Journal of Liberty and International Affairs | Volume 9 · Number 3 · 2023 | eISSN 1857-9760
Published online by the Institute for Research and European Studies at www.e-jlia.com

Copyright © 2023 The author/s
This work is licensed under a CC-BY 4.0 license
(*) Corresponding author
Peer review method: Double-blind
Review article
DOI: https://doi.org/10.47305/JLIA2393555cs
Received: 08.09.2023 · Revised: 24.09.2023 · Accepted: 05.10.2023 · Published: 26.12.2023

DATA PROTECTION AND PRIVACY AS A FUNDAMENTAL RIGHT: A COMPARATIVE STUDY OF BRAZIL AND INDIA

Paulo Campanha Santana[1*], Faiz Ayat Ansari[2]

[1]Federal District University Centre, Brasília, Brazil https://orcid.org/0000-0002-3959-8770 ✉ pcampanhap@gmail.com
[2]KIIT School of Law, KIIT Deemed to be University, Bhubaneswar, India https://orcid.org/0000-0003-3431-4561 ✉ faizkkr@yahoo.com

Abstract: *This paper aimed to analyze how Brazil and India faced the challenge of a large amount of personal information being exchanged, stored, and analyzed. The relevance lies in the fact that data protection and privacy were concepts discussed almost everywhere in the world since the era of Big Data highlighted the challenge of protecting these fundamental rights. Therefore, the research problem was to analyze to what extent these countries effectively faced the challenge presented. The methodology used was exploratory and hypothetical-deductive. As a result, it was identified that the rights to privacy and personal data were not absolute and had to be balanced with other social interests, such as public security, law enforcement, and freedom of expression. It was concluded that inspired by international standards on the subject, such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the General Data Protection Regulation (GDPR) of the European Union, both countries had legislative protection over these rights and a framework to address them. The legislation provided fundamental principles, but only time will show their effectiveness.*

Keywords: *Data Protection; Privacy; Fundamental Rights; Brazil; India*

INTRODUCTION

Concern about privacy and data protection is not something new in society. Over the years, several normative acts have been drawn up to protect them, starting with the Universal Declaration of Human Rights of 1948 (UDHR), which expressly provides, in Article 12, that "no one shall be subject to interference in his private life".

Subsequently, in the 1970s, countries in Europe, such as Germany, France, and others, began to have regulations restricting data use, starting a movement on the topic. In 1980, the issue became part of the agenda of an international organization, such as the Organization for Economic Cooperation and Development (OECD).

The topic evolved until it reached the European Parliament and the Council of the European Union, which regulated it in 2016 but came into force in 2018, serving as a reference for numerous countries. Therefore, this article aims to analyze how Brazil and India are facing the challenge of the large amount of personal information exchanged, stored, and analyzed. The relevance lies in the fact that data protection and privacy are concepts discussed almost everywhere in the world since the current era of Big Data highlights the challenge of protecting these fundamental rights.

To this end, an exploratory and hypothetical-deductive methodology will be used to identify the legal basis and definitions of privacy and data protection. It will then address these themes in India and Brazil.

LITERATURE REVIEW

Recognizing data protection and privacy as fundamental rights is crucial to safeguarding individual autonomy, dignity, and personal space in an increasingly interconnected world. That is why the connection of data protection and privacy to fundamental rights, a quintessential constitutional law concept, is essential to be established. The person has these rights towards the state, linking it to their freedom and human dignity (Bonavides 2020, 575-576).

In a multidimensional view, it is also considered a human right (Sarlet 2009, 29). It is also related to informative self-determination, which protects the personality of citizens, especially in an information society (Mendes 2021, 69). This protection expresses the freedom and dignity of the person, and it cannot be accepted or tolerated that someone's data is used as a surveillance tool. This right should resemble the promise made by the King to the gentlemen in the year 1215, in the then Magna Carta. Before, the prohibition was imprisonment or torture. Currently, this physical body must be taken to the electronic one so that the inviolability of the individual in the electronic dimension is guaranteed (Rodotá 2008, 19).

This recognition of data protection as an autonomous fundamental right binds public authorities and private entities (Sarlet 2009, 365). As a result, the data subject's right to choose whether or not to disclose them, including their information, manifestations, and individual preferences, is directly linked to the constitutional right to privacy (Tavares 2020, 551).

Therefore, this binding of the public authorities means that specific actions are forbidden, and there must be legal resources to make them effective (Silva 2020, 189). There will be negative state competencies, and the state must abstain or not interfere with the legally guaranteed individual autonomy (Sampaio 2013, 562). This is what is called "negative protections", which is protection by prohibitions (Alexy 2015, 234).

METHODOLOGY

This research was based on an exploratory methodology to identify how Brazil and India have faced the challenges of privacy and data protection. Initially, it addresses the legal foundations and definitions, highlighting the international panorama, the impact on society, challenges, and future directions. When dealing with the countries researched, the legislation in force and its key principles were considered, and the comparative study was concluded.

LEGAL FOUNDATIONS AND DEFINITIONS

The foundation of data protection and privacy as fundamental rights can be traced back to various legal instruments. The European Convention on Human Rights (ECHR), specifically Article 8, acknowledges the right to respect for private and family life, home, and correspondence.

This forms the bedrock upon which data protection principles are built. Furthermore, the General Data Protection Regulation (GDPR), effective within the European Union (EU), enshrines the right to protect personal data as a fundamental right, emphasizing the need for consent, purpose limitation, and accountability.

International Legal Framework

Besides the documents mentioned above, several generic international law documents have laid down much emphasis on the right to privacy over some time. The Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR) underscore the significance of privacy. Article 12 of the UDHR emphasizes that "no one shall be subjected to arbitrary interference with his privacy". In contrast, Article 17 of the ICCPR asserts the right to be free from "unlawful or arbitrary interference with [one's] privacy". The emergence of the digital landscape prompted the United Nations to emphasize the importance of online privacy, advocating for protecting personal data across borders. Such internationalization has further complicated the matter, even though it has built a solid framework (Wisman 2018, 118-19). The US has also developed the American Convention on Human Rights, which deals with the said issue (Paes 2017, 225-35).

In 1980 the Organization for Economic Cooperation and Development (OECD) issued Guiding Principles on the Protection of Privacy and Cross-border Flows of Personal Data. In 1981, the Council of Europe issued Convention 108, which dealt with the protection of people concerning the automated processing of personal data, being the international instrument that is legally binding in the field of data protection, having as one of its objectives strengthening privacy protection in the digital space.

In 2016, the European Parliament and the Council of the European Union issued Regulation (EU) 2016/679 on the protection of natural persons, the processing of personal data, and the free movement of such data. It was called GDPR, whose entry into force took place on May 25, 2018. This regulation inspired legislation in several countries, including Brazil and India.

The Impact on Society

Recognizing data protection and privacy as fundamental rights has profound implications for society. As individuals share more information online, the risk of misuse and unauthorized access to personal data intensifies. Fundamental rights provide a legal framework to ensure that personal data is treated with the utmost care, limiting its collection and processing to specific, legitimate purposes. This is particularly relevant in sectors such as healthcare and finance, where sensitive data is involved.

Balancing Rights and Interests: The Individual vs. the State Debate

While data protection and privacy are essential, they are not absolute rights and must be balanced against other legitimate interests. Law enforcement and national security concerns may require limited intrusion into privacy for public safety. Striking the right balance is a challenge that legal systems grapple with, emphasizing the need for proportionality and due process.

Enforcement and Accountability: Best Examples

Local administration and government policies are pivotal to the success of a data protection regime (Stoica 2021, 96-111). Robust enforcement mechanisms are crucial to ensure the efficacy of

(cc) BY

data protection and privacy rights. Regulatory bodies, such as the Information Commissioner's Office (ICO) in the UK, are pivotal in overseeing compliance with data protection regulations. Moreover, the GDPR introduced stringent penalties for violations, reinforcing the accountability of data controllers and processors. These are some examples of relatively successful data protection policies.

Challenges and Future Directions

The digital landscape continues to evolve, presenting new data protection and privacy challenges. Emerging technologies like artificial intelligence and the Internet of Things (IoT) generate unprecedented amounts of data, necessitating adaptability in legal frameworks. The concept of data ownership, consent mechanisms, and the applicability of these rights beyond national borders are areas that require ongoing deliberation.

Data protection and privacy are fundamental rights that are pivotal in upholding individual autonomy and dignity in the digital age. Legal instruments such as the ECHR and GDPR provide the foundation for these rights, while international agreements emphasize their global significance. The balance between these rights and legitimate interests is vital, ensuring a just and secure society. As technology advances, the continual evolution of legal frameworks and enforcement mechanisms remains imperative to safeguard these fundamental rights.

The Concept of Data Protection: Balancing Privacy and Innovation

In the era of rapid technological advancement and digital transformation, the concept of data protection has gained paramount importance. As personal information is increasingly collected, processed, and utilized across various sectors, safeguarding individuals' privacy while fostering innovation has become a delicate challenge. This article delves into the intricacies of the concept of data protection, its legal foundations, principles, challenges, and its role in maintaining a harmonious equilibrium between privacy and technological progress.

The Concept of Data Protection

The concept of data protection is grounded in several fundamental principles that guide its implementation. Consent remains a cornerstone, necessitating that individuals provide informed and voluntary consent for processing their data. The purpose limitation principle ensures that data is collected for specific, legitimate purposes and not repurposed without further consent. Data minimization mandates that only necessary and relevant data be collected, limiting the potential for privacy intrusion. Data controllers are further bound by the principles of accuracy to maintain accurate records and storage limitation to retain data only for as long as necessary. It is a social, economic, and legal concern (Byhovsky 2017, 235-55).

The principles of integrity and confidentiality oblige data controllers and processors to ensure the security and protection of personal data from unauthorized access or breaches. Additionally, data subjects are granted rights such as the right to access, rectification, erasure, and portability, enhancing their control over their personal information.

Challenges and Emerging Issues

While the concept of data protection serves to empower individuals and regulate data handling practices, it faces multifaceted challenges. The balancing act between privacy protection and technological innovation is a delicate one. Striking the right equilibrium necessitates adapting regulations to evolving technologies without compromising fundamental rights.

As discussed earlier, the advent of big data, artificial intelligence (AI), and the Internet of Things (IoT) has intensified data processing capabilities. However, these advancements also raise concerns about the potential for extensive profiling, discriminatory algorithms, and potential breaches. Additionally, cross-border data flows have complicated enforcement, as differing national laws create jurisdictional challenges.

Future Directions

As technology continues to evolve, the concept of data protection must adapt to new challenges and opportunities. Striking a balance between innovation and privacy will require technological-neutral regulations to accommodate unforeseen developments. Harmonizing international standards is crucial to addressing cross-border data protection issues and facilitating seamless data flows while upholding individuals' rights.

PRIVACY

Privacy is a fundamental human right that encompasses the ability of individuals to control and safeguard their personal information, activities, and spaces from unwarranted intrusion or exposure by others, including the government and private entities. It is crucial in maintaining personal autonomy, dignity, and individuality in the digital age.

Historical Evolution of Privacy

The notion of privacy has evolved, influenced by societal, cultural, and technological changes. Ancient civilizations recognized the importance of personal boundaries, which is evident in legal and philosophical texts from Greece and Rome. However, the modern understanding of privacy took shape in the late 19th and early 20th centuries, spurred by legal scholars such as Warren and Brandeis, who articulated the right to be let alone. The concept gained prominence with the Universal Declaration of Human Rights (UDHR) in 1948, recognizing the right to privacy as an inherent human entitlement (UDHR Article 12).

Aspects of Privacy

Privacy encompasses several dimensions, including informational privacy, bodily integrity, territorial privacy, and communication confidentiality. Informational privacy involves the right to control personal data and determine its usage. This is particularly relevant in the digital era, where data breaches and surveillance challenge this aspect of privacy. Bodily integrity protects individuals

from invasive procedures and medical examinations without consent, while territorial privacy safeguards the sanctity of one's physical spaces. Communication confidentiality ensures that individuals can engage in private conversations without unwarranted interception.

Challenges in the Digital Age

As discussed earlier, the digital revolution has reshaped privacy dynamics, bringing benefits and challenges. While technology has facilitated communication and access to information, it has also led to unprecedented data collection and surveillance. Social media platforms, smart devices, and online services often collect vast amounts of personal information, raising concerns about consent, data security, and potential misuse. Government surveillance programs, justified on national security grounds, have sparked debates about the balance between security and individual privacy. It has imbibed the features of a cross-jurisdictional concept (Lee 2010, 165-200).

Balancing Privacy and Other Interests

Privacy rights are not absolute and must be balanced against other societal interests, such as public safety, law enforcement, and freedom of expression. Courts often analyze proportionality to determine whether privacy infringements are justified in specific cases. For instance, the right to privacy may be restricted when necessary to prevent crime or protect national security.

Emerging Legal Issues

Emerging technologies like artificial intelligence (AI), biometrics, and facial recognition raise novel privacy concerns. AI algorithms processing personal data may lead to automated decision-making that impacts individuals' lives without transparent explanations. Biometric data, such as fingerprints and facial scans, offer convenience but can be exploited for surveillance or identity theft. Striking the right balance between technological advancements and privacy protection is an ongoing challenge for legal frameworks.

DATA PROTECTION AND PRIVACY IN INDIA: A BRIEF OVERVIEW

Data protection and privacy have become paramount concerns in the modern digital age, where vast amounts of personal information are processed, stored, and exchanged. In India, the legal framework governing data protection has changed significantly in recent years to address these concerns. This brief overview explores the critical aspects of data protection and privacy in India, focusing on the regulatory landscape and legal safeguards.

Data Protection Legislation

India's data protection landscape has evolved with the Personal Data Protection Bill (PDPB) 2019 introduction. The PDPB aims to provide individuals greater control over their data while imposing obligations on entities handling it. It draws inspiration from international norms, particularly

the European Union's General Data Protection Regulation (GDPR), to establish principles for data processing, consent, and rights of data subjects. The recent emergence of a digital economy is also a factor that plays in the favour of legislation (Duraiswami 2017, 166-87).

Key Principles

The PDPB outlines several fundamental principles that underpin data protection in India. These include transparency, purpose limitation, data minimization, accuracy, storage limitation, and accountability. The legislation requires organizations to specify the purpose of data collection and obtain explicit consent from individuals. Additionally, data collectors must ensure data accuracy and limit storage duration to the minimum necessary for the specified purpose.

Consent and Individual Rights: The PDPB emphasizes obtaining informed and affirmative consent from data subjects. Individuals must be adequately informed about the purpose and nature of data processing before providing consent. Furthermore, the legislation grants individuals various rights, such as the right to access their data, rectify inaccuracies, erase data under certain circumstances ("right to be forgotten"), and restrict processing in specific situations.

Cross-Border Data Transfers: The PDPB acknowledges the importance of international data transfers for businesses and incorporates provisions for such transfers. It empowers the Indian government to prescribe safeguards for cross-border data transfers to ensure adequate personal data protection, aligning with GDPR's provisions for data transfers to non-EU countries.

Data Protection Authority: To oversee and enforce data protection provisions, the PDPB establishes an independent regulatory body known as the Data Protection Authority of India (DPA). The DPA is responsible for monitoring compliance, investigating breaches, and imposing penalties for violations of data protection obligations.

Challenges and Criticisms: While the PDPB represents a significant step towards enhancing data protection in India, it has also faced criticism. Some stakeholders have raised concerns about the balance between individual privacy rights and the interests of businesses. Additionally, the effectiveness of enforcement mechanisms and the autonomy of the DPA have been subject to debate.

In conclusion, data protection and privacy have gained prominence in India's legal landscape with the introduction of the Personal Data Protection Bill 2019. This legislation incorporates fundamental principles such as transparency, consent, and individual rights, aligning India's data protection framework with international norms. Establishing the Data Protection Authority of India reinforces the country's commitment to safeguarding personal data in an increasingly digital world. However, ongoing discussions and potential amendments underscore the complexity of balancing privacy rights and business interests.

However, as we write this article, the Digital Personal Data Protection Bill, 2023, is about to be tabled in the Indian Parliament. The Bill outlines the key provisions of the Data Protection Bill, emphasizing its applicability to digital personal data collected within and outside India, the requirement for lawful processing with consent, obligations of data fiduciaries, individual rights, the establishment of a Data Protection Board, and certain exemptions for government agencies.

The Bill talks about the following issues:

- Exemptions and National Security: The exemption for data processing by the state on grounds of national security might lead to excessive data collection and processing, potentially infringing upon the fundamental right to privacy. The broad scope of these exemptions raises concerns about the balance between security and privacy.
- Lack of Regulation for Harms: The Bill does not address potential harms arising from the processing of personal data, leaving individuals vulnerable to risks like identity theft, data breaches, and unauthorized usage. The absence of comprehensive regulations to mitigate these risks weakens the data protection framework.
- Missing Rights: The Bill does not grant individuals the right to data portability (the ability to transfer their data from one service provider to another) and the right to be forgotten (the right to delete personal data under certain circumstances). The absence of these rights limits individuals' control over their data.
- Transfer of Personal Data: While the Bill permits the transfer of personal data outside India, the evaluation of data protection standards in recipient countries might be inadequate. This could potentially compromise the security and privacy of individuals' data.
- Data Protection Board Appointments: The short two-year term for members of the Data Protection Board, with the possibility of reappointment, could impact the independence of the Board. A longer term might be more conducive to ensuring the Board's autonomy in overseeing data protection matters.

In summary, the Data Protection Bill's highlights underscore its aim to regulate the processing of personal data within and outside India, focusing on consent, fiduciary obligations, and individual rights. However, the key issues and analysis point out potential shortcomings such as broad exemptions for government agencies, inadequate regulation of data processing risks, the absence of specific rights for data principals, and concerns about the independence of the Data Protection Board. Addressing these concerns would be crucial to creating a robust and balanced data protection framework that safeguards individuals' privacy rights in the digital era.

DATA PROTECTION AND PRIVACY IN BRAZIL: A BRIEF OVERVIEW

In Brazil, data protection and privacy are fundamental rights provided in the Federal Constitution of 1988. Protecting these rights has been a major challenge since the hyper-connectivity because not only people but things are also connected. Below, a brief overview of how the country regulated these rights will be presented, as well as some examples of cases of affront to them, which were decided by the Judiciary.

Privacy and Data Protection

Brazil's privacy and data protection landscape is in the Federal Constitution 1988. Article 5, X, provides for the inviolability of intimacy and private life. However, not only the Constitution, the Brazilian Consumer Protection Code (Law No. 8078/90), in article 43, § 2, provides that the opening of personal and consumption data must be communicated in writing to the consumer. The Civil Code of 2002, in article 21, provides that the private life of the natural person is inviolable.

In turn, Federal Decree No. 7, 962/2013, by the Republic president, which deals with contracting in electronic commerce, requires suppliers to use effective security mechanisms for payment and processing of consumer data (Article 4, VII). In 2014, Law No. 12,965 came into effect, establishing principles, guarantees, rights, and duties for using the Internet in Brazil. It expressly protects privacy (Article 3, II) and personal data (Article 3, III), the latter following the law.

In 2018, inspired by the European Union's General Data Protection Regulation (GDPR), Brazil published its General Personal Data Protection Law (LGPD in Portuguese). After several regulatory changes, the law entered into force in different periods. In December 2018, it was Chapter IX, which deals with the National Data Protection Authority (ANPD); on August 1, 2021, administrative sanctions (chapter VIII); and, in August 2020, 24 (twenty-four) months after their publication, the other articles.

Article 1 expressly provides that the Law aims to "protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person". Article 2 of the LGPD lists several grounds for data protection, including respect for privacy (I); informative self-determination (II); the inviolability of intimacy, honor, and image (IV); human rights, the free development of personality, dignity and the exercise of citizenship by natural persons (VII).

Chapter I deals with preliminary provisions (Articles 1 to 6); II, the processing of personal data (articles 7 to 16); III, the holder's rights (Articles 17 to 22); IV provides for the processing of personal data by the public authorities (Articles 23 to 32); V, on the international transfer of data (Articles 33 to 36); and VI, of personal data processing agents (Articles 37 to 45).

Chapter VII deals with safety and good practices (Articles 46 to 51); VIII, inspection (Articles 52 to 54); IX, from the ANPD and the National Council for the Protection of Personal Data and Privacy - CNPD - (Articles 55 to 59); and X, the final and transitional provisions (Articles 60 to 65).

Article 5 of the LGPD, in its XIX paragraphs, presents several concepts, highlighting what is considered personal data, sensitive personal data, anonymized data, anonymization, and consent, among others. The CNPD holders and their alternates were appointed by Decrees issued on August 9 and September 8, both in 2021. Participation in the CNPD includes representatives from the executive branch, civil organizations, scientific and technological innovation institutions, union confederations, and business and labor sectors.

In the context of this evolution, in 2020, the Federal Supreme Court, in the Direct Action of Unconstitutionality No. 6387/Federal District, decided that data protection is an autonomous Fundamental Right. In that action, the device of Provisional Measure 954/2020, which provided for the sharing of personal data of telecommunications companies with the Brazilian Institute of Geography and Statistics (IBGE), was questioned, which was considered unconstitutional.

With this, data protection conquered a new perspective, as it has been raised to constitutional status. However, on February 10, 2022, the Federal Constitution of 1988 was amended and began to provide this protection as a fundamental right expressly. As a result, data protection becomes expressly in the constitutional mandate as a fundamental right.

Key Principles

The LGPD outlines several fundamental principles that underpin data protection in Brazil. Article 6 provides that personal data processing activities must observe good faith and the following

principles: I) purpose; II) suitability; III) need; IV) free access; V) data quality; VI) transparency; VII) security; VIII) prevention; IX) non-discrimination; and X) accountability and accountability.

Consent and Individual Rights: Article 7 of the LGPD emphasizes the cases in which the processing of personal data may occur, starting with the holder's consent. There is also the fulfillment of a legal or regulatory obligation by the controller, the protection of the life or physical safety of the holder or another person, among other hypotheses.

Cross-border data transfers: The LGPD expressly allows for international transfers of personal data to occur. In the cases provided, there is what provides that it can only be transferred to other countries or international organizations that provide a degree of protection of personal data adequate to what the Brazilian law provides and other possibilities (Article 33).

Data Protection Authority: Item XIX conceptualizes the ANPD, defining it as a public administration body or entity responsible for overseeing, implementing, and supervising compliance with the LGPD throughout the country (Article 5, XIX). The ANPD's regimental structure and position framework were approved by Federal Decree No. 10, 747, of August 26, 2020. The central body for interpreting the law establishes the rules and guidelines so that the LGPD and the National Data Protection and Privacy Policy can be implemented. The Federal Government provides information on its website, such as its composition, service channels, documents, and publications.

Challenges and Criticism: While the PDPB represents a significant step towards improving data protection in India, it has also faced criticism. One of the significant challenges of this protective law is its effectiveness, as the country has a continental dimension, with inequalities between regions. The more structured federal states have better conditions to implement the law, while the others will face major challenges.

In conclusion, data protection and privacy have constitutional status as fundamental rights. The Civil Rights Framework for the Internet, 2014, already addressed something about this, but the topic gained more attention with the LGPD. As it is a recent norm, there are many challenges to be faced, which will be overcome with the adequate infrastructure of the state and the effective performance of the control bodies and the ANPD, with due accountability of the violators of the norm.

The Bill talks about the following issues:

Exemptions: The exemption for data processing by the state for reasons of public security, national defense, state security, or activities of investigation and repression of criminal offenses may generate excessive data processing, which, to some extent, may infringe the fundamental right to privacy. Of course, these questions the ethical limit of its use.

Civil Liability for Damages: The LGPD provides sanctions for violators of the rule, but there is a discussion about civil liability, whether objective or subjective. First, liability occurs, regardless of intent or fault, if damage and a causal link exist. In the second (subjective), intent and guilt are evaluated.

Absent Right: The LGPD does not grant individuals the right and right to be forgotten, and this absence limits individuals' control over their data.Transfer of Personal Data: While the Bill permits the transfer of personal data outside India, the evaluation of data protection standards in recipient countries might be inadequate. This could potentially compromise the security and privacy of individuals' data.

Data Protection Board Appointments: The two-year term of office of the Data Protection Board members, with the possibility of reappointment, raises two questions. The established time can compromise its independence in the face of the short term, but, on the other hand, the renewal can positively impact the renewal of ideas and proposals.

In summary, the LGPD highlights indicate a broad normative field, structuring the ANPD, the CNPD, and the other bodies. There is a provision for sanctions for non-compliance, which only time can be evaluated as effective or not. The law came into force in 2020, the year the pandemic began, the moment that expanded the digital age, making people more vulnerable to hacker actions. Several cases of data leakage were reported, both in the public and private spheres. Therefore, only an adequate supervisory and civil liability system will be able to curb future infringing practices.

CONCLUSION

Data protection and privacy are fundamental rights in the contemporary digital age due to the large volume of data and information that travels between people and things. This fundamentality confers constitutional status to these rights, which are essential to guarantee the individuality and dignity of the person.

The Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) provide the right to privacy. However, the current era of Big Data gives new perspectives to this right, expanding to protect personal data. As a result, the world began to have specific legislation on the subject, gaining more significant influence from the GDPR, which came into force in 2018 and influenced several countries, including Brazil and India.

The comparative analysis of Brazil and India's right to privacy and protection concluded that both have protective norms to guarantee them. As the GDPR inspired them, they have a National Data Protection Authority, with a National Data Protection Council, in addition to other bodies. Because they are recent, the Indian law is from 2019, and the Brazilian one is from 2018. Only time will allow us to evaluate the effectiveness of these rules.

Both countries anticipate exceptions in applying the protective law, one of which pertains to national security. This exception lies within a realm of subjectivity that can potentially make individuals vulnerable.

With this, the role of control bodies is highlighted to avoid undue invasion of privacy and data in the name of supposed security.

Finally, both foresee privacy and data protection as fundamental, with adequate norms for facing the challenges of the contemporary world. However, guaranteeing the effectiveness of these norms requires a strengthened inspection system and an adequate accountability system, both administrative and civil.

(cc) BY

CRediT AUTHOR STATEMENT

Paulo Campanha Santana: Conceptualization, methodology, data curation, writing - original draft preparation and editing.
Faiz Ayat Ansari: Conceptualization, methodology, data curation, writing - original draft preparation and editing.

All authors have read and agreed to the published version of the article.

COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments:
Not applicable.

Funding:
Not applicable.

Statement of Human Rights:
This article does not contain any studies with human participants performed by any authors.

Statement on the Welfare of Animals:
This article does not contain any studies with animals performed by any authors.

Informed Consent:
Not applicable.

Disclosure statement:
No potential conflict of interest was reported by the author/s.

PUBLISHER'S NOTE

The Institute for Research and European Studies remains neutral concerning jurisdictional claims in published maps and institutional affiliations.

(cc) BY

REFERENCES

1. Alexy, Robert. 2015. *Teoria dos Direitos Fundamentais*. Tradução: Virgílio Afonso da Silva. São Paulo: Malheiros.
2. Andrei-Alexandru, Stoica. 2021. "Drones, Privacy and Data Protection," Lex ET Scientia International Journal 28, no. 2: 96-111.
3. ANPD. *Autoridade Nacional de Proteção de Dados*. Available at: https://www.gov.br/anpd/pt-br.
4. Bonavides, Paulo. 2020. *Curso de Direito Constitucional*. São Paulo: Malheiros.
5. Brazil. *Lei Geral de Proteção de Dados.* Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
6. Daniel Garrie; Irene Byhovsky. 2017. "Privacy and Data Protection in Russia," Journal of Law & Cyber Warfare 5, no. 2: 235-255.
7. Dhiraj R. Duraiswami. 2017. "Privacy and Data Protection in India," Journal of Law & Cyber Warfare 6, no. 1: 166-187.
8. General Data Protection Regulation. Available at: https://gdpr-info.eu/.
9. Lee A. Bygrave. 2010. "Privacy and Data Protection in an International Perspective," Scandinavian Studies in Law 56: 165-200.
10. Mendes, Laura Schertel; Rodrigues Júnior, Otávio Luiz; Fonseca, Gabriel Campos Soares da. 2021. "O Supremo Tribunal Federal e a Proteção Constitucional dos Dados Pessoais: rumo a um Direito Fundamental Autônomo.In: Mendes, L.S.; Doneda, D.; Sarlet, I.W.; Rodrigues Jr, O.L.*Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense.
11. Personal Data Protection Bill. 2019. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
12. R on the application of Liberty v Secretary of State for the Home Department [2018] UKSC 70.
13. RODOTÁ, Stefano. 2008. *A vida na sociedade da vigilância – a privacidade hoje*. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar.
14. SAMPAIO, José Adércio Leite. 2013. *Teoria da Constituição e dos Direitos Fundamentais*. Belo Horizonte: Del Rey.
15. SARLET, Ingo Wolfgang. 2009. *A Eficácia dos Direitos Fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.* Porto Alegre: Livraria do Advogado.
16. Silva, José Afonso da. 2020. *Curso de Direito Constitucional Positivo*. São Paulo: Malheiros.
17. Tavares Paes, Antonio. 2017. "Privacy and Data Protection in Brazil", Journal of Law & Cyber Warfare 5, no. 2: 225-235.
18. Tavares, André Ramos. 2020. *Curso de Direito Constitucional*. São Paulo: Saraiva.
19. The European Convention on Human Rights. Available at: https://www.echr.coe.int/documents/d/echr/convention_ENG
20. TijmenWisman. 2018. "Privacy and Data Protection: Fundamentally Complex," European Data Protection Law Review (EDPL) 4, no. 1 (2018). 118-119
21. The International Covenant on Civil and Political Rights. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
22. The Universal Declaration of Human Rights. 1948. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights