RCMOS – Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.
Year IV, v.1, n.2, Aug./Dec. 2024. | submission: 11/15/2024 | accepted: 11/17/2024 | publication: 11/19/2024

DIGITAL LAW IN BRAZIL: PROTECTION OF PERSONAL DATAIN CYBERSPACE

DIGITAL LAW IN BRAZIL: PROTECTION OF PERSONAL DATA IN CYBERSPACE

Sarah Emelly Lopes de Andrade
Sousa[2]

Summary
The increasing digitalization of society and the popularization of the internet have brought significant challenges to the protection of personal data in Brazil. This article addresses the impact of the General Data Protection Law (LGPD) and the Internet Civil Rights Framework on the national scenario, contextualizing the main rules and regulations aimed at security in cyberspace. In addition, it discusses the role of the National Data Protection Authority (ANPD) and the relationship between Brazilian Digital Law and international regulations, such as the European Union's General Data Protection Regulation (GDPR).Finally, it discusses a little about the main challenges in the practical implementation of the LGPD and its future prospects.
Keywords: Digital Law. Data Protection. LGPD. Internet Civil Rights Framework. Cyberspace.

Abstract
The increasing digitalization of society and the popularization of the internet have brought significant challenges to the protection of personal data in Brazil. This article addresses the impact of the General Data Protection Law (LGPD) and the Civil Framework of the Internet on the national scenario, contextualizing the main norms and regulations focused on security in cyberspace. In addition, it discusses the performance of the National Data Protection Authority (ANPD) and the relationship between Brazilian Digital Law and international regulations such as the General Data Protection Regulation (GDPR) of the European Union. Finally, it discusses a little about the main challenges in the practical implementation of LGPD and its future perspectives. **Keywords:** Digital Law. Data Protection. LGPD. Civil Internet Framework. Cyberspace.

Introduction

The digital transformation, intensified by the growing use of technologies and the popularization of the internet, has brought new demands and challenges for the protection of personal data. In Brazil, the spread of connected devices, social networks and e-commerce platforms has resulted in a massive collection of personal information, often carried out in a non-transparent manner. The protection of privacy and data security have therefore become crucial issues for contemporary society.

In response to these demands, Brazil has implemented significant regulatory frameworks, such as the General Data Protection Law (LGPD) and the Internet Civil Rights Framework. Inspired by the European Union's General Data Protection Regulation (GDPR), the LGPD seeks to ensure that personal data is processed in accordance with the principles of transparency, purpose, necessity and security. In addition, the Internet Civil Rights Framework, enacted in 2014, already represented progress by establishing rights and obligations for internet use in the country.

The main problem faced by Digital Law in Brazil regarding the protection of personal data in cyberspace lies in the challenge of ensuring the security, privacy and control of individuals' information in a virtual environment that is dynamic, global and highly interconnected. With increasing digitalization and technological advancement, large volumes of personal data are collected, processed and shared.
daily, often without the proper consent or knowledge of the holders. This puts at risk
the privacy of individuals and paves the way for abuses such as the misuse of information for
commercial purposes, data leaks and violations of fundamental rights.

The central hypothesis of this article is that the effective implementation and monitoring of the General Law of
The implementation of the General Data Protection Regulation (LGPD) in Brazil, together with the strengthening of the National Data Protection Authority (ANPD), can significantly mitigate the risks of privacy violations in cyberspace. If digital companies and organizations are able to comply with legal requirements, and if there is widespread awareness of the rights of data subjects, it is expected that there will be a significant reduction in the number of incidents related to mismanagement and misuse of personal data.

The general objective of this article is to analyze Digital Law in Brazil, with a focus on data protection. personal data in cyberspace, assessing the impact of the General Data Protection Law (LGPD) on safeguarding personal information and regulating data processing activities by organizations and companies. It will also draw a parallel with regard to the Internet Civil Rights Framework. The study seeks to understand how current legislation, together with the actions of the National Data Protection Authority (ANPD), have contributed to building a safer digital environment.

The specific objectives of this article are to analyze the main aspects of the General Data Protection Law (LGPD) in Brazil, as well as the Internet Civil Rights Framework, and to examine the role of the National Data Protection Authority (ANPD) in monitoring and regulating the protection of personal data.. Finally, it seeks to discuss a little about the main challenges in the practical implementation of the LGPD and its future perspectives.

The justification for conducting this study is based on the growing importance of protecting personal data in the digital context, especially in view of the exponential increase in the use of the internet, social networks and emerging technologies such as artificial intelligence and the Internet of Things (IoT). In Brazil, the enactment of the General Data Protection Law (LGPD) represents a milestone in the regulation of the processing of personal information, however, many challenges still persist, both in the practical implementation of the law and in raising awareness among society about its rights and duties in the digital environment.

This work was carried out through a bibliographical research, which consists of a review of the literature related to the topic addressed. For this purpose, books, periodicals, articles and Internet sites were used. According to Bervian Servo: “Conducting a bibliographical research is essential for the deepening of the topic, enabling the researcher to understand the most recent approaches and the theoretical gaps that can be explored.” (CERVO; BERVIAN, 2002, p. 65)

1. Digital Transformation and Cyberspace

With technological advancement and the popularization of the internet, the concept of cyberspace emerged as a virtual environment where social, economic and cultural interactions occur.It is also worth noting that the term Cyberspace was coined by the American writer William Gibson in 1984 in his work “Neuromancer”. He portrayed it as a virtual space composed of each computer and user connected to a global network. In another definition, according to Lévy (1998), Cyberspace refers to the “universe of digital networks as a place for encounters and adventures, a terrain for global conflicts, a new economic and cultural frontier” (p. 104). From this point of view, it can be stated that this is a digital space parallel to the physical space, controlled by individuals who assume digital identities, and are granted the power to be interconnected worldwide and access the full range of information and commands provided by the “Digital”. It is in this context that the question of the importance of protecting personal data in this virtual environment arises.

This increasing digitalization has profoundly changed the way personal data is collected, stored and processed. From basic registration information to consumer preferences, companies and online platforms accumulate large volumes of personal data for the purposes of personalizing services, targeted marketing and product development.

A relevant quote about cyberspace can be found in Manuel Castells' book, which addresses the influence of digital networks in the contemporary world: “Cyberspace has become the space of flow where the information networks that structure social, economic, political and cultural activities in the information age are organized” (CASTELLS, Manuel. *The Network Society*. 2nd ed. São Paulo: Peace and Land, 2005, p. 389)

This quote from Castells highlights cyberspace as an environment that reconfigures human interactions on a global scale, directly impacting the way personal data is collected, processed and protected on digital networks.

However, this massive volume of information, combined with the increasingly advanced use of technologies such as big data, artificial intelligence (AI) and the Internet of Things (IoT), has made privacy a topic of global concern. The inappropriate handling of personal data — whether through leaks, inappropriate sharing or excessive use — can lead to the violation of fundamental rights, such as the right to privacy and the protection of personal information.

In this context, data protection legislation seeks to mitigate these risks by establishing standards and responsibilities for the processing of information in the digital environment. In Brazil, the LGPD and the Internet Civil Rights Framework play central roles in this regulatory effort.

The scholar Ingo Sarlet states that "The protection of personal data plays a fundamental role in the contemporary legal system, reflecting a new dimension of the right to privacy and intimacy, both guaranteed by the Federal Constitution of 1988" (SARLET, Ingo Wolfgang. *The effectiveness of fundamental rights*. 11th ed. Porto Alegre: Lawyer's Bookstore, 2021).

This quote provides a doctrinal view of the LGPD and its connection with fundamental rights, reinforcing the importance of this legislation for the preservation of human dignity in the digital context.

2. The General Data Protection Law (LGPD)

The General Data Protection Law (LGPD), enacted in 2018 and in force since 2020, is the most important regulatory framework in Brazil for the protection of personal data. Inspired by the GDPR, the LGPD establishes a set of principles and rules that guide the processing of personal data by both public and private entities. Among its main points are the definition of the legal bases for data processing, the rights of data subjects and the sanctions applicable in case of non-compliance.

2.1 Legal Basis and Principles

The General Data Protection Law (LGPD) defines ten legal bases that authorize the processing of personal data, with the aim of ensuring that activities involving data are carried out in a lawful, fair and transparent manner. These bases are essential for data processing to comply with the legislation and guarantee respect for the rights of data subjects. The ten legal bases are described in Art. 7 of the LGPD and are as follows:

the) Consent of the holder: The processing is authorized when the holder freely consents, informed and unequivocal with the use of your data for specific purposes.
b) Compliance with a legal or regulatory obligation: Processing is permitted when necessary for compliance with an obligation imposed by law or regulation to which the data controller is subject.
c) Execution of public policies: The processing may be carried out by the public administration for the execution of public policies, provided for in laws or regulations, or even based on contracts, agreements or similar instruments.
d) Conducting studies by research bodies: Data processing is permitted when necessary for conducting studies by research bodies, ensuring, whenever possible, the anonymization of the data.
e) Execution of a contract or preliminary procedures related to a contract: When processing is necessary for the execution of a contract to which the data subject is a party, or for preliminary procedures to his request.
f) Regular exercise of rights in judicial, administrative or arbitration proceedings: The processing is authorized to guarantee the exercise of rights in judicial, administrative actions or in arbitration proceedings.
g) Protection of the life or physical integrity of the data subject or third parties: Data processing is permitted when necessary to protect the life or physical integrity of a person, whether the data subject or third parties.
h) Health protection, exclusively, in a procedure carried out by health professionals, health services or health authorities: This legal basis allows the processing of data for health protection, provided that it is carried out by professionals in the area, health institutions or health authorities. i) Meeting the legitimate interests of the controller or third parties: The processing may be carried out based on the legitimate interest of the controller or third parties, provided that this interest does not prevail over the fundamental rights and freedoms of the data subject.
j) Credit protection: Data processing is authorized when necessary for credit protection, under the terms of the Consumer Protection Code.
k)

These legal bases are the foundations that legitimize the processing of personal data, and it is essential that data controllers identify which of them applies in each situation, in order to ensure compliance with the LGPD and guarantee the protection of the rights of data subjects.

Furthermore, the legislation (LGPD) also establishes fundamental principles that must be followed. in the processing of personal data. These principles ensure that the processing is carried out responsibly and in accordance with the law, respecting the rights of data subjects. The main principles of the LGPD are described in Art. 6 and are as follows:

the) Purpose: The processing of personal data must be carried out for legitimate purposes, specifically specific and explicit, informed to the holder, and cannot be used for purposes other than those for which the data were collected.

b) Adequacy: Data processing must be compatible with the purposes informed to the data subject. home, according to the context of the treatment.
c) Necessity: The data processed must be strictly necessary to achieve the intended purposes. The collection of excessive or irrelevant data in relation to the purpose must be avoided. d) Free access: The data subject has the right to consult, easily and free of charge, information about the processing of his/her personal data, and companies must guarantee continuous access to this information.

e) Data quality: Personal data must be accurate, clear, relevant and up-to-date, in accordance with the need and purpose of its processing.
f) Transparency: Data subjects must be informed in a clear, accessible and complete manner about the processing of their data, including the identification of those responsible and the purposes of the processing.
g) Security: The protection of personal data must be guaranteed against unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination.
h) Prevention: Measures must be adopted to prevent harm to data subjects resulting from the processing of their personal information.
i) Non-discrimination: The processing of personal data may not be carried out for discriminatory, unlawful or abusive purposes.
j) Accountability and accountability: The data controller must be able to demonstrate that it adopts effective measures capable of complying with data protection standards and that it ensures compliance with the LGPD.

These principles guide all data processing activities, ensuring that the rights of data subjects are respected and that processing occurs in an ethical, secure and transparent manner.

The law also guarantees rights such as access, rectification and deletion of data, as well as the right to portability, guaranteeing greater autonomy for citizens.

2.2 Rights of Data Subjects and Liability of Companies

The protection granted by the LGPD includes a set of rights guaranteed to data subjects, who have the prerogative to control how their information is used. Informed consent is central to the relationship between companies and data subjects, with the requirement that the individual be previously informed about the purposes of the processing.

Furthermore, the law introduces severe sanctions for violations, which may include fines of up to 2% of the company's annual revenue, capped at R$50 million per violation, which reinforces companies' responsibility regarding security and transparency in data processing.

In its articles 18, 19 and 20 it is listed:

Art. 18. The holder of personal data has the right to obtain from the controller, in relation to the data of the holder processed by him, at any time and upon request:
I - confirmation of the existence of processing;
II - access to data;
III - correction of incomplete, inaccurate or outdated data;
IV - anonymization, blocking or deletion of unnecessary, excessive data or data processed in non-compliance with the provisions of this Law;
V - portability of data to another service or product provider, upon express request, in accordance with the regulations of the national authority, observing commercial and industrial secrets; (As amended by Law No. 13,853, of 2019) Validity
VI - deletion of personal data processed with the consent of the holder, except in the cases provided for in art. 16 of this Law;
VII - information on public and private entities with which the controller shared data;

VIII - information on the possibility of not providing consent and on the consequences of refusal;
IX - revocation of consent, pursuant to § 5 of art. 8 of this Law.
§ 1 The holder of personal data has the right to file a petition regarding his/her data against the controller before the national authority.
§ 2 The holder may object to processing carried out based on one of the hypotheses of waiver of consent, in the event of non-compliance with the provisions of this Law.
§ 3 The rights provided for in this article will be exercised upon express request by the holder or legally constituted representative to the processing agent.
§ 4 If it is impossible to immediately adopt the measure referred to in § 3 of this article, the controller will send the holder a response in which he/she may:
I - communicate that it is not a data processing agent and indicate, whenever possible, the agent; or II - indicate the reasons in fact or in law that prevent the immediate adoption of the measure.
§ 5 The request referred to in § 3 of this article will be processed at no cost to the holder, within the timeframes and under the terms set forth in the regulations.

§ 6º The person responsible must immediately inform the processing agents with whom the data has been shared of the correction, deletion, anonymization or blocking of the data, so that they may repeat the same procedure, except in cases where this communication is demonstrably impossible or involves a disproportionate effort. (As amended by Law No. 13,853 of 2019) Validity

§ 7 The portability of personal data referred to in item V of the caput of this article does not include data that has already been anonymized by the controller.

§ 8º The right referred to in § 1º of this article may also be exercised before consumer protection bodies.

Art. 19. Confirmation of existence or access to personal data will be provided upon request by the holder:

I - in simplified format, immediately; or

II - by means of a clear and complete declaration, indicating the origin of the data, the non-existence of registration, the criteria used and the purpose of the processing, taking into account commercial and industrial secrets, provided within a period of up to 15 (fifteen) days, counting from the date of the holder's request.

§ 1º Personal data will be stored in a format that favors the exercise of the right of access. § 2º Information and data may be provided, at the discretion of the holder:

I - by electronic means, secure and suitable for this purpose;

or II - in printed form.

§ 3 When the processing originates from the consent of the holder or from a contract, the holder may request a full electronic copy of his/her personal data, taking into account commercial and industrial secrets, under the terms of the regulations of the national authority, in a format that allows its subsequent use, including in other processing operations.

§ 4 The national authority may make different provisions regarding the deadlines provided for in items I and II of the caput of this article for specific sectors.

Art. 20. The data subject has the right to request a review of decisions taken solely on the basis of automated processing of personal data that affect his or her interests, including decisions intended to define his or her personal, professional, consumer and credit profile or aspects of his or her personality.

The LGPD strikes a balance between the rights of data subjects and the responsibilities of companies that process this information. In addition to ensuring that data processing complies with legal bases, companies must adopt strict protection, communication and transparency measures to ensure respect for individuals' privacy. At the same time, data subjects have at their disposal a set of legal tools to exercise control over their personal data and ensure its security in the digital environment.

3. The Internet Civil Rights Framework

Although the LGPD is the main data protection legislation in Brazil, the Marco Civil da Internet, enacted in 2014, is considered the “constitutional framework” of the internet in Brazil. It establishes rights and duties for the use of the internet, with a focus on protecting privacy, freedom of expression and net neutrality.

The Brazilian Civil Rights Framework regulates the collection and storage of browsing data, and ensures that internet service providers are not held liable for content posted by third parties unless they fail to comply with court orders. This framework was a pioneer in establishing privacy as a fundamental right on the internet, paving the way for the LGPD.

A relevant quote about the Internet Civil Rights Framework can be extracted from the text of the legislation itself, which highlights its role as a regulator of rights and duties in the digital environment: “The Internet Civil Rights Framework establishes the principles, guarantees, rights and duties for the use of the Internet in Brazil, ensuring the protection of privacy, freedom of expression and net neutrality” (BRAZIL. Law No. 12,965, of April 23, 2014.*Internet Civil Rights Framework*, Art. 3).

Another important quote can be found in the work of Ronaldo Lemos, one of the main articulators of the Civil Framework:

> “The Internet Civil Rights Framework represents a significant advance in the regulation of the digital environment, by guaranteeing fundamental rights, such as freedom of expression and data protection, while establishing clear responsibilities for network providers and users” (LEMOS, Ronaldo.*The Civil Rights Framework for the Internet*. New York: Oxford University Press, 2015).

These quotes reflect the importance of the Marco Civil as a regulatory basis for internet governance in Brazil, especially on issues related to privacy, security and fundamental rights of users.

4. The National Data Protection Authority (ANPD)

With the implementation of the LGPD, the National Data Protection Authority (ANPD) was created, a regulatory body responsible for ensuring the application of the law. The ANPD plays a crucial role in monitoring data processing activities in Brazil, defining complementary standards and applying sanctions in case of violations of the legislation.

The ANPD's mission is to promote awareness about the importance of data protection, in addition to acting as a mediator between the rights of data subjects and the needs of companies. Its role is essential to ensure a balance between technological innovation and respect for privacy.

In the book*Personal Data Protection: The Role and Limits of Consent*, Bruno Ricardo Bioni addresses the regulatory function of the National Data Protection Authority (ANPD), highlighting its central role in the application and monitoring of the General Data Protection Law (LGPD). Bioni discusses how the ANPD is responsible for guiding and regulating the processing of personal data in Brazil, in addition to acting as a mediator between the rights of data subjects and the interests of organizations that process such data.

He also highlights the importance of the ANPD as an entity that must promote a balance between data protection and technological innovation, ensuring that the interpretation and application of the LGPD is uniform and effective. However, Bioni warns of the challenges that the authority faces in terms of autonomy and institutional structure to perform its regulatory role effectively.

These points make it clear that the author recognizes the ANPD as fundamental in the governance of privacy and data protection in Brazil, but with reservations regarding its independence and ability to act in a constantly evolving regulatory environment.

5. Harmonization with the General Data Protection Regulation (GDPR)

The LGPD largely mirrors the provisions of the European Union's General Data Protection Regulation (GDPR), which is considered the most stringent and comprehensive legislation on the subject in the international arena. Both laws share an approach of accountability and transparency, where companies need to demonstrate compliance with the regulations.

However, some differences remain, especially regarding sanctions and the role of national authorities. The GDPR, for example, adopts a stricter stance on certain aspects, such as fines, which can reach 4% of a company's global turnover. However, the similarity of the laws facilitates mutual recognition between jurisdictions, allowing the flow of data between Brazilian and European companies, as long as there is compliance with both standards.

6. Implementation Challenges and Future Perspectives

While the LGPD has set an important milestone for data protection in Brazil, its implementation still faces significant challenges. Many companies are still adapting to the legal requirements, while public understanding of privacy rights continues to evolve.

Many institutions still do not have a clear understanding of the obligations and rights established by the LGPD. Lack of awareness can result in non-compliance. Therefore, the need for training and qualification of employees regarding data protection is crucial, as the success of implementation depends on the involvement of all levels of the organization.

The data protection landscape is constantly changing, driven by both technological advances and changing societal demands for privacy. As new technologies emerge and become part of everyday life, legislation needs to evolve to keep up with the challenges and ensure that the rights of the holders continue to be protected.

The ability to adapt to new technologies is one of the biggest challenges for the future. With the rise of emerging technologies such as artificial intelligence and the Internet of Things, regulations on data collection and use must be constantly updated. In addition, international cooperation and harmonization of standards between different countries are essential to ensure effective global protection of personal data.

Finally, digital education also plays a key role. Raising awareness among users about their rights and how their information is used is crucial for the digital ecosystem to function.

operate ethically and safely.

Conclusion

The laws analyzed play a crucial role in protecting personal data in cyberspace, establishing strict standards and guaranteeing rights to data subjects. The effectiveness of these standards not only contributes to the protection of individual privacy, but also strengthens citizens' trust in the digital environment. The ongoing challenge will be to ensure compliance and adaptation of these laws in the face of technological innovations and changes in data processing practices.

Data protection in cyberspace is a complex and constantly evolving issue that requires coordinated efforts between governments, companies and citizens. With legislation such as the GDPR, LGPD and the Marco Civil da Internet, significant advances have been made to ensure greater security and transparency in the processing of personal information. However, with the emergence of new technologies and cyber threats, adapting and updating these regulations will be essential to ensure that data subjects' rights continue to be protected in the future.

The role of companies goes beyond simply complying with regulations: they need to adopt a culture of privacy and responsibility, incorporating data protection into every step of their operations. Likewise, the government has the responsibility to monitor, educate and promote a safe digital environment for everyone.

The actions of the ANPD and international cooperation to harmonize legislation are essential to ensure that citizens' rights are protected in the digital environment.

Implementing the LGPD is a complex process that requires commitment and continuous effort from organizations. By addressing these challenges, companies can not only comply with legal requirements but also build an environment of trust with their customers and partners, promoting the protection of personal data as a core value in their operations.

Finally, educating users themselves is essential. Only with a clear understanding of the risks and rights will individuals be able to fully exercise their digital citizenship, protecting their information in an increasingly connected environment.

References

GIBSON, William. *Neuromancer*. Ace Books, 1984

LEVY, Pierre. *Cyberculture*. New York: Routledge, 1998, p. 104

CERV, P. and BERVIAN, P.A. *Scientific methodology*. 5th ed. New York: Pearson Prentice Hall, 2002, p. 65

CASTELLS, Manuel. *The Network Society*. 2nd ed. São Paulo: Peace and Land, 2005, p. 389

SARLET, Ingo Wolfgang. *The effectiveness of fundamental rights*. 11th ed. Porto Alegre: Lawyer's Bookstore, 2021

BRAZIL. Law No. 12,965 of April 23, 2014. *Internet Civil Rights Framework*, Art. 3

READ, Ronaldo. *The Civil Rights Framework for the Internet*. New York: University of Chicago Press, 2010

BIONI, Bruno Ricardo. Protection of personal data: The function and limits of consent. São Paulo: Courts Magazine Publisher, 2020

SILVA, Alexandre Ribeiro da; BEZERRA, Francisco Wellery Gomes. Space and Cyberspace: The Construction of Subjectivity in the Digital Age. Id on Line Rev.Mult.Psic., October/2020, vol.14, n.52, p. 475-484. ISSN: 1981-1179

READ, Ronaldo. *The Civil Rights Framework for the Internet*. New York: University of Chicago Press, 2015

DALL'ACQUA, Alexandre. *LGPD: General Personal Data Protection Law*. New York: Courts Publishing House, 2020

GONCALVES, Rafael. *Privacy and Data Protection: An Analysis of the General Data Protection Law and the Internet Civil Rights Framework*. Curitiba: Juruá, 2020

ANPD. "Activity Report 2020-2021". National Data Protection Authority. Available at: www.gov.br/anpd

FARIA, Fabrício. "The Challenges of LGPD for Brazilian Companies". *Brazilian Journal of Digital Law*, v. 2, n. 1, 2021

MARTINS, Pedro. "Impacts of LGPD on the Digital Market". *Law and Technology Journal*, v. 3, n. 2, 2021

BRAZIL. Law No. 13,709, of August 14, 2018. *General Law on the Protection of Personal Data*. Available at: www.planalto.gov.br

BRAZIL. Law No. 12,965 of April 23, 2014. *Internet Civil Rights Framework*. Available at: www.planalto.gov.br

ANPD. "Guide to Good Practices for the Protection of Personal Data". Available at: www.gov.br/anpd

BRAZIL. *General Data Protection Law comes into force*. Federal Senate, September 18, 2020. Available at: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor. Accessed on: November 5, 2024.

BRAZIL. *General Data Protection Law (LGPD)*. Ministry of Sports. Available at: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd. Accessed on: November 5, 2024.

SILVA, Taziane Mara da; TEIXEIRA, Talita de Oliveira; FREITAS, Sylvia Mara Pires de. Cyberspace: a new configuration of being in the world. *Psychology in Review*, Belo Horizonte, v. 21, n. 1, p. 176-196, Apr. 2015.

BOFF, Salete Oro; FORTES, Vinícius Borges. Privacy and protection of personal data in cyberspace as a fundamental right: perspectives for building a regulatory framework for Brazil. *Sequence (Florianopolis)*, n. 68, p. 109-127, jun. 2014.

SILVA, Danilo Morais da; FERNANDES, Valdir. Cyberspace, cyberculture and metaverse: virtual society and cyber territory. *Humanities and Innovation Journal*, v. 8, n. 67, 2021.