LUMEN ET VIRTUS
ISSN: 2177-2789

CIVIL LIABILITY OF COMPANIES AND THE PROCESSING OF PERSONAL DATA: PROTECTION OF PERSONAL DATA AND CIVIL LIABILITY OF SUPPLIERS OF SERVICES OR PRODUCTS IN CASE OF LEAKAGE OF CONSUMER DATA[1]

https://doi.org/10.56238/levv16n47-062

Submitted on: 18/03/2025 **Publication date:** 18/04/2025

Yan Lucas Silva Corrêa[2], Henry Guilherme Ferreira Andrade[3].

ABSTRACT

This article analyzes the civil liability of companies in the processing of personal data, focusing on consumer protection and the prevention of information leaks. The General Data Protection Law (LGPD) establishes a legal framework for information security, imposing on companies the duty to adopt effective technical and administrative measures to protect personal data against unauthorized access and security incidents. It addresses the fundamentals of data protection in the Brazilian legal system, based on the Federal Constitution and the LGPD, highlighting the rights of data subjects and the duties of data controllers and operators. It also explores strict civil liability in consumer relations, according to the Consumer Protection Code (CDC), which establishes that suppliers of services and products must repair damages caused by failures in data processing, without the need to prove fault. It discusses the duty of information security, emphasizing the preventive measures that companies must adopt, such as encryption, multi-factor authentication, and compliance policies. Finally, the article addresses the legal consequences of data leaks, including administrative sanctions provided for by the LGPD, the civil liability of companies, and the reputational, financial, and legal implications, both for material and moral damages caused to consumers. The method used in this research was dialectical and deductive, being through the reading of articles and books, as well as the analysis of various legislations of the Brazilian legal system.

Keywords: Violation of Rights. Data Protection. Liability. Data Leakage.

[1] Article presented to the Bachelor's Degree in Law of the Institute of Higher Education of Southern Maranhão – IESMA/Unisulma.

[2] Academic of the Bachelor of Laws course at the Institute of Higher Education of Southern Maranhão – IESMA/Unisulma.
E-mail: yannlsc255@gmail.com

[3] Advisor Professor. Master in Sociology (UFMA). Specialist in Civil and Business Law (Damásio de Jesus Foundation – FDDJ) Professor of the Bachelor's Degree in Law at the Institute of Higher Education of Southern Maranhão – IESMA/Unisulma.
Email: henry.andrade@unisulma.edu.br

INTRODUCTION

Technological advancement and the growing digitalization of commercial and social relations have brought with them a series of benefits, but also significant challenges, especially with regard to the protection of privacy and security of personal data (CAPANEMA, 2020).

Personal data is information relating to an identified or identifiable natural person, which, when mismanaged, can cause irreparable damage to your privacy and security. With the increasing collection, storage and processing of data, especially in digital platforms and e-commerce services, there is an urgent need for a robust regulatory framework that regulates and protects the rights of individuals (BLUM, 2018).

In this context, the General Data Protection Law (LGPD), established by Law No. 13,709/2018, represented a significant advance in the regulation of data processing in Brazil, in line with international regulations, such as the European Union's General Data Protection Regulation (GDPR) (BIONI, 2018).

The LGPD aims to protect the privacy of individuals, establish clear rules for the processing of personal data, and create an accountability system for companies that handle this information.

With the LGPD in force, organizations are now responsible for adopting appropriate security measures, informing their consumers about the use of their data, and ensuring that the rights of data subjects are respected. The violation of these rights can generate serious consequences for companies, including civil liability, both for property and moral damages caused to data subjects, especially in case of leaks or misuse of personal information (BLUM, 2018).

The responsibility of companies in the event of a personal data leak is one of the most relevant aspects of the LGPD and is directly intertwined with consumer relations. According to the Consumer Protection Code (CDC), the civil liability of companies in cases of failures in the provision of services, such as inadequate data processing, is objective. This means that companies can be held liable for the damages caused, regardless of fault, as long as the defect or failure in the service offered is proven (BIONI, 2018).

In this sense, the CDC and the LGPD converge, establishing a protection network for the consumer, who can be significantly affected by the violation of their privacy.

Thus, the protection of personal data as a whole is necessary. Thus, in this context, Law No. 13,709/2018 or, as it is better known, the General Data Protection Law (LGPD) emerged. This law came to the Brazilian legal system to provide for the processing of personal data, whether by physical or digital means.

In addition, information security has become an essential duty for companies that deal with personal data. Organizations must adopt a series of preventive and corrective measures to ensure that their security systems are adequate and that personal data is protected from unauthorized access and security incidents, such as information leakage. Failure to adopt these measures can result in direct and indirect damage to data subjects and compromise the reliability and reputation of companies, in addition to giving rise to the application of sanctions by the National Data Protection Authority (ANPD), which is the body responsible for overseeing compliance with the LGPD (CAPANEMA, 2020).

This article aims to explore the civil liability of companies in the processing of personal data, with an emphasis on the legal consequences and reparation of damages arising from data leaks.

The fundamentals of personal data protection in the Brazilian legal system, the strict liability of companies in the context of consumer relations, the duty of information security and the sanctions imposed by the LGPD and other relevant legislation will be analyzed.

The discussion also covers the good practices that companies should adopt to avoid security incidents and mitigate the risks of harm to data subjects. In the end, it is intended to highlight the importance of compliance with data protection standards and the adoption of an information security culture, which not only avoids legal consequences, but also reinforces consumer confidence and the sustainability of companies in the market.

Thus, with the advance of the digitalization of business relations and the growing dependence on personal data in the context of modern economies, the civil liability of companies for failures in the protection of this data assumes a central role in the contemporary legal debate. The implementation of adequate security practices, in line with the principles of the LGPD, not only fulfills a legal function, but also preserves consumer trust, ensuring that the fundamental rights to privacy and data protection are respected, even in an environment of constant technological transformations (BIONI, 2018).

For this, it is necessary to read the General Data Protection Law, especially on the foundations, principles, concepts used by the law and the articles that discuss the processing of personal data. It is also essential to verify the Civil Code, the Consumer Protection Code and the Federal Constitution, especially the articles that deal with civil liability, especially on subjective and objective liability, of consumer rights in relation to the Internet and the fundamental rights guaranteed therein.

In addition, scientific articles, monographs, dissertations and doctrines on the civil liability of the supplier, consumer rights in the Internet age and the General Data Protection Law were read.

FOUNDATIONS OF PERSONAL DATA PROTECTION IN THE BRAZILIAN LEGAL SYSTEM

With the advancement of information technologies and the growing digitalization of social relations, the processing of personal data has become a central element for the functioning of companies, public agencies, and digital platforms. Given this scenario, concern about the protection of this data has also grown, especially regarding its misuse, leaks, and privacy violations. In Brazil, the protection of personal data has come to be expressly recognized as a fundamental right, finding support in the Federal Constitution and, more recently, in Law No. 13,709/2018 – the General Law for the Protection of Personal Data (LGPD) (CAPANEMA, 2020).

Currently, we live in the age of technology, in which one of its great characteristics is the absence of borders. This was possible, especially, with the invention of the Internet, given that access to information became easier, as well as communication between people (ARABI, 2017).

The Federal Constitution of 1988, in its article 5, items X and XII, already ensured the inviolability of the intimacy, private life and communications of individuals, providing for the right to compensation in case of violation. However, it was with the advent of the LGPD that the Brazilian legal system began to regulate the processing of personal data in a systematic and specific manner, establishing principles, rights, and duties for all parties involved, including private companies, public authorities, and individuals. (CAPANEMA, 2020). The LGPD was inspired by the European Union's General Data Protection Regulation (GDPR), and represents a milestone in the consolidation of the right to data protection as an autonomous right, linked to the dignity of the human person. The law defines personal data as any information related to an identified or identifiable natural person, ranging from name and CPF to consumption habits and location. In addition, it introduces the concept of sensitive data, which deserve an even greater degree of protection, such as racial origin, religious conviction, political opinion, health data, and biometrics (BIONI, 2018).

One of the main pillars of the LGPD is the set of principles that guide the processing of personal data. Among them, the following stand out: the purpose, which requires processing for legitimate, specific and explicit purposes; necessity, which imposes the

limitation of processing to the minimum necessary; transparency, which ensures the holder clear and easy access to information about his or her data; and security, which determines the adoption of technical and administrative measures to protect data against unauthorized access, leaks, and other forms of improper treatment (CAPANEMA, 2020).

Another key aspect is the recognition of the rights of data subjects, which include, among others, the right to access, correction, anonymization, portability, revocation of consent and deletion of data. Companies that process personal data, in turn, have a duty to clearly inform how the data will be used, for how long it will be stored, and with whom it will be shared. This set of guarantees aims to strengthen the individual's autonomy over their personal information and promote greater balance in the relationships between consumers and suppliers of products or services (BLUM, 2018).

In the face of this new reality, although there have been great technological advances, great dangers have also emerged. These dangers arise when data manipulation is done abusively or incorrectly by companies, which can hurt the rights guaranteed in the Federal Constitution, such as the right to privacy. The threat to data occurs because it has an intimate nature, and it is possible, through processing, to identify someone's personal information, or even to identify an individual (BLUM, 2018).

Thus, it is essential that the Law evolves and adapts to be able to protect the rights of society in this new reality, creating an imbricated relationship between Law and Technology. The need for legislation in order to remedy the legal vacuum in relation to the Internet has become evident worldwide (CAPANEMA, 2020).

The LGPD also establishes the figures of the data controller and operator. The controller is the natural or legal person responsible for decisions regarding data processing, while the operator performs the processing on behalf of the controller. Both figures are subject to liability in case of security incidents or non-compliance with legislation, as will be addressed in later sub-themes of this article (CALAZA, 2024). Finally, it is important to note that the enactment of Constitutional Amendment No. 115/2022, which included the protection of personal data in the list of fundamental rights and guarantees, consolidated the understanding that this is a basic right of the Brazilian citizen, to be respected by all entities of the federation. This amendment also gave the Union the exclusive competence to legislate on the matter, reinforcing the need for uniformity and effectiveness in public policies and in the regulation of data protection.

Thus, the legal foundations of personal data protection in Brazil rest on a robust and constantly evolving regulatory framework, which seeks to balance the economic interests of companies with the fundamental rights of citizens. The civil liability of

companies in case of failures in this processing will be one of the aspects that we will delve into in the next topics, highlighting the importance of ethical, transparent, and safe practices in the use of personal data (CALAZA, 2024).

In turn, Brazil, inspired by European law, passed Law No. 13,709 in August 2018, called the "General Law for the Protection of Personal Data" (LGPD). Although this law was only approved in 2018, there was an eight-year pedagogical process on the discussion of personal data protection in the country.

Thus, there was its first draft in 2010, when the Ministry of Justice launched the first public consultation of a Draft Law. The LGPD's main focus is to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person.

In direct relation to the new reality of the pandemic, therefore, there were several discussions about the entry into force of Law No. 13,709/2018, which was expected, according to article 65, item II, of said law, to take place in August 2020. In fact, the LGPD effectively came into force in September 2020, putting an end to the tumultuous period of *vacatio legis* of the aforementioned law, with the publication of Law No. 14,058/20.

That said, the aforementioned law seeks to merge the interests of legal entities, data handlers, and individuals, data holders. This combination of interests occurs in article 2 of the General Data Protection Law, *in verbis*:

> Art. 2 The discipline of personal data protection is based on:
> I - respect for privacy;
> II - informational self-determination;
> III - freedom of expression, information, communication and opinion;
> IV - the inviolability of intimacy, honor and image;
> V - economic and technological development and innovation;
> VI - free enterprise, free competition and consumer protection;
> VII - human rights, the free development of personality, dignity and the exercise of citizenship by natural persons.

It is verified that the law protects respect for privacy and the inviolability of intimacy, as well as guarantees the right to free competition and economic development. Thus, a balance of rights is guaranteed.

STRICT CIVIL LIABILITY IN CONSUMER RELATIONS

The liability of suppliers of products or services for damages resulting from the leakage of consumers' personal data is supported not only by the General Data Protection Law (LGPD), but also by the Consumer Protection Code (CDC). The latter establishes the regime of strict civil liability in consumer relations, which means that, for the configuration

of the duty to indemnify, proof of fault of the supplier is not required, the occurrence of the damage, the defect in the service or product and the causal link are sufficient (BLUM, 2018).

Article 14 of the CDC is clear in providing that the supplier is liable, regardless of fault, for the repair of damages caused to consumers by defects related to the provision of services. Thus, in cases of data leakage, the failure to provide the service – embodied in the absence of effective information security mechanisms – can be understood as a defect that generates indemnification liability (CALAZA, 2024). The application of strict liability in the event of security incidents involving personal data is especially relevant in times of intense digitalization, in which companies hold and process vast volumes of consumer information. The expectation that such data will be properly protected is legitimate, and its violation constitutes a breach of trust that underlies the consumer relationship. In this sense, the inadequate treatment of data or the undue exposure of sensitive information constitutes a defective service, giving rise to the duty to repair the damage caused (DE SOUZA; ANDRÉ, 2025).

In addition, the LGPD reinforces this understanding by providing, in its article 42, that the data controller or operator who, due to the exercise of personal data processing activities, causes property, moral, individual or collective damage, will be liable for this damage. Liability can be excluded only if the agent demonstrates that it did not process data, that there was no violation of the legislation or that the damage was due exclusively to the fault of the holder or third parties (SOUZA, 2025).

The merger of the LGPD regime with the CDC strengthens the consumer's position in the face of security incidents, since both legal diplomas seek to ensure the dignity of the human person, transparency in contractual relations and protection against risks arising from economic activity.

In addition, the Superior Court of Justice (STJ) has already taken a position in favor of the liability of companies in cases of data leakage, recognizing strict liability and admitting compensation for moral damages even in the absence of proof of direct material damage, given the violation of privacy and trust (DE OLIVEIRA, 2025).

It is important to highlight that civil liability in consumer relations also has a pedagogical and preventive function, by encouraging suppliers to invest in data protection measures, secure technologies, and digital compliance programs. At the same time, it promotes justice for the data subject, who is often placed in a situation of vulnerability and public exposure, with profound impacts on his or her personal and professional life (DE SOUZA; ANDRÉ, 2025).

Another relevant point is the possibility of joint and several liability between different processing agents, as established by the LGPD. If there is more than one company involved in the data processing cycle (for example, a controlling company that outsources storage to another), both may be held jointly and severally liable to the data subject for the damages caused. This reinforces the need for well-structured contracts and governance practices between trading partners, to mitigate risks and ensure compliance with legislation (DE OLIVEIRA, 2025).

In view of this scenario, it is evident that strict civil liability represents an important tool for consumer protection in the information society. Its application, combined with the principles and provisions of the LGPD, imposes on companies a redoubled duty of caution and diligence in the processing of personal data, under penalty of administrative sanctions and indemnification obligations (BLUM, 2018).

The liability of suppliers, therefore, should not be seen only from a sanctioning perspective, but as a mechanism of balance in legal relations, essential to the promotion of a more ethical, safe, and transparent digital environment.

Thus, both parties to the data processing relationship must pay attention to and act in accordance with such principles listed in article 6 of the LGPD:

> Article 6 - Personal data processing activities must observe good faith and the following principles:
> VIII - purpose: carrying out the processing for legitimate, specific, explicit and informed purposes to the data subject, without the possibility of further processing in a way that is incompatible with these purposes;
> IX - adequacy: compatibility of the processing with the purposes informed to the data subject, according to the context of the processing;
> X - necessity: limitation of the processing to the minimum necessary for the achievement of its purposes, with the scope of pertinent data, proportional and not excessive in relation to the purposes of the data processing;
> XI - free access: guarantee, to the holders, of easy and free consultation on the form and duration of the processing, as well as on the completeness of their personal data;
> XII - data quality: guarantee, to the holders, of the accuracy, clarity, relevance and updating of the data, according to the need and for the fulfillment of the purpose of its processing;
> XIII - transparency: guarantee, to the data subjects, of clear, precise and easily accessible information about the processing and the respective processing agents, observing commercial and industrial secrets;
> XIV - security: use of technical and administrative measures capable of protecting personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination;
> XV - prevention: adoption of measures to prevent the occurrence of damage due to the processing of personal data;
> XVI - non-discrimination: impossibility of carrying out the processing for unlawful or abusive discriminatory purposes;
> XVII - Accountability and accountability: demonstration, by the agent, of the adoption of effective measures capable of proving compliance with the rules for the protection of personal data, and even of the effectiveness of these measures.

As verified in the article above, the law gives a great distinction to the principle of good faith, detaching it from the other principles and placing it alone in *the caput* of the article. Thus, it is understood that good faith is the basis of all other principles.

In turn, the law in question determines that entities that handle personal information must ensure the protection of data from unauthorized access, as well as accidental or unlawful situations of destruction, loss, alteration, communication or dissemination. It also ensures that companies need to adopt preventive measures in order to avoid damage to data subjects (DE OLIVEIRA, 2025).

DUTY OF INFORMATION SECURITY: PREVENTIVE MEASURES AND GOOD PRACTICES

With the growing volume of personal data collected and stored by companies and institutions, the duty to ensure the security of this information has become one of the most relevant aspects of corporate governance in the digital age.

The General Law for the Protection of Personal Data (LGPD), in its article 46, determines that processing agents must adopt technical and administrative measures capable of protecting personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination.

This duty is a legal and ethical obligation that aims to ensure the integrity, confidentiality and availability of personal information.

The concept of information security is directly related to the idea of protecting data from internal and external risks, preventing leaks and improper access. To this end, the LGPD requires companies to take a proactive stance, based on prevention, monitoring, and rapid response to incidents. This involves the implementation of information security policies, definition of roles and responsibilities, training of employees, and adoption of appropriate technologies for each type of data processing carried out (DE OLIVEIRA, 2025).

Among the recommended technical measures, data encryption, the use of firewalls, multi-factor authentication, access control, regular backups, and the constant updating of software and systems stand out. Administrative measures include the preparation of incident response plans, internal audits, risk assessment, mapping of data flows, and the appointment of a Data Protection Officer (DPO), as provided for in article 41 of the LGPD (DE SOUZA; ANDRÉ, 2025).

The principle of accountability and accountability, provided for in article 6, item X, of the LGPD, requires companies not only to implement good security practices, but also to

be able to prove that they have adopted these measures effectively. This implies keeping records of data processing, documenting the preventive actions adopted, and demonstrating compliance with the principles of the law (DE OLIVEIRA, 2025).

In this context, the concept of privacy by design gains relevance, according to which projects, products and services must be developed with data protection as a structuring element, from their initial phases (DE SOUZA; ANDRÉ, 2025).

Similarly, the principle of privacy by default requires that the privacy settings offered to the consumer automatically ensure the highest possible level of protection, without the need for user intervention (DE OLIVEIRA, 2025). Adopting good security practices not only mitigates legal and financial risks, but also strengthens the company's reputation and consumer trust. In a scenario where privacy is increasingly valued, organizations that demonstrate commitment to data protection gain a competitive advantage and avoid irreparable damage to their institutional image.

In addition, the National Data Protection Authority (ANPD), created by the LGPD, plays a fundamental role in guiding, inspecting, and applying administrative sanctions to companies that fail to comply with legal requirements. The sanctions provided for by the LGPD include warnings, blocking, and deletion of personal data, as well as fines that can reach up to 2% of the company's revenue, limited to BRL 50 million per infraction (DE OLIVEIRA, 2025).

It is important to note that, although the LGPD does not establish an exhaustive list of mandatory security measures, it imposes the duty to adapt to the best market practices, taking into account the nature of the data processed, the size of the company, and the risks involved. Thus, each organization is expected to assess its specific context and implement a proportionate, effective, and continuously improved protection system.

Finally, it is worth emphasizing that the duty of information security is not exclusive to large corporations or the technology sector. Every organization that processes personal data — from a small business to a hospital, school, or public office — is subject to the requirements of the LGPD and must act diligently. Negligence, improvisation, or the absence of internal policies are factors that contribute to the occurrence of incidents and, consequently, to the company's liability for the damages caused to data subjects.

In this way, the duty of information security transcends simple legal compliance: it represents a true commitment to the fundamental rights of individuals, to ethics in business relationships, and to the sustainability of economic activity itself in the digital age.

LEGAL CONSEQUENCES AND COMPENSATION FOR DAMAGES FOR DATA LEAKAGE

The occurrence of personal data leaks not only represents a violation of the privacy of individuals, but also generates serious legal consequences for the companies involved. Given the seriousness of these incidents, the Brazilian legal system, through the General Law for the Protection of Personal Data (LGPD) and other related legislation, provides for administrative, civil and, in certain cases, even criminal sanctions. The objective is to ensure the reparation of the damages suffered by data subjects and, at the same time, prevent new breaches by organizations (MOURA, 2025).

In the field of civil liability, the LGPD establishes, in its article 42, that the controller or data operator who, due to the processing activity, causes property, moral, individual or collective damage to others, is obliged to repair it. This liability can be excluded only if the agent demonstrates that it did not process data, that there was no violation of the legislation or that the damage was due exclusively to the fault of the holder or third parties. Thus, the rule follows a strict liability model, in line with what is already provided for in the Consumer Protection Code (CDC) on defects in the provision of services (DE OLIVEIRA, 2025).

Compensation resulting from data leakage may include both material damages, such as financial losses resulting from fraud, cloning, or misuse of personal information, and moral damages, associated with the violation of privacy, intimacy, and undue exposure of sensitive data. In several precedents, the Brazilian Judiciary has recognized the right to compensation for moral damages even in the absence of proof of direct economic loss, based on the presumption that the leak, by itself, already constitutes an injury to personality rights (MOURA, 2025).

In addition, the LGPD provides for administrative sanctions, applied by the National Data Protection Authority (ANPD), ranging from warnings and blocking of affected personal data to the imposition of fines that can reach up to 2% of the company's revenue, limited to BRL 50 million per infraction. The penalties seek not only to punish unlawful conduct, but also to encourage the adoption of preventive measures and good governance practices in data protection (CALAZA, 2024).

Another important aspect is the reputational impact for the company involved in data leakage incidents. In an increasingly competitive market that is sensitive to security and transparency issues, the loss of trust on the part of consumers can mean even greater losses than those resulting from any judicial indemnities. In many cases, the

damage to the institutional image leads to the loss of contracts, a reduction in market value, and difficulty in attracting new customers (DE OLIVEIRA, 2025).

In the judicial context, it is also possible for the Public Prosecutor's Office, the Public Defender's Office and consumer protection entities to file public civil actions, aiming at collective reparation for damages caused to multiple data subjects. Collective protection is highlighted in cases where leaks affect large databases, as has already occurred in widely publicized episodes, involving banking institutions, telephone operators, e-commerce companies, and public agencies (MOURA, 2025).

In addition, depending on the severity of the case and the nature of the information exposed, repercussions may arise in the criminal sphere, especially if crimes such as invasion of a computer device (article 154-A of the Penal Code), misuse of confidential information, embezzlement, and other digital frauds are configured. Even if the company has not acted with intent, its omission or negligence in the duty to protect data can aggravate its legal situation (CALAZA, 2024).

National jurisprudence has moved towards consolidating criteria for the reparation of damages, taking into account factors such as: the volume of data leaked, the sensitive nature of the information, the company's conduct after the incident (such as transparency and communication with the holders), and the existence or not of adequate security measures. In many cases, the compensation is set taking into account the pedagogical nature of the sanction and the economic size of the offending agent (DE OLIVEIRA, 2025).

Thus, the legal consequences of data leakage are not limited to mere financial compensation to the injured holders. They reflect a broader process of maturation of legal relationships in the digital age, in which respect for privacy, information, and security comes to occupy a central place in business practices (DE OLIVEIRA, 2025).

Compliance with the LGPD and the adoption of a culture of data protection are, therefore, not only legal requirements, but also strategic ones, which directly impact the sustainability and legitimacy of organizations in society.

CONCLUSION

The growing digitalization of social and commercial relations imposes on companies a new paradigm of responsibility and transparency regarding the processing of personal data. The entry into force of the General Law for the Protection of Personal Data (LGPD) represented an essential regulatory milestone in the protection of individuals'

privacy, providing legal certainty to both data subjects and the organizations involved in its collection, storage, and processing.

In this context, it is evident that the inappropriate processing of personal data, especially when it results in leaks, imposes a series of legal, administrative, and reputational consequences on companies.

The present work demonstrated that the civil liability of companies, especially in consumer relations, is mostly objective, as established by the Consumer Protection Code and reinforced by the LGPD.

This means that, in the face of a data leak incident, the demonstration of fault is not required for the injured consumer to be compensated. Proof of the damage and the link with the failure to provide the service is enough for the duty to repair to arise.

In addition, the duty of information security is an essential obligation of companies, which must implement technical and administrative measures capable of mitigating risks, preventing unauthorized access, and responding efficiently to security incidents. Failure to comply with these requirements may result not only in civil damages, but also in administrative sanctions applied by the National Data Protection Authority (ANPD), as provided for in current legislation.

Therefore, it is concluded that the civil liability of companies in the processing of personal data requires not only regulatory compliance, but also an ethical commitment to the privacy and fundamental rights of citizens. The adoption of privacy governance policies, investments in information security, and the culture of data protection should not be seen as obstacles or burdens, but rather as strategic differentials in an increasingly competitive market that is attentive to the protection of consumer rights. The implementation of the LGPD thus represents an important step towards building a safer, more transparent, and more reliable digital environment for all involved.

REFERENCES

1. ARABI, Abhner Youssif Mota. Law and technology: an increasingly necessary relationship. **JOTA Info.** 3 Jan. 2017. Accessed on: 18 Apr. 2024.

2. BIONI, Bruno R. From 2012 to 2018: the Brazilian discussion on a general data protection law. **JOTA Info.** 2 Jul. 2018. Accessed on: 18 Apr. 2024.

3. BLUM, Rita Peixoto Ferreira. **The right to privacy and the protection of consumer data.** São Paulo: Almedina, 2018. *Electronic book.* Accessed on: 18 Apr. 2024.

4. BRAZIL. Law No. 8,078, of September 11, 1990. **Consumer Protection Code**. Provides for consumer protection and provides for other provisions. Federal Official Gazette: section 1, Brasília, DF, 12 Sept. 1990. Accessed 01 mar. 2025.

5. BRAZIL. [Constitution (1988)]. **Federal Constitution.** Brasília, DF: Senado Federal, 1988. Available at: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed on: 05 June 2024.

6. BRAZIL. **Law No. 13,709, of August 14, 2018**. General Law for the Protection of Personal Data (LGPD). Brasília, DF: Presidency of the Republic, [2018]. Accessed on: 20 Apr. 2024.

7. CALAZA, Tales. EVOLUTION AND REGULATION OF PRIVACY AND DATA PROTECTION IN THE CONTEXT OF THE INTERNET OF THINGS IN THE BRAZILIAN SCENARIO.
8. **CAAP Journal**. Ed.2024. PDF. Accessed 01 mar. 2025.

9. CAPANEMA, Walter Aranha. Civil liability in the General Data Protection Law. **Cadernos Jurídicos, São Paulo, year**, v. 21, p. 163-170, 2020. PDF DE OLIVEIRA, Jéssica Batista et al. The protection of personal data and the application of the LGPD in Brazil. **NATIVA-Journal of Sciences, Technology and Innovation**, v. 7, n. 1, p. 166-178, 2025. Accessed 01 mar. 2025.

10. DE SOUZA, VITÓRIA LIMA; ANDRÉ, VICTOR CONTE. GENERAL DATA PROTECTION LAW: COLLECTION OF SENSITIVE CONSUMER DATA AND CIVIL LIABILITY. **Revista Multidisciplinar do Nordeste Mineiro**, v. 6, n. 1,
11. p. 1-21, 2025. Accessed 01 mar. 2025.

12. MOURA, Luana Clara Fernandes de. **The responsibility of internet application providers on the right to deindexation and the right to be forgotten: a legal analysis based on the Civil Rights Framework for the Internet. 2025. Accessed 01 mar. 2025.**

13. SOUZA, Marcela Cristina de. **CIVIL LIABILITY IN DATA PROCESSING: Impacts of Artificial Intelligence on the Protection of Personal Information**. 2025. Accessed 01 mar. 2025.