ISSN: 2755-0133

Journal of Medical & Clinical Nursing

SCIENTIFIC Research and Community

Review Article

Open Access

Legislative Advances in the General Data Protection Law

Tricia Bogossian

Specialist, Santa Úrsula University in Rio de Janeiro-RJ, Brazil

ABSTRACT

This study aims to verify whether the protection provided by the General Data Protection Law (LGPD) has been shown to be sufficient to safeguard the fundamental right to privacy in times when technological evolution is progressing and how compliance regulations can help in this context. Therefore, it addresses the right to privacy in the information society; explains the relationship between technological evolution and information security; and exposes general aspects of the LGPD. As a methodology, the theoretical-dogmatic research was used, considering that a literature review on doctrines and legislation was carried out in order to answer the research problem.

***Corresponding author**

Tricia Bogossian, Specialist, Santa Úrsula University in Rio de Janeiro-RJ, Brazil. E-mail: tricia.bogossian@hotmail.com

Received: August 18, 2021; **Accepted:** August 23, 2021; **Published:** August 28, 2021

Keywords: Protection, Data, Legislative Advance

Introduction

Today we live in a time of great "media exposure". People are no longer able to live disconnected and daily a large volume of information and personal data is dumped on the internet, giving rise to a series of violations of fundamental rights. These violations, in turn, have led to efforts to contain them, such as the General Data Protection Law (LGPD), leading to thinking about the extent to which it would be reasonable to restrict the disclosure of this information on the Web in view of the risk of generating a collapse in technological advance. Given the reality exposed, the question that guided this research was: has the protection brought by the LGPD been sufficient to safeguard the fundamental right to privacy in times of Big Data and technological evolution?

In this path, the general objective of this study was to verify, based on doctrine, legislation and jurisprudence, whether the protection brought by the LGPD has been sufficient to safeguard the fundamental right to privacy in times of mass data and technological evolution. To achieve it, the following specific objectives were outlined: to understand the legal treatment given to the personal data of citizens in Brazil in times of mass data; and understand the current paradigms that give new meaning to privacy and protection of personal data in times of technological evolution.

Interest in the topic arose, therefore, it cannot be denied that the Internet has provided a virtual approach to individuals, substantially changing the way in which people (natural and legal) relate to each other. However, from the legal perspective, it is clear that this technological evolution has not been accompanied by the respective legal evolution that makes it possible to identify and adequately punish those who violate the honor, privacy and dignity of others.

The set of fundamental rights at any given time came into conflict. With the right to privacy and information it will be no different; they too came into conflict. However, there is a whole dogmatic of interpretation and consideration of this conflict. Thus, it is important to know what the LGPD has failed to bring to rationalize this problem, because, even though the law has not regulated something in specific, there is a constitutional, civil and penal dogmatic that can be used, in addition.

It is understood that new technologies have transformed social relations and, as is already the case in other areas of science, the Law needs to examine them in order to ensure their development without violating the individual and collective guarantees of citizens.

Thus, the aim is to demonstrate that any economic evolution is only justified if it is in tune with the most expressive axioms of the current legal sentiment and the promotion and protection of the person, their essential values and rights, which includes, inextricably, the protection of personal data.

The study proves to be relevant, because, whatever the way found to achieve satisfactory regulation on the impacts that the information society provides within the relationships that involve individuals, it is clear that this is a task that still requires ample contribution. of doctrine, in addition to dialogue between the systems of the most diverse countries, so that it is possible to reach a harmonic normative environment capable of acting in a joint and effective way.

In order to achieve the objectives proposed in this monograph, theoretical-dogmatic research was used, considering that a literature review was carried out on doctrines, legislation and jurisprudence in order to respond to the problem presented in order to find a solution to mitigate the conflict that formed around the right to privacy and the right to information.

As an intelligent and effective data analysis method, companies have been using Big Data to obtain valid information that will be beneficial to them in some way. In this way, companies use the results obtained to better understand the market, launch new products and services, and respond to constant changes in standards almost instantly [1]. In addition to companies, governments have also benefited from the possibilities of Big Data, making it possible for them to learn about the perceptions and behavior of certain communities through the analysis of digital data. This can be of great importance in city administration, healthcare, public safety and in several other sectors that interest citizens and politicians, such as the use of Big Data in electoral campaigns [2].

The term "big data" started appearing in dictionaries over the last decade, but the concept itself has been around since World War II. More recently, wireless connectivity, Internet 2.0 and other technologies have made managing and analyzing large data sets a reality [2].

Currently, with the evolution of the Internet, a variety of information is made available, as people want to interact with people they know, in addition to wanting to meet other people. Also, they got used to sharing on their social networks, photographs and, often, details of their routine. Often, the information shared is publicly accessible. It is possible to prevent the access of strangers to posted content, but often users do not even know how to handle such resources or just do not care to deprive them, thus allowing anyone to access all the content they post.

That said, before explaining how the protection of personal data has been done in Brazil over time, it is important to differentiate between sensitive and non-sensitive personal data.

The Protection of Personal Data in Brazil

The concern with the right to privacy, according to Silva started in the USA, in 1890, when at Harvard University, people started talking about the right to be alone and the right to be forgotten (right to be let alone) [2]. There is no doubt that the Internet has brought and benefits everyone, as the vast majority of tasks performed, whether at work or at home, demand the use of technologies to speed up processes that were previously done manually. In light of the facilities, new illegal practices arise, whose main instrument is the computer associated with the Internet, which means that existing crimes are being improved, as will be seen below.

Faced with this new reality that has come to be called globalization, communities around the world started to act in cyberspace, also called cyberspace, and, inevitably, individuals of different natures, including criminals, changed to this environment. Regarding cyber crimes, the most important legislation is the Marco Civil da Internet – MCI, which provides principles and provides guarantees, rights and duties for internet users in Brazil, originated in PLC n. 2,126/2011, on 10.26.2011.

The initial project of the MCI sought to present clear norms about the rights, duties, guarantees and principles to regulate the use of the Internet in Brazil. It was necessary to defend some fundamentals so that the Internet in Brazil was preserved as a space for collaboration. Thus, as Malaquias reminds us, any subsequent regulatory initiative must observe the guidelines and principles chosen as fundamental, such as privacy [4].

Judicial interpretations at the time neglected the fundamental principles and architecture of the Internet, leading the Brazilian Internet Steering Committee (CGI.br) to edit, in 2009, the "Guidelines for the Use and Governance of the Internet in Brazil", in which the ten fundamental principles to regulate the Internet were outlined, taking into account the harmony of the constitutional precepts to ensure the adequate technological functioning in the same rhythm required by the homeland cybernetic society, extensively analyzed previously by this research.

Another important project voted and approved was PLC 89/03 (PL 84/99), presented on 11.13.2003 (Dep. Luiz Piauhylino), which became Law 12.737, dated 11.30.2012, typifying computer crimes and modifying the Code Criminal. These provisions were included in Chapter VI, which regulates crimes against individual freedom and, in turn, are included in Section IV, where crimes against the inviolability of secrets are typified.

In this project, the invasion of systems in order to obtain commercial and industrial secrets or private content, using unauthorized remote techniques and violating security mechanisms, has a penalty of imprisonment from 6 months to 2 years and a fine. It brings as an aggravating factor the possibility that the criminal discloses, commercializes or transmits the data obtained illegally to third parties.

The invasion of a device or local network with the objective of destroying or altering data or information, in addition to installing malware to obtain illicit advantages or just for vandalism, was penalized with 3 months to 1 year of detention and a fine. An individual who produces, offers, distributes, sells or discloses a computer program with the purpose of carrying out cyber crimes on computers, smartphones, tablets or other informational devices and on local networks was included in the same crime.

According to the author of that bill, this structuring of types fills the current omission in criminal law. However, its most fervent opponent, Federal Deputy Eduardo Azeredo (PSDB-MG), rapporteur of another project (PLC n.84/1999) with very different characteristics, denounces the governmental casuistry, claiming that the government, for a long time, was silent and that, due to the leak of photographs of actress Carolina Dieckmann, a project was quickly voted on that was not even discussed in any committee. These statements are quite significant to demonstrate and illustrate the importance that parliamentarians have attributed to the topic of cybercrime.

Until 2012, when it was possible to reach the cybercriminal, the laws that already existed were used to punish the crimes committed. There were still no specific legal mechanisms to punish the perpetrators of crimes committed over the Internet. As an example, a criminal who might steal information from a certain internet user using cunning or benefiting from the good faith of the victim, could be framed, for example, in the crime of embezzlement (art. 171 of the CP).

With the leaking of sexy photos of actress Carolina Dieckman in October 2012 on the Web, former president Dilma Rousseff sanctioned two laws that changed the Brazilian Penal Code to establish virtual crimes and their respective sanctions. The Carolina Dieckman Law (12,737/2012) and the Azeredo Law (12,735/2012) entered into force on April 2, 2013 in the Brazilian Penal Code with the aim of typifying various conducts in the virtual environment (MALAQUIAS, 2015).

In Brazil, as a result of the growing number of Internet users, its regulation was urgently made and, in such a reality, the MCI originated, with Law No. 12.965/2014, which established principles, guarantees, rights and duties that should considered in the use of the Internet in Brazil. This legislation seeks, in addition to guaranteeing users' principles, such as their privacy, respect for human rights and the exercise of citizenship in digital media, to establish guidelines related to the commercial and governmental exploitation of this digital space.

Initiated by Bill 2,126/2011, by the Executive Branch, Law 12,965/14, before its sanction, was the subject of numerous controversies. Taking care of issues such as net neutrality, storage of connection records, keeping of Internet application records, privacy, social function of the network, responsibility for infringing material, data storage in the country and compliance with national legislation, among other points, emerged too many debates, in which users, connection providers and national and international content, copyright holders and the government participated [5].

Regarding the guarantee of privacy of Internet users, the new law brought certain certainties that until then gave rise to doubts, both for those who considered themselves affected in their dignity in the virtual world, as well as for the operators of the Law. Thus, with Law 12.965/14, the idea that constitutional rights also apply to the virtual world was consolidated [5].

Indeed, it is clear that greater attention to the rights concerning the user's private life was positive in the Brazilian legal system. However, there are still several questions regarding the limits of invasion of the privacy, especially when discussing labor relations, even because the legislator cannot predict all the new situations faced by employers and employees every day. Furthermore, the legislator sought to protect the privacy of Internet users in other points as well. An example is in the caput of art. 10, of Law 12.965/14, which aims to protect privacy with regard to the custody and availability of connection, access and personal data records, thus expressing:

The custody and availability of records of connection and access to Internet applications referred to in this law, as well as personal data and the content of private communications, must comply with the preservation of intimacy, privacy, honor and image of the parties directly or indirectly involved [5].

In such a circumstance, the citizen would be able to limit the information he allows to be made public, even if to the detriment of his privacy. "This is informational self-determination based on the perspective that the user must have control over their personal information, self-determining them" [6].

As can be seen, even in the midst of clashes for the approval of the new law, it covered several contents, changing norms, as well as the relations between users and companies in the area. Until the approval of the MCI, the multiple legal uncertainties regarding the matter barred constitutional rights and guarantees, when linked to the virtual world. It was, therefore, necessary to have a regulation for the Internet that would limit not only the powers of companies, but also of governments over users, giving the opportunity to implement a different management model for the large network.

The Right to Informative Self-Determination

According to Ruaro, informative self-determination is the possibility of an individual, holder of a given data, to demand that their data not be processed [7]. In other words, it is the capacity, possibility and freedom that people have to decide on the treatment of their data, and if they wish, to interrupt this treatment. As emphasized by Rodotà, this right considers any collection of personal information that is carried out without prior knowledge and explicit consent from the interested party to be illegitimate [6]. This right is that certain information collected about a particular person must not circulate outside the public or private institution that originally collected this information for a certain purpose.

According to the provisions of Law 12,965/2014, this right is reflected in the provisions that: 1) prohibit the provision to third parties of connection records and access to Internet applications, except by means of free, express and informed consent; 2) requires clarity and completeness of information about the collection, use, processing and protection of your personal data; and 3) that they can only be used for the purposes on which their collection was based. The LGPD expressly provides that informational self-determination is one of the foundations of the discipline of personal data protection. The legal objective is to give the person the right to know what is done with personal information and decide whether or not to authorize its use for a purpose other than that obtained.

However, an essential question arises: How can this control be exercised by the person to secure this right? The most important answer is that the issue is no longer legal. It is a matter of public policy management which the law has already regulated. Thus, in the same sense that computer engineering is able to create artificial intelligences to process information, through the most diverse methods of analysis, the creation of tools so that the individual can have this knowledge and express their consent is something very simple to do. be developed and made available to the person who is the target of this situation. This is one more challenge that must be transposed in order for this right to be effective.

Nether explains that historically, just as absolutist regimes gave way to democratic regimes in several countries around the world, this right to informative self-determination is gradually being recognized by legal systems, and consolidating as a result of the constant affirmation of the need for democratic regimes [8]. As can be seen, in Brazil it is in an initial or embryonic phase, considering the phase that the Law has recently been in force. This right, as a result of the fundamental right to the protection of personal data, is being essential nowadays.

That said, it can be seen that personal data need to have a different meaning and value, as well as a broader one than when it was included in the list of fundamental rights in the 1980s, when the CRFB/1988 was enacted.

The General Data Protection Law

The LGPD enters the national system late, because only more than fifteen years after the creation of the RIPD, perhaps because Brazil integrates only as an observer country. However, the LGPD had its processing relatively quickly in the national Legislative Power, entering at the end of May 2018 and being sanctioned in August of the same year. The speed of this process was due to cyber attacks that occurred recently in several private and public networks, especially in previous years.

The purpose of the LGPD is the protection of privacy, as in this context, dominated by information technologies, the risks of invasion of the individual's private sphere are accentuated, making the sphere of privacy more vulnerable to undue and unjustified invasions [9].

An important issue is the delimitation of ownership of the right to the protection of personal data. There seems to be no doubt about the natural person's condition as the immediate recipient of this modality of guardianship. However, these are not the only ones deserving of protection in relation to their data, because, as explained by Sarlet, Marinoni and Mitidiero, natural persons (and even depersonalized entities) are also deserving of acting as recipients of the rules on proper data management [10].

Regarding the application of this Law, it is provided that it is applicable in any operation in which personal data are processed by a natural or legal person governed by public or private law, regardless of the environment, country of its headquarters, or country in which the data is located . However, such application observes the territoriality aspect when it only covers: 1) operations carried out in the national territory (objective criterion); 2) when the operation to be treated is carried out outside the national territory, but the data are from people who are in the national territory (subjective criterion); or 3) regardless of the place where these data will be processed, their collection must have taken place in the national territory (objective criterion) [11].

It should be noted that when the Law establishes that "personal data whose owner is found therein at the time of collection is considered to be collected in the national territory", the aspect of the individual's location, through Internet protocols , known as the acronym IP , is a necessary reference to assess whether or not there was this violation of the rights protected by the LGPD [12]. In a society in which information is the true wealth, the protection of privacy based on personal data that travels on the Internet contributes decisively for the powers to achieve balance. Power that migrated from the sovereign's hand and was constitutionally attributed to the people. Therefore, the end of privacy would not only represent a risk to individual freedoms, it would effectively lead to the end of democracy [6].

The LGPD sought to establish a protection system made up of representatives of the State and civil society. However, the effectiveness of this protection will depend on how much the individual is informed of what instruments they have so that their privacy is not violated without their knowledge, through the various technological interfaces that the current computerized world offers for consumption in general and convenience.

Thus, this protection provided for in the Law aims to protect the privacy that is a personality right. In this scope of protection, the dignity of the person is the principle of absolute value, as argued by Alexy when elaborating the equations to solve the collision of principles [13]. It is even stated by Rodotà that data protection is not only a fundamental right among others: it is the most expressive of the contemporary human condition, and that this protection can be understood as the combination of rights that underlie the citizenship of the new millennium [6].

With regard to territorial effectiveness, as explained by Mèlo, the law applies to treatment operations that take place in the Brazilian territory, extending to treatment operations that: take place outside the country, but the data were collected in Brazil; if the data relate to people located in the Brazilian territory; and if the personal data processed have been collected in Brazil [11]. In Europe, the current standard, which entered into force on 25.05.2018, is the Regulation (EU) 2016/679 – known as GDPR (General Data Protection Regulation). The LGPD was built on the GDPR foundation. It also has global jurisdiction, as any website, headquartered in any nation that processes personal data of Brazilian citizens, must comply with it.

As for the legal grounds for data processing, Castro demonstrates that the LGPD differs only superficially from the GDPR when it comes to its legal basis for data processing [14]. Thus, the LGPD and GDPR are aligned, with small variations. At the point where the GDPR has 6 legal bases for processing, 10 is identified in the LGPD. The latter divides the more general wording of the GDPR into more specific provisions.

By way of illustration, the legal foundation of the GDPR, whose precept is "to save someone's life", in the LGPD presents the following division: "a) protect life or physical safety; and, b) protect health, in a procedure performed by health professionals or health entities" [12]

Furthermore, the LGPD presents, as a plus, a legal basis regarding the credit protection that the GDPR has not adopted in its entirety. Also, personal data has a more extensive definition in the LGPD than in the GDPR. According to the LGPD, anything that relates to an identifiable natural person can be considered as "personal data". In GDPR, the specification comes from examples like names, gender and addresses. Castro points out that in the LGPD, sensitive data is, as in the GDPR, a distinct category from personal data, including information on race, ethnicity, religious beliefs, political ideas, health, biometrics, sexuality, among others [14]. Limitations on confidential data to be processed in the LGPD are more severe than in the GDPR.

Another point observed by Lemoalle and Carboni is that the LGPD does not provide definitions about pseudonymized data, as well as the GDPR [15]. The exception is research carried out by organizations that work in public health. In turn, the GDPR is quite specific with regard to its requirements related to the processing of personal data for advertising/marketing purposes, while the LGPD has nothing on the subject. It should also be noted that at GDPR, the Data Protection Impact Assessment (AIPD) was instituted, whose objective is to measure the risks related to data processing. The AIPD requires processors to notify data protection authorities if high risks related to data processing are identified.

Also, according to Mèlo the LGPD institutes the AIPD, but it does not make it clear how this assessment should be used, nor does it provide requirements for any supervisory authorities to be notified. However, in the LGPD it is mandatory for companies to have a data protection officer (OPD), whereas this professional is only needed in a few circumstances in the GDPR [11]. Time restrictions for data breaches to be notified are explicitly specified in the GDPR (72 h), while the LGPD freely mandates that breaches be notified to the authorities in "a reasonable time"[11].

Regarding fines, Lemoalle and Carboni emphasize that, compared to the GDPR, in the LGPD, if violations occur for non-compliance, the penalties are less severe [15]. The maximum amounts of fines for non-compliance in the GDPR are set at 20 million euros, which corresponds to 4% of an organization's annual global revenue. LGPD limits its fines to a maximum of 50 million reais (around 11 million euros) or 2% of what a company invoices annually in Brazil.

As for territorial applications, the LGPD treats the transfer of personal data internationally in the same way as the GDPR, assessing whether the other country has adequate data protection laws. However, the LGPD (unlike the GDPR) does not mandate that data be transmitted across Brazil without any further

processing. The LGPD was approved with a text that focused on the protection of personal data, that is, it does not directly protect data that are not held by individuals. In other words: the law was born to protect individuals and their privacy. Business secrets, purely financial items, strategic plans, algorithms, software and any other documents or information that do not concern an individual are not protected by law3 [11].

Furthermore, it is worth mentioning that, although we live in a world where everything has been born in digital environments, it is not ignored that there are still records in various other types of repositories, many on paper. The LGPD does not make any distinction about the repository where the personal data are located, being fully applicable to everything that is registered on paper [16].

Conclusion

We currently live in a network society. As the internet has no borders, in digital relationships, the limit of individual and business freedom is ethics. Everyone on the network has the same power to act both protectively and destructively, and therefore the duty to practice information security. Hence, the importance of fostering a cybersecurity culture.

It is, in principle, a cultural change, which must be carried out through investments in training and technical improvement with a view to identifying and pointing out the socioeconomic impacts and the methods for the change to comply with the rules. This cultural change consists of an educational work so that everyone is aware of the way it works: risks, rights, limits and responsibilities. Along with technological solutions and contract reviews, the training of teams is among the pillars that should guide the institutions' planning.

For legislation to really be more effective, it is necessary for the user to be made aware, especially regarding their role in implementing the best practices in digital security. For this reason, the laws themselves are bringing with them the duty to carry out awareness campaigns.

The recent pandemic was a significant factor of changes, many even related to the processing of personal data due to the need to work in a home office. But adaptability depends on other factors, such as regulatory challenges (with more standards regulating data protection in the country and around the world), as well as the challenges posed by technological development.

References

1. FREITAS JR, José Carlos da Silva, MAÇADA, Antônio Carlos Gastaud, OLIVEIRA Mirian (2016)Big Data and knowledge management: definitions and research directions. Revista Alcance 23: 529-546.
2. SCHMIDT Eric, COHEN Jared (2013) The new digital age: what the future of people, nations and business will be like. Translated by Ana Beatriz Rodrigues and Rogério Durst. Rio de Janeiro: Intrinsic https://www.amazon.in/New-Digital-Age-Reshaping-Business/dp/0307957136.
3. SILVA, Alexandre Assunção (2017) Confidentiality of Communications on the Internet. Curitiba: Juruá Editora.
4. MALAQUIAS, Roberto Antônio Darós (2015) Cyber Crime and Evidence: The Criminal Investigation in Search of the Truth. 2. ed. Curitiba: Juruá Editora https://www.sciencedirect.com/topics/computer-science/cybercrime-investigator.
5. BRAZIL Law No. 12.965, of April 23, 2014. Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
6. RODOTÀ, Stefano (2008) Life in the surveillance society: privacy today. Organization, selection and presentation by Maria Celina Bodin de Moraes. Translated by Danilo Doneda and Luciana Cabral Doneda. Rio de Janeiro: Renew https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2008;000834435.
7. RUARO (2018) Regina Linden. Privacy and informational self-determination: obstacles to the surveillance state? Legal Archive, Teresina 2: 41-60.
8. NETHER, Nicholas Augustus de Barcellos (2018) Protection of Application Users' Data. Curitiba: Juruá Editora https://www.jurua.com.br/.
9. BIONI, Bruno Ricardo. Protection of personal data. Rio de Janeiro: Forensics, Publisher, 2019.
10. SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Constitutional Law Course. São Paulo: Revista dos Tribunais, 2014.
11. MÈLO, August (2019) Protection of Personal Data in the Information Age. Curitiba: Juruá Editora.
12. BRAZIL. Law no. 13.709, of August 14, 2018. General Data Protection Law (LGPD). Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
13. ALEXY, Robert (2008) Fundamental rights theory. Translated by Virgílio Afonso da Silva. São Paulo: Malheiros, (Theory & Public Law Collection).
14. CASTRO, Nuno Teixeira (2016) A new European legal framework for data protection envisioning the Digital Single Market for Europe. Daily Insomnia. [S.l.], Available at: http://www.insonias.pt/um-novo-quadro-legal-europeu-materia-proteccao-dados-vislumbrando-mercado-unico-digital-europa/amp/.
15. LEMOALLE Edouard, CARBONI William (2018) European Personal Data Protection Law (GDPR) and its effects in Brazil. JOT. [S.l.], Available at: https://www.jota.info/opiniao-e-analise/artigos/lei-europeia-de-protecao-de-datos-pessoais-gdpr-e-seus-efeitos-no-brasil-12022018.
16. CRESPO, Marcelo Xavier de Freitas (2019) Digital Compliance. In: CRESPO, Marcelo Xavier de Freitas. Governance, Compliance and Citizenship. 2. ed. São Paulo: Revista dos Tribunais.

Copyright: ©2021 Tricia Bogossian. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.