GENERAL CONSIDERATIONS ABOUT THE GENERAL DATA PROTECTION LAW AND ITS MAIN CHALLENGES IN BRAZIL

ORIGINAL ARTICLE

TORREÃO, André D Albuquerque[1], DENDASCK, Carla Viana[2]

ABSTRACT

If, on the one hand, the concern with data protection represents an advance in Brazil, on the other hand, it is considered that the ignorance of technology, as well as, the infrastructure resources still limited in Brazil are presented as a major obstacle in this relationship, and tends to create a line of judicialization that can and should be discussed. Thus, this study has as a guide question: What are the main challenges in Brazil in the implementation of a Data Protection Law? Its main objective was to bring subsidies for reflection in order to serve as a basis for deeper and more interdisciplinary discussions on the subject. Seeking then, to bring a brief overview of the obstacles that are still being little discussed.

Keywords: LGPD, General Data Protection Act, Knowledge in technology.

INTRODUCTION

The LGPD is a general law aimed at establishing guiding principles and concepts with regard to the safe use of data (BIONI; DAYS, 2020). It seeks to preserve the balance between the need to effectively protect the rights of the holders of such data, and at the same time allows the processing of personal and sensitive data for specific purposes, including scientific research (DIVINO; LIMA, 2020). The General Data Protection Law, Law No. 13,709/2018, established, for the first time in the Brazilian legal system, a set of rules composed of rules and principles related to the regulation

of the processing of personal data in all daily activities of the citizen, including the most diverse sectors (MIRAGEM, 2019). The impact of this reconfiguration on the legal system is equivalent to that of the social contract itself, because people are currently judged and evaluated based on what their personal data reveals.

Several situations of human life are filtered by the processing of their data, especially in the contemporary context where virtually all human relations are being carried out over the Internet, whether in the process of acquiring products, or in the professional practice, or in the process of education, search for knowledge, or, to meet legal obligations, such as income tax returns, Transit service etc. Life is constantly passing, happening at a speed never before seen, taking and bringing countless data by billiards of digital tools. Thus, the central question of this study was the search to understand: What are the main challenges in Brazil in the implementation of a Data Protection Law? For this, a brief explanation was made on this theme, seeking to make reflective surveys that allow the real effectiveness of this law.

REFLECTIONS ON LGPD AND LIMITING FACTORS OF BRAZIL

The General Law for the Protection of Personal Data provides for the strategies necessary for the protection of such data. Amended Law No. 12,965 of April 23, 2014, entitled "*Marco Civil da Internet*" (MENDES; DONEDA, 2018). It fills the gap left by the legislator in relation to the content of Art. 3rd, III, of this diploma. Therefore, the LGPD has undergone several vetoes and some modifications by the Presidency. The first article deals with the scope of the LGPD: how it will deal with personal data, including in the digital field (digital media), whether these acts are committed by a legal entity under public or private law or by a natural person (LAW, 2020). The objective is the protection of the fundamental rights of freedom, privacy and the free development of the personality of the natural person. Thus, the device discusses, throughout its articles, about what configures the domain of privacy and how personal data should be protected, especially in the digital space (CARVALHO, 2018).

The fundamental right to freedom shares a leading role in the right to privacy. The legislator, without fear of sounding redundant, leaves expressed, as well as protected,

the freedom to develop the personality of the natural person, and thus builds a diploma capable of covering the different aspects of privacy and the values related to it, taking into account the complexity of the situation in which personal data are inserted (CARVALHO, 2018).

O Art. 2nd lists the fundamentals about the discipline of the protection of personal data, being: I) respect for privacy; II) informative self-determination; III) freedom of expression, information, communication and opinion; IV) inviolability of intimacy, honor and image; V) economic, technological and innovation development; VI) free initiative, competition and consumer protection; and VII) human rights and development of personality, dignity and exercise of citizenship (CARVALHO, 2018).

These foundations are in accordance with the ideas presented and defended by the scholars of the theme in the country, and thus, general delineations, beacons and limits for this exercise are established (RONCOLATO, 2018). We must bear in the right care of the complexity of contextualising privacy in the context of the protection of personal data. At the same time, respect for privacy, human rights, freedom and values related to the dignity of the human person with regard to the dignity of the human person in the process of regulating the processing of personal data is sought, and also aims at economic, technological development, innovation, free initiative and free competition (SILVA, 2017). The protection of personal data tries, at the same time, to protect the privacy of the subjects of law and seeks to achieve the construction of a scenario that does not cast, gag or interrupt the economic, technological and interests of those involved (CARVALHO, 2018).

Therefore, in this area, the various situations, paradigms and processes experienced in network society are encompassed. Some of these possibilities can be listd, such as the voluntary overexposure of certain subjects on virtual social networks; the opening of a significant portion of privacy and freedom of expression (which puts these subjects in an exposure situation); among other processes. It is also noteworthy that some people make the exhibition on social networks such as Facebook, Instagram and YouTube, a way of life, and thus, voluntarily, the content of their shadow protected by privacy is mitigated (CARVALHO, 2018). O Art. 3rd, in turn, refers to what was once

foreseen by Art. 11 of the *Marco Civil da Internet*, and thus it is established that the approved law will be applied to any treatment operation carried out by the natural person or by the legal entity of public or private law (MENDES; DONEDA, 2018).

This application is independent of the environment, the country of its head or the country where the data are located, that is, the conditions that led to this situation are observed. O Art. 4º, therefore, deals with situations of exception to the application of the possible General Law on the Protection of Personal Data, as is the case of the hypotheses of processing by natural person for exclusively private and non-economic purposes, those for journalistic, artistic or academic purposes, processing of data for exclusive purposes of public security, national defense, state security or investigative and prosecution activities for criminal offences, among other similar situations (LAW, 2020). The second paragraph of the provision deserves special attention because, expressly, it prohibits the processing of data by a person under private law, for the purposes of public security, national defense, state security or investigation and prosecution activities of criminal offenses (CARVALHO, 2018).

There is once again a certain caution on the part of the legislator with regard to the protection of the privacy, freedom and dignity of the subjects of law. O Art. 5, in turn, it deals with the names used by the LGPD: it defines what would be a personal data, which is identified as information related to the natural or identifiable person, as well as establishing what would be the "sensitive data" and the "anonymized data" (SILVA, 2017). The specification of sensitive data is of paramount importance to understanding privacy protection. This data is related to the issues that predict that, in a possible violation of privacy, harmful consequences may occur (CARVALHO, 2018). Greater protection is given to these data intrinsically related to freedom, dignity and the free development of personality, and thus greater strength is given to the protection of privacy and values linked to it (MENDES; DONEDA, 2018).

Personal data characterized as sensitive as a kind of personal gender are conceived, and thus scholars draw attention to the need for greater care with the protection of these data (FRAZÃO; OLIVE; ABILIO, 2019). Anonymization, despite its criticism, is a necessary tool in some situations, because, if not prevent, it can at least curb and

hinder any violations of privacy. Therefore, it is necessary to de-identify the data, assigning codenames, codes or other distinctive elements related to data subjects, and also, it is necessary to process as a protective layer, a stage of difficulty imposed on eventual and potential violations, thus creating a kind of "lock at the gate". In this process, resorting to the use of encryption and other technologies capable of promoting and ensuring privacy is of paramount importance (SILVA, 2017).

However, here, there is a duality in the very concept of privacy, since in order to have such a right towards technological privacy servers, websites and other systems must be able to support such privacy, either in the sense of infrastructure and in the maintenance of digital data security. O Art. 6º provides guidelines for the processing of personal data, and thus stipulates the principles to be observed in this activity. Among them, we highlight the principle of good faith and the principles of purpose (carrying out the treatment for specific legitimate purposes, explicit and informed to the holder, without the possibility of further treatment in a manner incompatible with these purposes), adequacy (compatibility of the treatment with the purposes informed to the holder, according to the context of the treatment), the need (limitation of the treatment to the minimum necessary for the accomplishment of its purposes, covering the relevant, proportionate and non-excessive data in relation to the purposes of data processing) and free access (this is about the guarantee to holders of the facilitated and free consultation on the length of processing, as well as focusing on the completeness of their personal data) (CARVALHO, 2018).

Other principles are also at stake: data quality (it is guaranteed, to the holders, accuracy, clarity, relevance and updating of the data, according to the need and for the fulfillment of the purpose of its processing); transparency (information is provided in a clear, precise and easily accessible way with regard to the performance of the treatment and its treatment agents, in view of trade and industrial secrets); (technical and administrative measures are taken to protect personal data for unauthorized access and accidental or unlawful situations related to destruction, loss, alteration, communication or dissemination); prevention (measures are taken to prevent the occurrence of harm due to the processing of personal data); non-discrimination

(impossibility of processing for discriminatory and unlawful purposes); accountability and accountability (CARVALHO, 2018).

In the latter axis, the agent is expected to comply with measures that are effective and capable of proving compliance with and compliance with the rules of protection of personal data, including ensuring the effectiveness of such measures (CARVALHO, 2018). In Art. 7, in turn, the LGPD presents a list of hypotheses, and thus deals with the multiple situations aimed at the treatment of such data. Throughout the items, the need for consent by the holder is expressed, and thus, the prominence of the right to informational self-determination in the context of the processing of personal data is expressed, as well as that the processing can be carried out for the fulfillment of a legal or regulatory obligation by the controller (CARVALHO, 2018). It also deals with the possibilities of processing by the public administration and the research bodies of such data, ensuring, whenever possible, the anonymization of personal data.

FINAL CONSIDERATIONS

This article sought a reflection on some parameters that should be considered for the understanding, application and effectiveness of the General Data Protection Law. It also drew attention that, in order for this right to be possible and preserved, it is necessary to rethink a question of infrastructure and performance of professionals who can establish criteria so that, especially in the digital context, security can occur.

It is believed that although the law is considered an advance in the legal context, discussions should still prevail, especially in understanding the flow of information and data in the digital context, providing an exchange between legal knowledge and knowledge in information technology, so that this right is effective.

REFERENCES

BIONI, B. **Proteção de Dados Pessoais** – A Função e os Limites do Consentimento. 2. ed. São Paulo: Forense, 2019.

BIONI, B.; DIAS, D. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, v. 9, n. 3, p. 1-23, 2020.

CARVALHO, L. *et al*. Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais. *In*: VII WORKSHOP DE TRANSPARÊNCIA EM SISTEMAS, 2019.

CARVALHO, L. P.; OLIVEIRA, J.; CAPPELLI, C. Pesquisas em Análise de Redes Sociais e LGPD, análises e recomendações. *In*: IX BRAZILIAN WORKSHOP ON SOCIAL NETWORK ANALYSIS AND MINING. **Anais**. SBC, p. 73-84, 2020.

CARVALHO, V. M. B. de. **O direito fundamental à privacidade ante a monetização de dados pessoais na internet**: apontamentos legais para uma perspectiva regulatória. 2018. 146f. Dissertação (Mestrado em Direito) – Universidade Federal do Rio Grande do Norte, Natal, RN, 2018.

DIVINO, S. B. S.; LIMA, T. M. M. Responsabilidade civil na Lei Geral de Proteção de Dados brasileira. **Revista Em Tempo**, v. 20, n. 1, 2020.

FRAZÃO, A.; OLIVA, M. D.; ABILIO, V. da. S. Compliance de dados pessoais. *In*: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (org.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. São Paulo: Thomson Reuters, 2019. 677-715.

LAW, T. **A Lei Geral de Proteção de Dados**: uma análise comparada ao novo modelo chinês. 2020. 306f. Tese (Doutorado em Direito Comercial) – Pontifícia Universidade Católica de São Paulo, São Paulo, SP, 2020.

MENDES, L. S.; DONEDA, D. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, v. 120, Ano 27, p. 469-483, 2018.

MIRAGEM, B. A lei geral de proteção de dados (lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, v. 1009, 2019.

RONCOLATO, M. **O que diz o projeto de lei de proteção de dados que tramita no Senado**. 2018. Disponível em: https://www.nexojornal.com.br/expresso/2018/06/07/O-que-diz-o-projeto-de-lei-de-prote%C3%A7%C3%A3o-de-dados-que-tramita-no-Senado. Acesso em: 28 jun. 2021.

SILVA, M. **O arquivo e o lugar**: custódia arquivística e a responsabilidade pela proteção aos arquivos. Niterói: Eduff, 2017.

[1] Graduated in Law from Faculdade Unipê. Specialization in Constitutional and Administrative Law by Uniamérica.

[2] PhD in Psychology and Clinical Psychoanalysis. Doctorate in progress in Communication and Semiotics at the Pontifícia Universidade Católica de São Paulo (PUC/SP). Master's Degree in Religious Sciences from Universidade Presbiteriana Mackenzie. Master in Clinical Psychoanalysis. Degree in Biological Sciences. Degree in Theology. He has been working with Scientific Methodology (Research Method) for more than 15 years in the Scientific Production Guidance of Master's and Doctoral Students. Specialist in Market Research and Health Research. ORCID: 0000-0003-2952-4337.