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportionate, and not excessive in relation to the purposes of the data processing; 4) transparency, that is, the guarantee offered to data subjects of clear, precise, and easily accessible information about the processing and the respective processing agents, subject to commercial and industrial secrecy; and 5) responsibility and accountability, referring to the demonstration, by the agent, of the adoption of effective measures capable of proving observance and compliance with personal data protection rules and, moreover, the effectiveness of those measures.

It is worth noting that the most current scholarship advocates stricter rules for the management of these groups' personal data.

> Restrictive interpretations, which make the protection of children's data equivalent to 'consent to data processing,'

> relieve States, companies, and other organizations of responsibility for the harmful use of personal data and privacy violations. There is a power imbalance between the efforts of data collectors to capture larger amounts of data and the ability of families and children to protect themselves in an increasingly complex digital world [19].

2.2 Excessive exposure

The uncontrolled exposure of children to social networks generates phenomena and behaviors that call for reflection. One of them is preference profiling, which, in a few words, means the offering of content and products according to the user's browsing on the platform. Another is the risk of isolating this person, still in formation, in discussion bubbles, which can contribute to worsening social and political polarization, reduced diversity of opinions [20], increased intolerance, the spread of disinformation, among other social effects.

> Far beyond improving existing economic strategies, such as classification and profiling and targeting marketing, the data processed have implications that can lead to a complete transformation of the economic, social, and political landscape [21].

The unsupervised presence of these users, lacking educational tools and skills for reflection and critical thinking, can mean opening virtual doors to criminals. There are already records of new methods, such as "digital kidnapping," which is what occurs when someone steals photos of children from the internet and posts them as if they were their own children. Ten years ago, these crimes had not yet become issues to be addressed when the first and principal legal instrument aimed at the internet, the Brazilian Civil Rights Framework for the Internet (MCI), was enacted. Not that it should have dealt with crimes, since the MCI is a regulation of civil relations, as can be inferred. However, it is the first Brazilian law specific to the internet and, as such, could have looked more closely to the future, which necessarily involves the safeguarding 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 that circulates on social networks and is distributed by algorithms. These are products considered to be of low quality, in terms of both content and pedagogy, and that contain biases and little diversity.

21. FRAZÃO, A. In: FERNANDES, E.; TEFFÉ, C. S. de; BRANCO, S. (Coords.). Privacidade e Proteção de Dados de Crianças e Adolescentes. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021, p.87.

protection of the lives and development of children and adolescents. But that is not what one sees in the text.

Law No. 12.965/2014 is the first piece of legislation to establish principles, guarantees, rights, and duties for the use of the internet in Brazil. It consists of 32 articles and is structured into five chapters, but none is devoted specifically to children, as in the LGPD. Nevertheless, 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 fulfillment of the State's constitutional duty to provide education, at all levels of schooling, 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 nude scenes. And not by reason of the literal wording of the norm, but as a result of interpretation, since in these cases the ECA applies together with Article 21 of the MCI [22]. Case law considers that any dissemination of images of children and adolescents in situations of nudity or with sexual connotation constitutes a serious crime, as provided in Article 241-A of the ECA. It also holds that the internet provider is responsible for removing 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) [23].

> An application provider that, after being notified, fails to remove offensive content involving a minor is civilly liable, regardless of a court order, because the principle of full protection of children and adolescents prevails over the Brazilian Civil Rights Framework for the Internet [24].

Another provision worth mentioning is Article 19, whose constitutionality analysis awaits judgment within the scope of Extraordinary Appeal (RE)

22. The text states that the provider of internet applications that makes third-party-generated content available shall be held subsidiarily liable for the violation of privacy resulting from the disclosure, without the participants' authorization, of images, videos, or other materials containing nudity or private sexual acts when, after receiving notification from the participant or their legal representative, it fails to diligently take steps, within the scope and technical limits of its service, to make that content unavailable.

23. See Jurisprudência em Teses, Edition No. 224. Available at https://bit.ly/3WdtIVO. In addition, it is worth noting that, according to the STJ, the pornographic exposure without consent set out in the Brazilian Civil Rights Framework for the Internet is not limited to total nudity, nor to sexual acts that involve only sexual intercourse, but extends to conduct that may cause harm to the victim's personality.

24. The text refers to the following provisions: Article 19 of Law No. 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 Supreme Federal Court (STF) [25]. 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 arising from content generated by third parties if, after a specific court order, it fails to take steps to make the content identified as infringing unavailable, within the scope and technical limits of its service and within the time period set, subject to legal provisions to the contrary. This legal basis treats the provider's liability as fault-based, assessing it by its omission when it does not take the offending content down after due judicial notification. It is worth recalling that the STJ has already held that "the liability of internet application providers for third-party-generated content is fault-based and becomes joint and several when, after judicial notification, removal of the offending material is refused or delayed" [26].

With regard to the protection of the groups studied here and the literal text, the MCI says that the user will have the option of freely choosing to use a computer program on their terminal to exercise parental control over content they consider inappropriate for their minor children, provided the principles of the ECA are respected (Law No. 12.965/2014, Art. 29). Considering that only 17% of all parents surveyed in the aforementioned Nielsen study [27] declared that they know and use technological means of access control as a way of making minors' experience safer, this provision alone seems insufficient to meet the challenges posed to childhood and youth in today's reality.

Finally, it should be noted that the term "child" appears only twice in the MCI and occurs only in the final provisions—almost as if, at last, the legislator had remembered to look to tomorrow. According to the text, it falls to the public authorities, together with connection and internet application providers and civil society, to promote education and provide information on the use of the computer programs provided for in the caput of Article 29, as well as to define good practices for the digital inclusion of children and adolescents. A text as principle-based as it is vague, as can be seen.

25. This is RE 1.037.396, Theme 987 of general repercussion, with Justice Dias Toffoli as rapporteur, which discusses whether Article 19 of the Brazilian Civil Rights Framework for the Internet is constitutional or not. That article requires that a specific court order be issued before websites, internet providers, and social media applications can be held liable for harmful content posted by other people.

26. See Jurisprudência em Teses, Edition No. 222. Available at https://bit.ly/3RUyDYR

27. See comment in footnote No. 3.

3. Future framework

As seen, Brazil has rules for the protection of 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 the groups and the social structures. From this perspective, we turn to regulatory innovations.

3.1 Digital cybersecurity and the regulatory future

One of the most consensual conceptualizations of cybersecurity was developed by the Telecommunication Standardization Sector of the International Telecommunication Union of the UN, known by the 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, assurances, and technologies that can be used to protect the assets of the cyber environment, of the organization, and of users [28]. ã

Thus, when understood from technical aspects, cybersecurity refers to the protection of computers, networks, and software applications and operating systems against possible digital threats. However, when interpreted from other fields, such as the applied social sciences [29], the term can include meanings that encompass measures to defend countries' sovereignty (including digital sovereignty), respect for fundamental human rights, and impacts on people's well-being and mental health.

Social cybersecurity would thus be an emerging field that arises in response to digital threats and the challenges of cybersecurity, focused on

> characterizing, understanding, and forecasting changes in human behavior and in social, cultural, and political outcomes mediated by cyber environments; and building a social cybersecurity infrastructure that allows the essential character of a society to persist in an information environment mediated by cyber means, 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 merely a technical issue and recalls that the topic is highlighted in different parts of EU legislation, including the new Artificial Intelligence Act (AI Act) and various other laws 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 broad collaboration is needed among technical experts, lawyers, and other social scientists in order to understand the topic. Available at https://encurtador.com.br/o6D0u

real or imminent social cybersecurity, and cyber-mediated threats [30].

It 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 [31]. From this, social cybersecurity has objectives geared toward anticipating phenomena, such as 1) characterizing, understanding, and forecasting technology-mediated changes in human behavior and in social, cultural, and political dynamics and 2) building a social cyber infrastructure (emphasis added) that allows society to preserve its essential character in a technology-mediated information environment [32].

Another meaning considers cybersecurity as a broad field of study that encompasses others, in addition to including essential dimensions such as oversight and governance, research, operation and maintenance, protection and defense, also dedicated to the protection of life, property, and information security, as argued by Aguilar and Fonseca [33].

In studying technological impacts in the school context, the authors advocate a broader understanding of and training in cybersecurity, focused on the conscious and healthy use of the internet, especially in childhood and adolescence.

This conceptual broadening is what enables the instructional, informed, and coordinated action of fathers and mothers, the school community, and other members of the context. It is based on teaching and appropriation of guidelines for network use and security, 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, whether theoretical, scientific, and technological, or

30. BESKOW, D. M.; CARLEY, K. M. Social cybersecurity: an emerging science. 2019, p. 1. The original English text reads as follows: "As noted by the National Academies of Science NAS (2019): Social cybersecurity is an applied computational social science with two objectives - 'characterize, understand, and forecast 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 cyber-threats, and cyber-mediated threats'".

31. *Idem,* p.3.

32. Ibid.

33. ASTORGA-AGUILAR, C.; SCHMIDT-FONSECA, I. Peligros de las redes sociales: Cómo educar nuestros hijos e hijas en ciberseguridad. Educare [online], vol. 23, no. 3, pp. 339-362, 2019. Epub Oct. 30, 2019.

> those provided by the groups participating in the process and by society itself. In relation to teaching and knowledge, it is necessary that children and adolescents acquire knowledge about cybersecurity as applied to social networks, but, above all, that they appropriate and internalize this learning, so that this information passes into their cognitive structures, in order to identify dangers on the network [34].

According to The Global Risk Report 2024 - 19th edition [35], cyber risk will be the fourth-greatest threat to countries over the next two years and the eighth over 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, counter, and measure (or assess) the impact of communication objectives” 36. , making it possible even to draw on it to analyze and promote safer and healthier digital environments for children and adolescents.

That is why governments around the world are increasingly interested in developing national cybersecurity strategies (NCSs) that are capable and effective in confronting and preventing, in an integrated and efficient manner, a wide range of issues related to the topic. According to the Organization of American States (OAS), developing an NCS is fundamental to dealing with cyber threats and building desirable measures to prevent them.[37] In Brazil, the national cybersecurity strategy, created in 2020, is under review and, at the eleventh hour 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 [38] techniques have exploited human vulnerabilities. Thus, this new area of research would respond to the cyber effects of the present

34. Idem. Free translation of the original text in Spanish: Los actores del proceso pueden trabajar con distintos tipos de conocimiento, tanto los teóricos, científicos y tecnológicos, así como los que aportan los grupos participantes del proceso y la sociedad misma. En relación con la didáctica y el conocimiento, se requiere que la niñez y la adolescencia obtengan conocimiento sobre ciberseguridad aplicada a redes sociales, pero que principalmente se apropien e interioricen con el aprendizaje, de manera que dicha información pase a sus estructuras cognitivas con el fin de identificar peligros en la red .

35. WORLD ECONOMIC FORUM. The Global Risks Report 2024 [e-book]. Cologny/Geneva: World Economic Forum, 2024.

36. BESKOW, D. M.; CARLEY, K. M. Social cybersecurity: an emerging science. 2019, p.2. The original text reads: “Social cybersecurity uses computational social science techniques to identify, counter, and measure (or assess) the impact of communication objectives” .

37. See the OAS cybersecurity program proposal at https://www.oas.org/ext/en/security/prog-cyber

38. Social engineering refers to the tactics used to manipulate people into revealing confidential information or taking actions that compromise security. Examples include phishing, pretexting, and other forms of deception aimed at influencing human behavior. More information at https://bit.ly/3L8IIh8

day, drawing on 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 operations of influence and manipulation of beliefs, behaviors, and public trust take place within digital platforms, and how social groups can be defended against them. Methods and results arising from this research domain can be critical for policymakers and scholars, insofar as their applied theoretical components have the potential to develop into analyses of high-dimensional networks [39] , machine learning, natural language processing, and agent-based simulation [40] .

Along these lines, Wu et al . define social cybersecurity as a field that studies security and privacy behaviors and threats in an ecosystem of interconnectivity and social influence, recognizing the domain of social interactions and seeking to create security systems that are more closely aligned with users' social practices and needs. Among other issues, they explain that families and households exhibit complex practices when it comes to sharing content, including that of their children. They also explain that conceptions of what is sensitive or not vary among families, which likewise diverge on access control mechanisms for combating violations that affect the sensitive information of children and adolescents [41] .

> However, users frequently adapt their ideal access control policies iteratively rather than conform to the ones initially reported, suggesting that access control policies, a priori , may be insufficient in the household context [42] .

39. High-dimensional network analyses are techniques and methods 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 an ordinary social network), but consider multiple layers of data and types of interactions, in addition to their complexities and dimensionalities. They rely on mathematical models and algorithms and can be applied to social networks and cybersecurity.

40. In the field of regulation of emerging technologies, one example is the European AI Act, which mentions cybersecurity 45 times in its text. In one passage, the European authority states that Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, 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

41. U, Y. W.; EDWARDS, K.; DAS, S. SoK: Social Cybersecurity. In: 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022, pp. 1863-1879, p. 4. Here is the text in the original 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 rules can lead to inappropriate behaviors and reduce security, whereas designing for and harnessing human social behaviors in these contexts can mean greater effectiveness and performance of these systems and regulatory norms.

On this topic, Bill 2628/2022, authored by Senator Alessandro Vieira, is pending in the National Congress, proposing more protective measures for children and adolescents in digital environments. Among the proposed changes, the following stand out: the requirement that digital platforms adopt, by default, strict settings for data collection; the requirement that technology services aimed at children and adolescents offer simple and effective parental control mechanisms; the prohibition of reward boxes (loot boxes) in electronic games and of advertising aimed at children—which is already prohibited by the Consumer Protection Code, but the text restricts communication elements that may induce consumption; and the provision for 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, as well as possible interference with family autonomy.

Another example is the U.S. legislative proposal Kids Online Safety Act (Kosa), an unprecedented and historic proposal that advocates improving the online safety of children and adolescents by changing the design of platforms, something quite consistent with social cybersecurity. It also proposes not using algorithm-based recommendation systems and creating a new responsibility or a duty of care [43] for apps and digital platforms, specifically with regard to content inappropriate for minors.

Pending for more than two years in the U.S. Congress, the bill is divided between supporting forces in the Senate and significant opposition from human rights organizations and internet freedom advocacy groups. The amendments made to the bill sought to appease detractors but were not considered sufficient. Critics maintain that the law still presents

43. An 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 damage and that any harmful content or behavior is properly monitored and managed. This includes preventing abuse, protecting privacy, safeguarding against exploitation, and promoting a safe digital environment. The “duty of care” is also contemplated in Bill 2628/2022, insofar as it provides for more protective default settings, child monitoring, and the creation of mechanisms for reporting and removing content that violates the rights of children and adolescents without the need for a court order, among other things.

risks of censorship and excessive restrictions, especially for marginalized communities [44] . Opponents such as the Center for Democracy and Technology and the Electronic Frontier Foundation say they fear that the bill's vague language could lead to excessive content moderation and, consequently, harm vulnerable communities [45] , such as LGBTQ+ youth.

That said, Kosa can be considered an instrument of social cybersecurity, since it addresses both the 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) content and design regulation, 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, insofar as it proposes including guidance from a diverse council of actors, 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 the digital environment safely [46] ; and 3) protection against manipulation and disinformation, through the implementation of security mechanisms and the requirement that social networks adopt specific measures to protect young users.

Final Considerations

The growing integration of children and adolescents into the digital universe requires a transdisciplinary, multifaceted, and multidimensional approach that encompasses education, regulation, technology, cybersecurity, and other dimensions that make it possible to pave paths oriented toward protection and healthier, more humane digital experiences. This requires strengthening the regulatory environment, with specific rules, 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 specfic 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 the similarity between the proposal and Article 29, sole paragraph, of the Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet). The text states: "[i]t is incumbent upon the public authorities, together with internet connection and application providers and civil society, to promote education and provide information on the use of the computer programs provided for in the caput , as well as to define best practices for the digital inclusion of children and adolescents".

not only prohibit specific harmful practices, such as the excessive collection of their data and profiling carried out by algorithms, but also promote a digital culture more conducive to human development.

In light of this, although subject to criticism, regulatory innovations such as those proposed in Bill 2628/2022 and in Kosa can be seen as instruments of social cybersecurity, because they seek to address digital threats beyond technological issues. However, one must not lose sight of the fact that regulatory effectiveness will depend on the capacity for implementation and enforcement. Specific regulatory rules can certainly contribute to improving the protection of these groups in the digital environment, but they will surely need to be accompanied by measures, protocols, and policies that help develop connections and ecosystems favorable to the presence of young people.

Along these lines, the importance of collaboration among governments, educators, parents, and digital service providers in creating a safer and more enriching digital environment for children and adolescents must be emphasized —something set out in the Brazilian Civil Rights Framework for the Internet but not yet realized in Brazilian reality. As technology continues to evolve, so too must the understanding, means, and instruments for protecting people's well-being, especially that of the most vulnerable, such as children and adolescents. Only this coordination among those social agents can offer both the youngest and their families the security and trust necessary for digital experiences.

Integrating social cybersecurity into the debate on cyberchildhood is essential, because 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 ones, in addition to digital education initiatives that address the social nature of cyber threats. Educational programs that prioritize digital literacy and foster awareness of technological risks can positively reach other emerging challenges beyond digital networks, such as the use and applications of artificial intelligence.

Thus, it was observed that social cybersecurity, although an emerging field of research, should be studied and explored so as to formulate and propose a combination of lenses, concepts, approaches, and methods from the applied social sciences and computer engineering to build infrastructures

and social instruments that are more resilient, aware, and attuned to user behavior. As a result, it is possible to protect society and its groups more effectively, as well as to keep their dynamics and institutions free from (or less vulnerable to) technological risks.

References

ASTORGA-AGUILAR, C.; SCHMIDT-FONSECA, I. Peligros de las redes sociales: Cómo educar nuestros hijos e hijas en ciberseguridad . Educare [online], v. 23, no. 3, pp. 339-362, 2019. Epub Oct. 30, 2019. Available at: https://bit.ly/PeligrosRedes2019. Accessed: June 2024.

BRASIL. Constituição Federal . Available at: https://l1nk.dev/Qzkdl. Accessed: June 2024.

_____. Lei nº 12.965, de 23 de abril de 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. Accessed: June 2024.

_____. Lei nº 8.098, de 11 de setembro de 1990 . Provides for consumer protection and other measures. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Accessed: July 2024.

_____. Decreto nº 7.962, de 15 de março de 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. Accessed: July 2024.

_____. Lei nº 13.709, de 14 de agosto de 2018 . Lei Geral de Proteção de Dados (LGPD). Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed: July 2024.

_____. Lei nº 13.257, de 8 de março de 2016 . Marco Legal da Primeira Infância. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13257.htm. Accessed: May 2024.

_____. PL 2628/2022 . Proteção de crianças e adolescentes em ambientes digitais. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/154901. Accessed: July 2024.

_____. PL 2630/2020 . Lei das Fake News. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Accessed: July 2024.

_____. SUPERIOR TRIBUNAL DE JUSTIÇA . Jurisprudência em Teses, Edição nº 222. Available at: https://scon.stj.jus.br/SCON/jt/doc.jsp?livre=%27222%27.tit.&_gl=1%2a1tyc6aj%2a_ga%2aMTU2MzYxNzg0OS4xNjQ2MzQ5MDAy%2a_ga_F31N0L6Z6D%2aMTY5NjQ1NTI4OS40MTguMS4xNjk2NDU4NjUyLjYwLjAuMA. Accessed: June 2024.

_____. SUPERIOR TRIBUNAL DE JUSTIÇA . Jurisprudência em Teses, Edição nº 224. Available at: https://scon.stj.jus.br/SCON/jt/doc.jsp?livre=%27224%27.tit. Accessed: June 2024.

ALANA, Instituto. Programa Criança e Consumo . Available at: https://criancaeconsumo.org.br/. Accessed: June 2024.

_____. Sobre o Instituto Alana . Available at: https://alana.org.br/.

ANGELINE, K.; BARBOSA, A.; SENNE, F.; DINO, L. A. Privacidade e Proteção de Dados de Crianças e Adolescentes . Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; 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.; GASPAR, W. Cibersegurança [electronic resource]: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano . Rio de Janeiro: FGV, Direito Rio, 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, Fundação Getúlio Vargas. Guia de Tratamento de Dados de Crianças e Adolescentes . Available at: https://portal.fgv.br/sites/portal.fgv.br/files/criancas_e_adolescentes.pdf. Accessed: [access date missing].

FRAZÃO, A. In: FERNANDES, E.; TEFFÉ, C. S. de; BRANCO, S. (Eds.). Privacidade e Proteção de Dados de Crianças e Adolescentes . Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. Available at: https://bit.ly/3xGBo9v.

HENRIQUES, I.; PITA, M.; HARTUNG, P. *Tratado de Proteção de Dados Pessoais*. São Paulo: Ed. ABDR, 2023.

LATERÇA, P. S.; FERNANDES, E.; TEFFÉ, C. S. de; BRANCO, S. (Eds.). Privacidade e Proteção de Dados de Crianças e Adolescentes . Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; 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.

___

MEIO & MENSAGEM. Apenas 17% dos pais usam ferramentas para monitorar filhos na internet . Available at: https://www.meioemensagem.com.br/midia/apenas-17-dos-pais-usam-ferramentas-para-monitorar-filhos-na-internet. Accessed: May 2024.

NIELSEN. Medição, coleta de dados e análises globais de audiência das mídias tradicionais e digitais para avaliar tendências e comportamentos . Available at: https://www.tiktok.com/business/pt-BR/blog/tiktok-funciona-meta-analise-nielsen. Accessed: May 2024.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2023 [e-book] = Survey on Internet use by children in Brazil: ICT Kids Online Brazil 2023 . 1st ed. São Paulo: Comitê Gestor da Internet do Brasil, 2024. Available at: https://bit.ly/TicKids2023. Accessed: June 2024.

PRINSKY, M. Nativos Digitais . Available at: https://pt.wikipedia.org/wiki/Nativo_digital. Accessed: May 2024.

SOUZA, J.; NOVELLI, A.; CASTRO, J. Quadro regulatório de enfrentamento às fake news no Brasil: uma análise das propostas legislativas . Revista Ibero-Americana de Informação. Available at: https://periodicos.unb.br/index.php/RICI/article/view/45659/35275. Accessed: May 2024.

TIKTOk. Diretrizes da Comunidade . 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 [e-book] . Cologny/Geneva: World Economic Forum, 2024. Available at: https://www.weforum.org/publications/global-risks-report-2024/. Accessed: July 2024.

WU, Y. W.; EDWARDS, K.; DAS, S. SoK: Social Cybersecurity . In: 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022, pp. 1863-1879. Available at: https://ieeexplore.ieee.org/abstract/document/9833757. Accessed: July 2024.

UNICEF. The Case for Better Governance of Children's Data: A Manifesto . Available at: https://encurtador.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 for Collecting Information on Diversity in Health and in Digital Health

MAIRA LIMA DE SOUZA

Contents: Introduction. 1. Health Information Systems and Digital Health. 2. Diversity Information. 2.1. The Trajectory of Diversity as Social Information. 3. Methodology. 4. The Legal Bases and the Incorporation of Diversity into Health Systems. 4.1. The Trajectory of Diversity as Social Information. 4.2. Ethnicity. 4.3. Lesbians, Gays, Bisexuals, Travestis, and Transsexuals (LGBT). Final considerations. References.

Introduction

This article addresses how the legal bases adopted by the Brazilian government influence the collection of diversity information in the electronic health records generated by the main national Health Information Systems (HIS) and how this influence affects the quality of information in the context of Digital Health. In addition to influencing collection, these legal frameworks also affect 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 [2] .

Diversity data can be categorized as cultural (for example, shared norms and behaviors), biological (for example, age, sex), and defined in personal terms (for example, sexual orientation, religion) [3] .

Health information systems collect this information by means of forms or registration records. However, this recording does not follow

1. PhD in Knowledge Dissemination (UFBA), master’s in Ethnic and African Studies (UFBA), bachelor’s in Computer Science (UNIFACS), and certified in Privacy and Data Protection by Data Privacy Brasil (2024). I work in the fields of science, technology, and the humanities, on the topics of data policy, governance, and management, and decoloniality. I am also a member of the research group on Network Science and Theory called Fuxicos & Boatos (http://redessociaisecomplexas.org). I am a Senior Data Curator (data steward), focused on the handling of sensitive data and diversity, and I lead the Data Curation Unit of the Centro de Integração de Dados e Conhecimentos para Saúde (Cidacs/Fiocruz BA), the center with the largest collection of government administrative data among all low- and middle-income countries in the world, affiliated with the Fundação Oswaldo Cruz Bahia. My work ranges from supervising a multidisciplinary team of curators and developing sociotechnical data curation policies and models for public health projects, to curating research projects in compliance with the LGPD, defining measures that ensure the safe use of data, in accordance with ethics and the law.

2. BALESTRA, C.; FLEISCHER, L. Diversity statistics in the OECD: how do OECD countries collect data on ethnic, racial and indigenous identity? . OECD Statistics Working Papers, No. 2018/09, Paris: OECD Publishing, 2018. Available at: https://doi.org/10.1787/89bae654-en. Accessed: 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 identity? . OECD Statistics Working Papers, No. 2018/09, Paris: OECD Publishing, 2018. Available at: https://doi.org/10.1787/89bae654-en. Accessed: April 21, 2023. P. 7.

a linear or uniform trajectory. Although the definition of the fields in these forms is decisive for collection, the link between these fields and the process of identity formation makes that process more complex.

Health information systems have functioned as instruments for producing raw data intended for building statistical indicators on the population. Examples include the Mortality Information System (SIM), the Live Birth Information System (SINASC), 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) [4-5] .

Individually, these systems make it possible to map aspects such as mortality, birth, and disease in a given context. When combined, they capture comprehensive information about the life course, from birth, through the onset of disease, to death. Within the scope of Digital Health, the HIS can take part in interoperability and modernization strategies, such as the one provided for in the e-SUS Linha da Vida Program [6] . Within e-Health, they feed the active transparency portals [7] .

Just as the HIS do not serve the entire care system, since they were designed for specific health care purposes [8] , the legal bases that delimit the feeding of these systems may 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 race/color information became mandatory in all health information systems in Brazil under Ordinance No. 344/MS of February 1, 2017, although it had been in force as an attribute of individual recognition 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, G. C. ; CHIORO, A. Afinal, quantos Sistemas de Informação em Saúde de base nacional existem no Brasil? Cadernos de Saúde Pública, v. 37, no. 7, p. e00182119, 2021. Available at: https://www.scielo.br/j/csp/a/RzNmvjHqmLhPHZp6gfcdC6H/?format=pdf&lang=pt. Accessed: April 29, 2024.

5. BRASIL. Ministério da Saúde. *A experiência brasileira em sistemas de informação em saúde.* Brasília: Editora do Ministério da Saúde, 2009. (Série B. Textos Básicos de Saúde, v. 1 - Produção e disseminação de informações sobre saúde no Brasil).

6. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. Guia de Vigilância em Saúde [electronic resource] / Ministério da Saúde, Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. – 5th ed. rev. and updated. Brasília: Ministério da Saúde, 2022. 1,126 p.

7. BRASIL. Ministério da Saúde. Sistemas de informação da atenção à saúde: contextos históricos, avanços e perspectivas no SUS. Brasília, DF: Cidade Gráfica e Editora LTDA, Oct. 2015.

8. BRASIL. Ministério da Saúde. Sistemas de informação da atenção à saúde: contextos históricos, avanços e perspectivas no SUS. Brasília, DF: Cidade Gráfica e Editora LTDA, Oct. 2015.

existing at the time.[9] It should be noted that, as an indirect participant in the mandatory collection established by Ordinance 344/MS, ethnicity is blended with the collection of race/color, since 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 may also be linked to the classification of quilombola populations, treated as ethnic-racial groups.

Information on sexual orientation and gender identity has been found in the Notifiable Diseases Information System (SINAN) since 2014, specifically and only when violence is reported, whether interpersonal or self-inflicted.[10] It is noted that this information is tied to Brazil's legislation on the recording of violence, which aims at the defense and guarantee of rights.[11]

Although there are national health policies for the Black population, Lesbians, Gays, Bisexuals, Travestis, and Transsexuals (LGBT), and Indigenous Peoples, as well as legislation that favors migrants' access to health care and the 1988 Federal Constitution itself, which guarantees the right to health for all in Brazilian territory, health systems face limitations in capturing information on diversity.

The hypothesis is that the legal bases governing the collection of information on diversity stem 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 bringing together the national legal norms that directly and indirectly influence the collection of information on diversity in health, the article is based on documentary research of technical publications made available by official national agencies. The selected material sought to answer the following question: which national norms affect or have affected 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. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Análise de Situação de Saúde. Legislação Relativa aos Sistemas de Informações sobre Mortalidade (SIM) e sobre Nascidos Vivos (SINASC). Brasília: Ministério da Saúde, 2004.

10. OLIVEIRA, D.C. Representatividade da população LGBTQIA+ nas pesquisas epidemiológicas, no contexto da Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais: ampliar a produção de conhecimento no SUS para a justiça social. Epidemiologia e Serviços de Saúde, v. 31, no. 1, e2022020, 2022.

11. LEAL, C. H. S.; SCALCO, M. L. A.; NUNES, R. P. D.; CONSORTII, E. R.; KITAGAWA, B. Y. Vigilância de violências: considerações sobre as informações relativas às violências perpetradas contra a população LGBT no município de São Paulo. Bis, São Paulo, v. 2, no. 19, pp. 55-61, Dec. 2018. Available at: https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n2-diversidade-55-61.pdf. Accessed: 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 on the population of Lesbians, Gays, Bisexuals, and Transsexuals (LGBT).

1. Health Information Systems and Digital Health

Electronic health records are generated as part of the state's normal business transactions and contain information on individuals who access the public service, characterizing both individual and collective facts. Used as instruments of public administration and created for operational purposes, these nationwide data have come to be used to generate public information and statistics.

These records, as we know them today, stem from the evolution of the process of systematizing government public services and their information, marked by the development of tools and methods. Two elements stand out in this process: the incorporation of statistics as an element of scientific government, and digitalization.[12] The former reinforced the call for organizing and systematizing information, a necessary condition for providing national statistics. The latter, part of the administrative rationalization efforts of the 1990s, emphasized managerial public administration and made use of Information and Communication Technology (ICT) as an instrument of electronic government. This initiative gained strength from the discursive association that links information (and, consequently, ICTs) to governance and development.[13-14] At the time, with neoliberalism as a backdrop, it was important for developing countries to have "good governance of public management" in order to secure international financial benefits.[15]

The potential to generate statistics and complement the knowledge produced about the population to which these records refer has expanded

12. BRASIL. Ministério da Saúde. *A experiência brasileira em sistemas de informação em saúde.* Brasília: Editora do Ministério da Saúde, 2009. (Série B. Textos Básicos de Saúde, v. 1 - Produção e disseminação de informações sobre saúde no Brasil).

13. WORLD BANK. Managing development: the governance dimension. Washington, D.C.: World Bank Group, 1991. Available at: http://documents.worldbank.org/curated/en/884111468134710535/Managing-development-the-governance-dimension. Accessed: February 14, 2024.

14. PANZARDI, R.; CALCOPIETRO, C.; IVANOVIC, E. F. New-economy sector study: electronic government and governance - lessons from Argentina. Working paper. Washington, DC: World Bank, July 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: February 14, 2024.

15. WORLD BANK. Managing development: the governance dimension. Washington, D.C.: World Bank Group, 1991. Available at: http://documents.worldbank.org/curated/en/884111468134710535/Managing-development-the-governance-dimension. Accessed: February 14, 2024.

their adoption among researchers, governments, and statistical agencies.[16,17,18] This is because the continuous collection of this information over time favors longitudinal analyses, making population-based approaches possible.

With regard to administrative health records, Brazil has invested in recent years in active transparency measures aimed at broadening its stance on data openness, encouraging the use and reuse of these (de-identified) records as secondary data for research and policy purposes.[19] At the national level, the perception brought from the United Kingdom resonates that these records are an invaluable resource for the common public good.[20] This value is amplified by the possibility of linking these records together.

The scope of monitoring aimed at producing knowledge relevant to society can be expanded through actions such as:

a) Linkage between databases (Data Linkage). The application of this statistical technique, which can be carried out through probabilistic and deterministic methods,[21] makes it possible to link data from different sources based on common records and is spreading as a surveillance strategy.[22-23]

b) Interoperability. The capacity for interconnection and communication between information systems of different technologies. This strategy is incorporated into the National Health Information and Informatics Policy (PNIIS),[24] of 2003, which advocates for the organization of the National Health

16. SENRA, N. de C. A questão dos registros administrativos vis-à-vis a geração de estatísticas. Revista Brasileira de Estudos de População, [S. l.], v. 13, no. 2, pp. 199–205, 1996. Available at: https://rebep.org.br/revista/article/view/437. Accessed: July 23, 2024.

17. FERREIRA, F. P. M. Registros administrativos como fonte de dados estatísticos. Informática Pública, year 10, no. 1, pp. 81-93, 2008.

18. MELLO, Janine. Produção estatal de evidências e uso de registros administrativos em políticas públicas. In: KOGA, Natália Massaco (Ed.) et al. Políticas públicas e o uso de evidências no Brasil: conceitos, métodos, contextos e práticas. Brasília: IPEA, 2022. pp. 897-914.

19. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde e Ambiente. Departamento de Análise Epidemiológica e Vigilância de Doenças não Transmissíveis. Dados para Vigilância: perfis das bases de dados produzidas pela Vigilância em Saúde no Brasil. Brasília: Ministério da Saúde, 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. Ciência de dados populacionais. Epidemiologia e serviços de saúde: revista do Sistema Único de Saúde do Brasil, v. 31, no. 3, e2022119, Dec. 19, 2022. doi:10.1590/S2237-96222022000300001.

22. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. Guia de Vigilância em Saúde [electronic resource] / Ministério da Saúde, Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. – 5th ed., rev. and updated. Brasília: Ministério da Saúde, 2022. 1.126 p.

23. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Nota Técnica nº 34/2023: atualizações e recomendações para a vigilância de anomalias congênitas no Brasil. Brasília, DF, 2023. Available at: http://plataforma.saude.gov.br/anomalias-congenitas/nota-tecnica-34-2023.pdf. Accessed: March 8, 2024.

24. BRASIL. Ministério da Saúde. Secretaria Executiva. Departamento de Informática do SUS. Política Nacional de Informação e Informática em Saúde: Proposta Versão 2.0 (Inclui deliberações da 12ª Conferência Nacional de Saúde). 2004. Available at: http://bvsms.saude.gov.br/bvs/publicacoes/PoliticaInformacaoSaude29_03_2004.pdf. Accessed: August 1, 2024.

Information System (SNIS) and its alignment with the guidelines of the Brazilian Electronic Government Program (e-Gov) and the e-Health strategy.[25-26]

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. According to their operating purpose, these systems are organized for surveillance of events relevant to public health, control and monitoring of Ministry of Health health programs, registration of users of care (population, professionals, and health services), and support for 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.[27]

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 system management, and of technical specialization, which creates a system for every new need. As a result, the systems produce the same information but are guided by different collection methods and rules.[28] In addition, changes in system versions for the purposes of modernization and improvement can lead to inconsistent information due to data loss or discontinuity.[29] Information collection is also an issue, since few systems have incorporated electronic records.

2. Diversity information

Diversity refers to social categories used to describe the differences among the people who make up a given population. These data focus on characteristics such as race/ethnicity, citizenship, migration status,

25. BRASIL. Ministério da Saúde. Portaria nº 589 de 20 de maio de 2015. Establishes the National Health Information and Informatics Policy (PNIIS). Diário Oficial da União: edition 96, section 1, Brasília, DF, p. 72, May 22, 2015.

26. BRASIL. Ministério da Saúde. Portaria nº 2.073, de 31 de agosto de 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. Diário Oficial da União: section 1, Brasília, DF, p. 63, September 1, 2011.

27. COELHO NETO, G. C.; CHIORO, A. Afinal, quantos Sistemas de Informação em Saúde de base nacional existem no Brasil? Cadernos de Saúde Pública, v. 37, no. 7, p. e00182119, 2021. Available at: https://www.scielo.br/j/csp/a/RzNmvjHqm-LhPHZp6gfcdC6H/?format=pdf&lang=pt. Accessed: April 29, 2024. p. 9.

28. BRASIL. Ministério da Saúde. Sistemas de informação da atenção à saúde: contextos históricos, avanços e perspectivas no SUS. Brasília, DF: Cidade Gráfica e Editora LTDA, Oct. 2015.

29. BRASIL. Ministério da Saúde. *Consolidação do Sistema de Informações sobre Nascidos Vivos.* Coordenação Geral de Informações e Análise Epidemiológica. 2011.

religion, gender (including gender identity), age, social class, disability, sexual orientation, marital status, among others. The relevance and impact of each category vary according to society, time, and context.[30] 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.[31]

Diversity information is situated within a broader debate on: 1) the rights of minorities and the monitoring of compliance with human rights obligations; 2) the application of anti-discrimination legislation; and 3) tracking progress toward achieving the sustainable development goals and social equality, among others.[32] More forcefully, however, it is a debate about citizenship, centered on reflections on the multiethnic composition of a nation.33 34 [35]

In Brazil, social considerations of diversity rest on categories such as race/color; ethnic-racial groups; traditional peoples and communities, such as quilombolas, Indigenous peoples, Romani people, terreiro communities, rubber tappers, artisanal fishers, among others; Lesbians, Gays, Bisexuals, Travestis, and Transsexuals (LGBT); and the migrant, refugee, and stateless population.36 37

In the health field, these groups participate directly or cross-cuttingly in national policies, such as the National Food and Nutrition Policy (1999), the National Policy for the Reduction of Morbidity and Mortality from Accidents and Violence (2001), the National Emergency Care Policy, the National Policy on Health Care for Indigenous Peoples (2002), and the National Policies on Comprehensive Health for Specific Populations, such as those for the Black population (2009) and the LGBT population (2011).[38]

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: 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: 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. Brasil mostra a tua cara: imagens da população brasileira nos censos demográficos de 1872 a 2000. Rio de Janeiro: Escola Nacional de Ciências Estatísticas, 2003. 75 p. ISSN 1677-7093; no. 6.

34. COSTA, Fabiana Claudia Viana. Designação e referência enunciativa do Censo demográfico 2000. 2004. Dissertation (Master's in Linguistics) – UNICAMP, Instituto de Estudos da Linguagem, Universidade Estadual de Campinas, Campinas, São Paulo, 2004.

35. LOVEMAN, M. A política de um cenário de dados transformado: estatísticas etnorraciais no Brasil em uma perspectiva comparativa regional. Sociologias, v. 23, no. 56, pp. 110–153, Jan. 2021.

36 ARRUTI, José Maurício. Etnicidade. In: SANSONE, L.; ALVES FURTADO, C. (Eds.). Dicionário crítico das ciências sociais dos países de fala oficial portuguesa. Salvador: EDUFBA, 2014. pp. 199-2013.

37. MIGUEL, Nadya Maria Deps. O Perfil do brasileiro construído pelo IBGE: uma memória discursiva dos Censos Demográficos de 1940 a 2010. Thesis (Graduate Program in Social Memory) – Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2012.

38. BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Nota Técnica nº 18/2014. Revisão da Política Nacional de Promoção da Saúde. 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: 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 took on 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.[39] To that end, the following was envisioned: “training in the use of administrative records and the improvement of existing systems. By improvement is meant the inclusion, in all records concerning individuals, of the items sex, age, and race.”[40]

At the core of these initiatives was the creation of indicators. The collection of data on diversity generally uses indicators, which are measurable parameters that represent specific aspects of a diversity category. Once given meaning, these statistics are treated as indicators of a situation that will be the target of policy intervention. The aim is for the effectiveness of the policy to positively affect the reality of these indicators.[41]

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 into the scope of Information Systems (SIS), to provide inputs for official surveys that use the individual as the unit of analysis.[42] It should be noted, however, 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 documentary analysis, qualitative in nature, was carried out through consultation of the official websites of the Brazilian government. Technical documents, bylaws, and manuals were prioritized. The survey gathered information on public policies and rights related to race, ethnicity, and the

39. UNITED NATIONS POPULATION FUND. Projetos e Programas Propostos: Assistência ao Governo do Brasil (DP/FPA/BRA/3). United Nations Population Fund, 2001. Available at: https://brazil.unfpa.org/sites/default/files/pub-pdf/country_programme20022006_0.pdf. Accessed: April 29, 2024.

40. OSÓRIO, Rafael Guerreiro. *O Sistema Classificatório de Cor e Raça do IBGE*. Brasília: Ipea, Ministério do Planejamento, Orçamento e Gestão, 2003. (Texto para discussão, 996). P. 37.

41. OSÓRIO, Rafael Guerreiro. *O Sistema Classificatório de Cor e Raça do IBGE*. Brasília: Ipea, Ministério do Planejamento, Orçamento e Gestão, 2003. (Texto para discussão, 996).

42. OSÓRIO, Rafael Guerreiro. *O Sistema Classificatório de Cor e Raça do IBGE*. Brasília: Ipea, Ministério do Planejamento, Orçamento e Gestão, 2003. (Texto para discussão, 996).

population of Lesbians, Gays, Bisexuals, Travestis, and Transsexuals (LGBT). The survey of decrees was carried out from the citations contained in those documents. As for the assessment of the conditions of social information in Health Information Systems, for the purposes of this article, only those linked to Primary Care were prioritized: the Mortality Information System (SIM), the Live Birth Information System (SINASC), the Food and Nutrition Surveillance System (SISVAN), the Notifiable Diseases Information System (SINAN), and the Outpatient Information System (SIA/SUS). The cases were assessed according to the system's objective and its adequacy to the legal basis of the diversity categories analyzed.

4. Legal bases and the incorporation of diversity into 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 guarantees health as a right to be ensured by the State.[43] It should be noted that the Constitution guarantees other rights and safeguards for diversity, which, in general terms, can be grouped into 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 fall within the scope of Human Rights and Citizenship, in addition to being included in the legislation dealing with crimes related to prejudice.

4.1 Race/color

The mapping carried out on the legal bases identified a normative landscape composed of two laws, one decree, and three ordinances. Ordinances No. 3.947/GM/MS and No. 344/MS have a direct effect on the inclusion of the variable in SUS collection forms. Law No. 12.288, considered a fundamental legal milestone in Ordinance No. 344/MS, although it addresses the right to health, among other issues, also engages with legislation dealing with crimes related to prejudice, violence, and intolerance. This law and Ordinance No. 992/GM/MS emerge as milestones for minimizing discrimination both in the social sphere and within the Unified Health System (SUS). Below is the list of the milestones identified:

43. BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República. Available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Accessed: April 29, 2024.

• Decree No. 65.810 of December 08, 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, on a mandatory basis, by all systems and databases of the Ministry of Health, as of January 1, 1999.

• Ordinance No. 992/GM/MS of May 13, 2009: National Policy on Comprehensive Health for the Black Population (PNSIPN).
• Law No. 12.288 of July 20, 2010: Racial Equality Statute.
• 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 01, 2017: mandatory completion of the race/color item on 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 hiring and termination forms, workplace accident forms, record instruments of the National Employment System (SINE), and documents for enrollment in the General Social Security Regime. The inclusion also applies to the Annual Report of Social Information (RAIS) and to IBGE survey questionnaires.

Since 1995, SINASC has used the field “RACACOR” for recording. However, reflecting the impact of Ordinance No. 992/GM/MS/2009 and Law No. 12.288/2010, there was a change in the form of notification. Starting in 2011, in addition to collecting information on the race/color of the newborn, information on the mother also began to be collected.[44] This change made it possible to map access to maternal and child health policies and was a strategy for identifying racial discrimination. Until then, SINASC’s emphasis had been the production of vital statistics.[45] [46]

44. BRASIL. Ministério da Saúde. *Consolidação do Sistema de Informações sobre Nascidos Vivos.* Coordenação Geral de Informações e Análise Epidemiológica. 2011.

45. BRASIL. Ministério da Saúde. Fundação Nacional de Saúde. *Manual de procedimentos do sistema de informações sobre nascidos vivos.* Brasília: Ministério da Saúde, 2001. 32 p.

46. BRASIL. Ministério da Saúde. *Consolidação do Sistema de Informações sobre Nascidos Vivos.* Coordenação Geral de Informações e Análise Epidemiológica. 2011.

In SIM and SINASC, where the introduction of completing the race/color item is older, the completeness of the information is greater.[47] Part of this characteristic stems from the legal framework that supported the creation of the systems. Both began collection in the same year and derive from the rules governing public records (Law 6.015 of December 31, 1973) and civil records, specifically the notarial rules, respectively.[48]

4.2 Ethnicity

Since the 2000 census, IBGE has surveyed the race, color, and ethnicity of the Brazilian population.[49] According to the criteria defined by the institute, the population may be classified as white (branca), Black (preta), yellow (amarela), brown (parda), or Indigenous. An Indigenous person is considered to be one who identifies as such, whether through ties to Indigenous lands or links to traditions[50] (Brasil, 2017). Thus, the concept of "Indigenous" developed by IBGE is tied to Indigenous groups. Since then, this classification criterion has been used, especially from Ordinances No. 3.947/GM/MS/1998 and No. 344/MS/2017.

It was through Decree No. 6.040 of February 7, 2007, that the National Policy on the Sustainable Development of Traditional Peoples and Communities was established, broadening the notion of ethnicity. The category of traditional peoples and communities (PCTs) includes quilombola communities, Indigenous peoples, Romani people, terreiro communities, rubber tappers, artisanal fishers, among others. This is a formal legal recognition that falls within the framework of land regulation.[51]

Traditional peoples and communities have their legal recognition marked by their relationships with territory. Since the 1988 Federal Constitution (CF/88), the Brazilian State has treated PCTs as social organizations that occupy and use territories.[52]

47. COELHO, R.; REMÉDIOS, J.; NOBRE, V.; MREJEN, M. O quesito raça/cor no DataSUS: evolução e determinantes da completude. Nota Técnica n. 30. IEPS: São Paulo, 2023.

48. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Análise de Situação de Saúde. *Legislação Relativa aos Sistemas de Informações sobre Mortalidade (SIM) e sobre Nascidos Vivos (SINASC).* Brasília: Ministério da Saúde, 2004.

49. BRASIL. Ministério da Saúde. Guia de implementação do quesito Raça/Cor/Etnia. Ministério da Saúde, Universidade de Brasília. Brasília: Ministério da Saúde, 2018. 38 p.: ill.

50. BRASIL. Ministério do Desenvolvimento Social. *Trabalho social com famílias indígenas na proteção social básica.* Brasília, DF: MDS, Secretaria Nacional de Assistência Social, 2017.

51. BRASIL. Ministério da Cidadania. Informativo PCT. [Informativo]. Secretaria Nacional de Assistência Social, 2017. Available at: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf. Accessed: February 14, 2024.

52. BRASIL. Ministério do Desenvolvimento Social. *Trabalho social com famílias indígenas na proteção social básica.* Brasília, DF: MDS, Secretaria Nacional de Assistência Social, 2017.

In this sense, care for PCTs is characterized by a notion of collectivity that goes beyond the notion of family or individual, and it is governed by territory-based Primary Health Care services, whether through Special Indigenous Health Districts (DSEI) or Remnant Quilombo Communities (CRQ).[53] Health care covers specialized care, women's and children's health care, and food and nutrition surveillance, among other areas. Thus, there is a "social assistance surveillance with socio-territorial diagnosis."[54]

The legal parameters guiding the collection of data on PCTs, which began with the census, are incorporated into the framework of actions of the Ministry of Social Development and Fight Against Hunger (MDS), pursuant to Decree No. 6.040/2007 [55] [56]. Thus, within the scope of social protection, duly registered Indigenous and quilombola families were included in the records of the Cadastro Único for Social Programs.[57] Based on these considerations, the regulatory bases for the collection of data on ethnicity are related to:

- Article 194 of the 1988 Federal Constitution, on social security.
- Law No. 8.742 of December 7, 1993, the Organic Law of Social Assistance (LOAS)
- Law No. 9.459 of May 13, 1997, which adds to Article 140 of the Penal Code the clause on Racial Insult.
- 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 Labour Organization concerning Indigenous and Tribal Peoples.

53. BRASIL. Ministério do Desenvolvimento Social. *Trabalho social com famílias indígenas na proteção social básica.* Brasília, DF: MDS, Secretaria Nacional de Assistência Social, 2017.

54. BRASIL. Ministério da Cidadania. Informativo PCT. [Informativo]. Secretaria Nacional de Assistência Social, 2017. Available at: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf. Accessed: February 14, 2024. p. 15.

55. BRASIL. Ministério do Desenvolvimento Social. *Trabalho social com famílias indígenas na proteção social básica.* Brasília, DF: MDS, Secretaria Nacional de Assistência Social, 2017.

56. BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Departamento de Atenção Básica. Coordenação-Geral da Política de Alimentação e Nutrição. *Manual operacional para uso do Sistema de Vigilância Alimentar e Nutricional. SISVAN Versão 3.0. Normas e Manuais Técnicos.* Brasília: Ministério da Saúde, 2017.

57. BRASIL. Ministério da Cidadania. Informativo PCT. [Informativo]. Secretaria Nacional de Assistência Social, 2017. Available at: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf. Accessed: February 14, 2024. p. 15.

• Ordinance No. 254/GM/MS of January 31, 2002, on the National Policy on Health Care for Indigenous Peoples.

• Ordinance No. 98 of November 26, 2007, on the General Registry of Remnant Quilombo Communities

• Decree No. 6.040 of February 07, 2007, which established the National Policy on the Sustainable Development of Traditional Peoples and Communities.

• Decree No. 6.261/2007 (repealed by Decree No. 11.447 of March 21, 2023). Aquilomba Brasil Program and its Steering Committee.

• Ordinance No. 992/GM/MS of May 13, 2009: National Policy on Comprehensive Health for 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, addresses expanding access for Black, Indigenous, and Romani populations and, within the scope of family health, for quilombola communities.

• Decree No. 10.088 of November 05, 2009 (and Decree 5.051/2004), which adopts the legislative decree on ILO Convention 169 and the legal principle of ethnic self-determination.

• Ordinance No. 177 of June 16, 2011, which defines differentiated service for certain population groups for inclusion in the Cadastro Único.

• Ordinance No. 2.866 of December 2, 2011, on the National Policy on Comprehensive Health for Rural and Forest Populations (PNSIPCF)

• GM/MS Ordinance No. 3.396 of December 11, 2020

• Decree No. 12.128 of August 1, 2024, officially establishes the National Plan of Policies for Romani Peoples.

The mapping of the legal bases identified a normative landscape oriented toward the recognition of rights, the demarcation of territories, and the administrative management of those territories. Health actions are referenced by the National Policy on Comprehensive Health for Rural and Forest Populations (PNSIPCF) and the National Policy on Comprehensive Health for the Black Population (PNSIPN). These policies highlight the specific health needs of these populations, including vulnerabilities in access, violence and territorial disputes, mental health issues and the use of psychotropic drugs, access to food, and

sexually transmitted diseases, among others. The PNSIPCF, in particular, emphasizes aspects of citizenship, food and nutrition security, and sustainable development.[58]

The health assessment of these groups tends to be characterized by geographic space and by categories of gender, age, race/ethnicity, and other markers of specific populations. In health systems (SIS), ethnicity can be collected from two fields: race/color and traditional people and community. Among the systems linked to Primary Care, the Mortality Information System (SIM), the Live Birth Information System (SINASC), and the Notifiable Diseases Information System (SINAN) use the race/color field to collect information on ethnicity. In some cases, the street-name field (logradouro), associated with the address (street, avenue, etc.), can be used to record the name of the traditional community.[59] Because of its connection to the nutritional surveillance program and to the actions of the Bolsa Família Program, the Food and Nutrition Surveillance System (SISVAN) has a traditional people and community field.[60]

Lesbians, Gays, Bisexuals, Travestis, and Transsexuals (LGBT)

The health concerns of lesbians, gays, bisexuals, travestis, and transsexuals (LGBT) are closely related to issues of violence, the process of transsexualization, and the response to HIV/AIDS and sexually transmitted diseases (STDs). In fact, it was through the response to the HIV/AIDS epidemic that the health issues of this population gained prominence in Brazil.[61] 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,[62] as shown below:

58. IEPS; UMANE; INSTITUTO VEREDAS. Relatório Técnico nº1/2023. Saúde dos Povos Indígenas e Quilombolas. Rio de Janeiro: IEPS, 2023.

59. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. *Sistema de Informação de Agravos de Notificação. Ficha de Notificação.* Brasília: Ministério da Saúde, 2006.

60. BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Departamento de Atenção Básica. Coordenação-Geral da Política de Alimentação e Nutrição. *Manual operacional para uso do Sistema de Vigilância Alimentar e Nutricional. SISVAN Versão 3.0. Normas e Manuais Técnicos.* Brasília: Ministério da Saúde, 2017.

61. BRASIL. Ministério da Saúde. Secretaria de Gestão Estratégica e Participativa. Departamento de Apoio à Gestão Participativa. Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais. Ministério da Saúde, Secretaria de Gestão Estratégica e Participativa, Departamento de Apoio à Gestão Participativa. Brasília, DF: Ministério da Saúde, 1st ed., 2013.

62. BRASIL. Ministério da Saúde. Secretaria de Gestão Estratégica e Participativa. Departamento de Apoio à Gestão Participativa. Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais. Ministério da Saúde, Secretaria de Gestão Estratégica e Participativa, Departamento de Apoio à Gestão Participativa. Brasília, DF: Ministério da Saúde, 1st ed., 2013.

• Law No. 7.716 of January 5, 1989, on crimes resulting from prejudice.

• Ordinance No. 2.227 of October 14, 2004, provides for the creation of the Technical Committee to formulate a proposal for the national health policy for the population of gays, lesbians, transgender people, and bisexuals – GLTB.

• MS/GM Ordinance No. 104 of January 25, 2011, universalizes the reporting of domestic violence, sexual violence, and other forms of violence.

• Ordinance No. 2.836 of December 1, 2011, National Policy on Comprehensive Health for Lesbians, Gays, Bisexuals, Travestis, and Transsexuals (National Policy on Comprehensive LGBT Health).

• MS/GM Ordinance No. 1.271 of June 06, 2014, adds cases of sexual violence and attempted suicide to the list of diseases and conditions subject to compulsory notification.

• Consolidation Ordinance GM/MS No. 02 of September 28, 2017, which consolidates the National Policy on Comprehensive LGBT Health among the national health policies of the Unified Health System.

• CIT Resolution No. 26 of September 28, 2017, second operational plan (2017-2019) of the National Policy on Comprehensive LGBT Health within the scope of the Unified Health System.

• Bill No. 1082 of 2023 (pending), which proposes amending Law No. 8.184 of May 10, 1991, and making mandatory the collection of data on the LGBTQIA+ population (lesbians, gays, bisexuals, transsexuals, queer, intersex, asexual, and others) in the censuses and other periodic surveys of the Brazilian Institute of Geography and Statistics Foundation (IBGE).

• Ordinance No. 762 of December 7, 2023, establishes the National Human Rights Evidence Network within the scope of the Ministry of Human Rights and Citizenship.

The trajectory of collecting and incorporating information on the LGBT population into Health Information Systems (SIS) begins with the Notifiable Diseases Information System (SINAN), through its violence surveillance module, from 2015 onward.[63] The structure of this module's form is able to record sexual orientation (heterosexual, homosexual (gay/lesbian), bisexual) and gender identity (travesti, transsexual woman,

63. LEAL, C. H. S. ; SCALCO, M. L. A. ; NUNES, R. P. D. ; CONSORTII, E. R. ; KITAGAWA, B. Y. Vigilância de violências: considerações sobre as informações relativas às violências perpetradas contra a população LGBT no município de São Paulo. Bis, São Paulo, v. 2, no. 19, pp. 55-61, Dec. 2018. Available at: https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n2-diversidade-55-61.pdf. Accessed: April 19, 2024.

transsexual man), as well as the motivation for the violence (sexism, homophobia/lesbophobia/biphobia/transphobia, racism, religious intolerance, xenophobia, generational conflict, homelessness, disability).[64]

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)).[65] For the systems that do not capture this information, the sex variable remains (male, female, unknown).

Final considerations

This brief analysis of the national norms governing the inclusion of the social categories that represent diversity in health information systems shows that the relevant legislation was built and drafted as these categories gained social recognition. However, even though they are safeguarded by public policy programs, statistical invisibility still persists for some of these categories.

The lack of infrastructure and of information management, in the sense of creating a standard, has proven to be a limiting factor for expanding the inclusion of information fields capable of representing these categories. Administrative records are seen to be a relevant source of data on the country's diversity, in addition to the census.

Moreover, 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 how they are included in information systems and which systems will be considered.

The strategic path of Digital Health, like that of all digital government business, is being outlined by a framework that assesses institutional maturity in the use of data. Considerations about how the

64. LEAL, C. H. S. ; SCALCO, M. L. A. ; NUNES, R. P. D. ; CONSORTII, E. R. ; KITAGAWA, B. Y. Vigilância de violências: considerações sobre as informações relativas às violências perpetradas contra a população LGBT no município de São Paulo. Bis, São Paulo, v. 2, no. 19, pp. 55-61, Dec. 2018. Available at: https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n2-diversidade-55-61.pdf. Accessed: April 19, 2024. p. 57.

65. CANAVESE, D. et al. Pela urgente e definitiva inclusão dos campos de identidade de gênero e orientação sexual nos sistemas de informação em saúde do SUS: o que podemos aprender com o surto de monkeypox?. Ciência & Saúde Coletiva, v. 27, no. 11, pp. 4191–4194, Nov. 2022.

population is incorporated into official surveys, although longstanding, 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 an era, its context, and the ideals of the constituents of society.

What should be problematized 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 certain way, social policies become data and information policies, determining how, when, and why collection should take place, the challenge lies in creating a moderating strategy that is incorporated into data processing, especially between the collection and the use of this information. The mismatch between the public entity's readiness to capture, collect, and, consequently, properly process this information and the advance of rights legislation can be offset by data governance strategies.

Although individual information is collected, the analysis of diversity data aims to understand a collective context. In addition, the collection and use of data have 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, in order to meaningfully address concerns related to the use (and enjoyment) of these data and of other technologies.

In this sense, international bodies advocate that public authorities adopt data governance models that are differentiated by social group and its specificities. Such models can be improved to meet the rights of these communities, using normative strategies and data principles geared toward social justice. This is an area little debated 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 and coding of these data and guiding their use. This strategy can also help address the (persistent) gap linking the need to adjust the collection instrument to capture relevant information and the capacity to incorporate that instrument into information systems, by creating strategies for data processing and coding.

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. Etnicidade. In: SANSONE, L.; ALVES FURTADO, C. (Eds.). Dicionário crítico das ciências sociais dos países de fala oficial portuguesa. Salvador: EDUFBA, 2014. pp. 199-2013.

BALESTRA, C.; FLEISCHER, L. Diversity statistics in the OECD: how do OECD countries collect data on ethnic, racial and indigenous identity? OECD Statistics Working Papers, No. 2018/09, Paris: OECD Publishing, 2018. Available at: https://doi.org/10.1787/89bae654-en. Accessed: 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: March 8, 2024.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República. Available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Accessed: April 29, 2024.

BRASIL. Ministério da Cidadania. Informativo PCT. [Informativo]. Secretaria Nacional de Assistência Social, 2017. Available at: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf. Accessed: February 14, 2024.

BRASIL. Ministério da Cidadania. Informativo PCT. [Informativo]. Secretaria Nacional de Assistência Social, 2017. Available at: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf. Accessed: February 14, 2024. p. 15.

BRASIL. Ministério da Saúde. A experiência brasileira em sistemas de informação em saúde. Brasília: Editora do Ministério da Saúde, 2009. (Série B. Textos Básicos de Saúde, v. 1 – Produção e disseminação de informações sobre saúde no Brasil).

BRASIL. Ministério da Saúde. *Consolidação do Sistema de Informações sobre Nascidos Vivos.* Coordenação Geral de Informações e Análise Epidemiológica. 2011.

BRASIL. Ministério da Saúde. Fundação Nacional de Saúde. *Manual de procedimentos do sistema de informações sobre nascidos vivos.* Brasília: Ministério da Saúde, 2001. 32 p.

BRASIL. Ministério da Saúde. Guia de implementação do quesito Raça/Cor/Etnia. Ministério da Saúde, Universidade de Brasília. Brasília: Ministério da Saúde, 2018. 38 p.: ill.

BRASIL. Ministério da Saúde. Portaria nº 2.073, de 31 de agosto de 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. Diário Oficial da União: section 1, Brasília, DF, p. 63, September 1, 2011.

BRASIL. Ministério da Saúde. Portaria nº 589 de 20 de maio de 2015. Establishes the National Health Information and Informatics Policy (PNIIS). Diário Oficial da União: edition 96, section 1, Brasília, DF, p. 72, May 22, 2015.

BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Departamento de Atenção Básica. Coordenação-Geral da Política de Alimentação e Nutrição. Manual operacional para uso do Sistema de Vigilância Alimentar e Nutricional. SISVAN Versão 3.0. Normas e Manuais Técnicos. Brasília: Ministério da Saúde, 2017.

BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Departamento de Atenção Básica. Coordenação-Geral da Política de Alimentação e Nutrição. Manual operacional para uso do Sistema de Vigilância Alimentar e Nutricional. SISVAN Versão 3.0. Normas e Manuais Técnicos. Brasília: Ministério da Saúde, 2017.

BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Nota Técnica nº 18/2014. Revisão da Política Nacional de Promoção da Saúde. 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: April 29, 2024.

BRASIL. Ministério da Saúde. Secretaria de Gestão Estratégica e Participativa. Departamento de Apoio à Gestão Participativa. Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais. Ministério da Saúde, Secretaria de Gestão Estratégica e Participativa, Departamento de Apoio à Gestão Participativa. Brasília, DF: Ministério da Saúde, 1st ed., 2013.

BRASIL. Ministério da Saúde. Secretaria de Gestão Estratégica e Participativa. Departamento de Apoio à Gestão Participativa. Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais. Ministério da Saúde, Secretaria de Gestão Estratégica e Participativa, Departamento de Apoio à Gestão Participativa. Brasília, DF: Ministério da Saúde, 1st ed., 2013.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde e Ambiente. Departamento de Análise Epidemiológica e Vigilância de Doenças não Transmissíveis. Dados para Vigilância: perfis das bases de dados produzidas pela Vigilância em Saúde no Brasil. Brasília: Ministério da Saúde, 2023. 127 p.: ill.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. Guia de Vigilância em Saúde [electronic resource] / Ministério da Saúde, Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. – 5th ed., rev. and updated. Brasília: Ministério da Saúde, 2022. 1.126 p.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Análise de Situação de Saúde. *Legislação Relativa aos Sistemas de Informações sobre Mortalidade (SIM) e sobre Nascidos Vivos (SINASC).* Brasília: Ministério da Saúde, 2004.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Nota Técnica nº 34/2023: atualizações e recomendações para a vigilância de anomalias congênitas no Brasil. Brasília, DF, 2023. Available at: http://plataforma.saude.gov.br/anomalias-congenitas/nota-tecnica-34-2023.pdf. Accessed: March 8, 2024.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Sistema de Informação de Agravos de Notificação. Ficha de Notificação. Brasília: Ministério da Saúde, 2006.

BRASIL. Ministério da Saúde. Secretaria Executiva. Departamento de Informática do SUS. Política Nacional de Informação e Informática em Saúde: Proposta Versão 2.0 (Inclui deliberações da 12ª Conferência Nacional de Saúde). 2004. Available at: http://bvsms.saude.gov.br/bvs/publicacoes/PoliticaInformacaoSaude29_03_2004.pdf. Accessed: August 1, 2024.

BRASIL. Ministério da Saúde. Sistemas de informação da atenção à saúde: contextos históricos, avanços e perspectivas no SUS. Brasília, DF: Cidade Gráfica e Editora LTDA, Oct. 2015.

BRASIL. Ministério do Desenvolvimento Social. Trabalho social com famílias indígenas na proteção social básica. Brasília, DF: MDS, Secretaria Nacional de Assistência Social, 2017.

CANAVESE, D. et al. Pela urgente e definitiva inclusão dos campos de identidade de gênero e orientação sexual nos sistemas de informação em saúde do SUS: o que podemos aprender com o surto de monkeypox?. Ciência & Saúde Coletiva, v. 27, no. 11, pp. 4191–4194, Nov. 2022.

COELHO NETO, G. C. ; CHIORO, A. Afinal, quantos Sistemas de Informação em Saúde de base nacional existem no Brasil? Cadernos de Saúde Pública, v. 37, no. 7, p. e00182119, 2021. Available at: https://www.scielo.br/j/csp/a/RzNmvjHqmLhPHZp6gfcdC6H/?format=pdf&lang=pt. Accessed: April 29, 2024.

COELHO, R. ; REMÉDIOS, J. ; NOBRE, V. ; MREJEN, M. O quesito raça/cor no DataSUS: evolução e determinantes da completude. *Nota Técnica n. 30.* IEPS: São Paulo, 2023.

COELI, Cláudia Medina. Ciência de dados populacionais. Epidemiologia e serviços de saúde: revista do Sistema Único de Saúde do Brasil, v. 31, no. 3, e2022119, Dec. 19, 2022. doi:10.1590/S2237-96222022000300001.

COSTA, Fabiana Claudia Viana. Designação e referência enunciativa do Censo demográfico 2000. 2004. Dissertation (Master's in Linguistics) – UNICAMP, Instituto de Estudos da Linguagem, Universidade Estadual de Campinas, Campinas, São Paulo, 2004.

DE OLIVEIRA, Jane Souto. Brasil mostra a tua cara: imagens da população brasileira nos censos demográficos de 1872 a 2000. Rio de Janeiro: Escola Nacional de Ciências Estatísticas, 2003. 75 p. ISSN 1677-7093; no. 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, F. P. M. Registros administrativos como fonte de dados estatísticos. Informática Pública, year 10, no. 1, pp. 81-93, 2008.

UNITED NATIONS POPULATION FUND. Projetos e Programas Propostos: Assistência ao Governo do Brasil (DP/FPA/BRA/3). United Nations Population Fund, 2001. Available at: https://brazil.unfpa.org/sites/default/files/pub-pdf/country_programme20022006_0.pdf. Accessed: April 29, 2024.

IEPS; UMANE; INSTITUTO VEREDAS. *Relatório Técnico nº1/2023. Saúde dos Povos Indígenas e Quilombolas.* Rio de Janeiro: IEPS, 2023.

LEAL, C. H. S. ; SCALCO, M. L. A. ; NUNES, R. P. D. ; CONSORTII, E. R. ;

KITAGAWA, B. Y. Vigilância de violências: considerações sobre as informações relativas às violências perpetradas contra a população LGBT no município de São Paulo. Bis, São Paulo, v. 2, no. 19, pp. 55-61, Dec. 2018. Available at: https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n2-diversidade-55-61.pdf. Accessed: April 19, 2024.

LOVEMAN, M. A política de um cenário de dados transformado: estatísticas etnorraciais no Brasil em uma perspectiva comparativa regional. Sociologias, v. 23, no. 56, pp. 110–153, Jan. 2021.

MELLO, Janine. Produção estatal de evidências e uso de registros administrativos em políticas públicas. In: KOGA, Natália Massaco (Ed.) et al. Políticas públicas e o uso de evidências no Brasil: conceitos, métodos, contextos e práticas. Brasília: IPEA, 2022. pp. 897-914.

MIGUEL, Nadya Maria Deps. O Perfil do brasileiro construído pelo IBGE: uma memória discursiva dos Censos Demográficos de 1940 a 2010. Thesis (Graduate Program in Social Memory) – Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2012.

OLIVEIRA, D.C. Representatividade da população LGBTQIA+ nas pesquisas epidemiológicas, no contexto da Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais: ampliar a produção de conhecimento no SUS para a justiça social. Epidemiologia e Serviços de Saúde, v. 31, no. 1, e2022020, 2022.

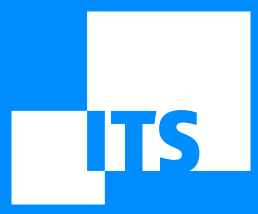
OSÓRIO, Rafael Guerreiro. O Sistema Classificatório de Cor e Raça do IBGE. Brasília: Ipea, Ministério do Planejamento, Orçamento e Gestão, 2003. (Texto para discussão, 996).

PANZARDI, R.; CALCOPIETRO, C.; IVANOVIC, E. F. New-economy sector study: electronic government and governance – lessons from Argentina. Working paper. Washington, DC: World Bank, July 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: February 14, 2024.

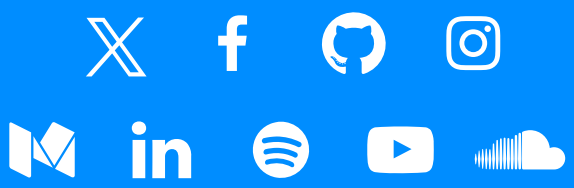
ROSENSTREICH, G. et al. Diversity Data Collection: Exploratory Mapping & Reflection. Una Europa, 2022. Available at: https://una-europa.imgix.net/resources/Diversity-Data-Collection-Exploratory-Mapping-Reflection.pdf. Accessed: February 14, 2024.

SENRA, N. de C. A questão dos registros administrativos vis-à-vis a geração de estatísticas. Revista Brasileira de Estudos de População, [S. l.], v. 13, no. 2, pp. 199–205, 1996. Available at: https://rebep.org.br/revista/article/view/437. Accessed: July 23, 2024.

WORLD BANK. Managing development: the governance dimension. Washington, D.C.: World Bank Group, 1991. Available at: http://documents.worldbank.org/curated/en/884111468134710535/Managing-development-the-governance-dimension. Accessed: February 14, 2024.



Visit our social media



itsrio.org

This book was set in the typefaces Termina, FreightSans Pro, and Public Sans and published by the Instituto de Tecnologia e Sociedade, in January 2025.