



Brazil's General Data Protection Law and GDPR:

history, analysis
and impacts.



B/
LUZ

/ Authors

Renato Leite Monteiro

Maria Cecília Oliveira Gomes

Adriane Loureiro Novaes

Gabriela Moribe

Dennys Eduardo Gonsales Camara

Pamela Michelena De Marchi Gherini





/ Preface

Until recently, the matter of data protection was peripheral to the activities of companies. Despite the concern there were no risks and exposure as they multiply at present. Furthermore, domestic regulations are now coming with more severe penalties.

Thinking ahead of our time has always been our culture and innovation is part of our institutional mission. In addition to having worked with technology and data protection matters for more than ten years, we have been one of the early full-service law firms in structuring a Data Protection team with credited knowledge and experience in the domestic and international markets, long before the GDPR and the LGDP, the main legislations on the matter.

Currently, we have a team of specialists who are well prepared to advise domestic and foreign companies over the most complex legal compliance processes, as well as over matters related to consulting, contracts and litigations in the different sectors of the economy, among which, aviation, logistics, health, financial, payment, insurance, retail, digital advertising, e-commerce, online platforms, urban mobility, and data brokers.

This study comes as a small demonstration of another important characteristic of our firm; we have always favored the democratization of knowledge and the broad access to information. Several of our initiatives corroborate this perspective that we have of the world: **(i) the large number of studies widely shared through our website;** (ii) the structuring of a **Research & Development** team consisting of lawyers and interns dedicated to producing relevant legal content inside and outside of our premises; (iii) the creation of **Privacy Hub**, a collaborative initiative looking to raise awareness on the importance of data protection for the market; (iv) the **Espaço Startup**, which allows access to entrepreneurs of all sizes and free of charge to documents, contracts, studies and content that would normally come with a price, made unfeasible at times; and (v) the various associations throughout the world with which we actively contribute to the **development of knowledge**.

With this in mind and our all-time objective of contributing to the understanding of the development of personal data protection, elucidating the Brazilian Data Protection Act, how it relates to the European legislation and the modifications made by the recently published Provisional Measure, let us present this study prepared by our areas of Data Protection and Research & Development.

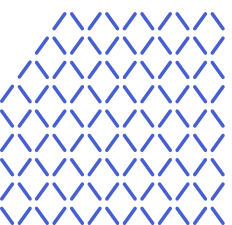
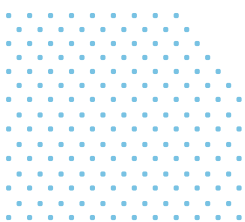
Baptista Luz Advogados



/Abstract

The Lei Geral de Proteção de Dados in Brazil ("LGPD"), Law 13709 was passed on August 14, 2018, the Brazilian General Data Protection Law. In this study we will set out to describe the process and the result of creating a normative structure seeking to harmonize and expand the right to personal data protection within the Brazilian regulatory context. In order to achieve that, we will analyze how the right to personal data protection has arisen in the world as well as how it has gradually been developed in the European Union and Latin America. Our scope of analysis will occur between the LGPD and Regulation of the European Union no. 2016/679, known popularly as the General Data Protection Regulation ("GDPR") which came into force in 2018.

We will compare European and Brazilian norms so that we can understand the historical context from 2010 to 2018, which culminated in the approval of the LGPD. Moreover, we must understand how this law will conciliate with the sectoral rules of data protection already existing in the country, also addressing the main cornerstones and relevant points of the LGPD in order to clarify its importance and impact. Finally, considering that the GDPR also came into force in 2018, we will superficially address some points of contact between both norms.



Summary

06

/ Introduction

- 1.1. The First Steps in Data Protection over the World
- 1.2. From Public Consultation to Presidential Decree (2010-2018)
- 1.3. Objective

13

/ Data Protection: The Construction of a Right

- 2.1. Has the Eight-year Debate Resulted in a Good Law?
- 2.2. Then, what about the Sectorial Laws over Data Protection in Brazil?

16

/ The scope of the General Law on Data Protection in Brazil

- 3.1. Personal Data and Categories of Data
- 3.2. Legal basis
- 3.3. Anonymization vs. Pseudonymization
- 3.4. Data Sharing
- 3.5. Hypotheses of Data Deletion
- 3.6. Rights of Data Subjects
- 3.7. Cross-border Processing
- 3.8. Incident Reporting
- 3.9. Information Security Standards
- 3.10. Sanctions
- 3.11. Data Protection Authority
- 3.12. Data Protection Impact Assessment

27

/ GDPR vs. LGPD: what changes under the new Brazilian law?

- 4.1. Legal Basis
- 4.2. Data Protection Officer
- 4.3. Consent
- 4.4. Retention Period

/ Conclusion

/introduction

1.1 The First Steps to Data Protection over the World

Even though privacy is a universal right, provided for in Article 12 of the Universal Declaration of Human Rights¹, the fact is that the privacy of an individual is a right related to their personal sphere. The notion is then to protect the private life of a person by separating it from the public sphere.

.....
1. UN GENERAL ASSEMBLY. Resolution 217 A (III). Paris, Dec. 10, 1948. Universal Declaration of Human Rights.

In 1970, after the growth and development of the computer technology scenario in the 1960s, the first state law on data protection in history was instituted in the Hesse's German state. Denominated the Hessisches Datenschutzgesetz, the Hesse's Data Protection Act² was created as a result of the need to handle with more care the personal information of individuals stored in electronic media. Such law pioneered the gathering and processing of data from individuals, although not objectively and under segmented criteria.

Some years afterwards, in 1973, Sweden's first national data protection law, i.e. the Sw. Datalagen, or the Swedish Data Act³ was passed. Like Hesse's law, the Swedish law provided for the protection of data in a generic manner, not setting forth, for instance, in which situations data collection could occur or not; merely providing that such collection should be made with the authorization of the competent government agency⁴. Nor did the law provide general principles on the processing of personal data; something recurrent in the modern laws over the matter. Nevertheless, the law was innovative as it brought the matter of data protection of citizens to the public agenda of the government.

Following this trend six years later, in 1979, several other European nations such as France, Germany and Denmark had already passed their own data protection legislation. Such laws, although very important, were nonspecific, e.g. the Swedish and the German. It should be noted that Portugal, Spain and Austria even considered privacy as a fundamental right in their Constitutions - which clearly illustrates the importance given

2. GERMANY. Hessisches Datenschutzgesetz, Jan. 7, 1999. Available at < <http://www.ess-koeln.de/dokumente/160/151010084004Hessen.pdf> >. Accessed Sept. 29, 2018.

3. ÖMAN, Sören. Implementing Data Protection in Law. Available at <<http://www.scandinavianlaw.se/pdf/47-18.pdf> >. Accessed Aug. 18, 2018.

4. Ibidem

to the matter by these nations in the late 1970s⁵.

In 1981 the European Council approved Convention 108 on the protection of individuals regarding the automatic processing of personal data⁶, as it was "desirable to extend the protection of fundamental rights and freedoms to all persons, the respect to their privacy, taking into account the growing flow of personal data across borders, which are subject to automatic processing". This would be the first cross-border legal framework on data protection. The convention went through a recent updating process which ended up in its modernized version known as Convention 108+⁷. After two decades, along with the increasing development of the technological scenario, data protection laws gained more space adopting a more similar format to that of the laws we have today, a framework that consolidated when the European Union, 25 years after the Hesse Law, promulgated Directive 95/46/EC⁸ in 1995.

The norm was a landmark in data protection as it provided for the processing of data and user rights in all member countries of the bloc, putting them all under the same legislation. In addition to establishing how data collection and processing should be conducted, the Directive sets out the principles to follow in such operations, among which the most

5. RUDGARD, Sian. Origins and Historical Context of Data Protection Law. Available at <https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf >. Accessed Aug. 18, 2018.

6. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Jan. 10, 1981. Available at <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> >. Accessed Nov. 21, 2018.

7. Council of Europe. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. May 18, 2018. Available at <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf>. Accessed Nov. 21, 2018.

8. EUROPEAN PARLIAMENT. Directive 95/46/CE. of Oct. 24, 1995. Relating to the Protection of individuals in regard to the processing of personal data and free circulation of such data. Available at < <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT> >. Accessed Aug. 18, 2018.

noteworthy is the lawfulness of processing, limitation of purpose, adequacy, necessity and transparency, aimed at curbing possible abuse by persons in charge. Directive 95/46/EC was in force until May 2018, when it was replaced by Regulation 2016/679 of 27 April 2016, known as the General Data Protection Regulation (“GDPR”), the new European general law on data protection⁹.

Many see the GDPR as the most comprehensive data protection legislation in the world¹⁰. It turns out to be an evolution of Directive 95/46/EC, the result of a long democratic process¹¹, with its scope of application including not only data of natural persons within the European Union, but all the data flow existing in the member countries as well as the countries around the world which have points of contact with the European market¹². Within the main advances of the new law are the expansion of user rights¹³ and more accountability of entities and companies that

conduct data processing¹⁴.

Outside of the European environment we can see that out of the 12 South American countries, only Argentina, Chile, Colombia, Peru, Uruguay, Paraguay and the French Guiana have general laws for data protection of data subjects. Brazil became part of this group after the approval of Law 13709 of August 14, 2018, also known as the Lei Geral de Proteção de Dados (“LGPD”). Furthermore, within the South American context, it should be noted that Ecuador¹⁵, Bolivia¹⁶, Venezuela¹⁷ and Guyana¹⁸ also have sectoral laws on data protection, Suriname being left as the only country in the continent without laws on the matter as of this date.

In Argentina, the Law on Personal Data Protection, or Ley de Protección de los Datos Personales¹⁹, of October 2000, contains provisions and general principles regarding the rights of data subjects, the responsibility of the organizations processing data, applicable sanctions and protective measures. It should be mentioned that Argentina and Uruguay are today the only South American countries with adequate levels of data protection pursuant to

9. For a thorough view of the history of the data protection laws you can access: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection--regulation_en

10. ALBRECHT, Jan Philipp. How the GDPR Will Change the World. Available at <https://edpl.lexxion.eu/data/article/10073/pdf/edpl_2016_03-005.pdf> Accessed Aug. 18, 2018.

11. EUROPEAN DATA PROTECTION SUPERVISOR. The History of the General Data Protection Regulation. Available at: < https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>. Accessed Aug. 18, 2018.

12. EUROPEAN COMMISSION. Who does the data protection law apply to? Available at <https://ec.europa.eu/info/law/law--topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en>. Accessed Aug. 19, 2018.

13. According to the LGPD, the rights of the data subjects are based on the fundamental rights of freedom, intimacy and privacy provided for in our Constitution whose application will therefore be to the greatest extent possible. In general terms and further elaborated throughout this article are the rights of the data subjects, i.e. those who own the data: awareness of the existence of data processing; access and deletion of data; correction of incomplete, inaccurate or outdated data; anonymization, blocking or deletion of unnecessary, excessive or data processed inconsistently with the provisions of the LGPD; portability, upon express request; information of the public and private entities with which the controller shared the data; information about the likelihood of not granting consent and the consequences of refusal; and revocation of consent, at any time, for the processing of data.

14. INFORMATION COMMISSIONER'S OFFICE. Guide to the General Data Protection Regulation (GDPR). Available at <<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>>. Accessed Nov. 12, 2018.

15. OAS. Normative Development by Country – Ecuador. Available at <http://www.oas.org/es/sla/ddi/proteccion_datos_personales_dn_ecuador.asp>. Accessed Aug. 19, 2018.

16. RED IBEROAMERICANA DE PROTECCION DE DATOS. Legislación-Bolivia. Available at <<http://www.redipd.org/legislacion/bolivia-ides-idphp.php>>. Accessed Nov. 12, 2018.

17. RED IBEROAMERICANA DE PROTECCION DE DATOS. Legislación-Venezuela. Available at < <http://www.redipd.org/legislacion/venezuela-ides-idphp.php>>. Accessed Nov. 12, 2018.

18. Guiana has the Statistics Act of 1965 and the Access to Information Act 2011, which are sectorial data protection laws.

19. ARGENTINA. Ley N° 25.326, of Oct. 4, 2000. General Provisions. General Principles related to data protection. Rights of data subjects. Users and persons in charge of files, registries and databases. Control. Sanctions. Action for Personal Data Protection. Available at <<http://www.oas.org/es/sla/ddi/docs/A7%20ley%20proteccion%20datos.pdf>>. Accessed Aug. 19, 2018.

the European Union²⁰. As we will see later, this classification is very important in the context of the GDPR. Countries with such “appropriate levels” can more easily conduct international transfers of data to countries under the jurisdiction of the GDPR. The Argentine Law is currently through a process of modernization by which it will become more similar to the European regulation²¹.

Chile has the Ley de Protección de Datos de Carácter Personal²², i.e. the Personal Data Protection Act, of August 1999. The norm guarantees rights to the “subjects” of the data processed (the persons whom the data refer to), such as the right to data correction and data deletion, as well as obligations, such as limiting the use of data collected for the purpose informed by the person in charge of its processing.

In Colombia the Ley Estatutaria no. 1581²³ of 2012 is in force; such establishes the general provisions for the protection of personal data in the country and provides detailed information about the principles governing the processing of data, the rights of the subjects and the responsibility of the organizations in charge of such processing.

In Peru in force since July 2011 is the Ley

de Protección de Datos Personales²⁴. This Peruvian law, as well as the others mentioned, provide the principles of the personal data processing, the rights of the subjects, the obligations of the subjects and controllers, the operation of the databases and of a national authority for data protection, as well as the administrative sanctions on the controller.

The Ley de Protección de Datos Personales y Acción de Habeas Data²⁵ came into force in Uruguay in 2011. Such law places Uruguay as one of the only South American countries with adequate levels of data protection pursuant to the European Commission²⁶. As, along with Argentina, it establishes the principles governing the processing of data and the rights and duties of the subjects and those responsible for the processing, besides establishing the creation of a government controlling entity.

Unlike the other countries mentioned, Paraguay does not have a general data protection law, but rather, just a generic norm on the matter. The Ley no. 1682, which regulates the Información de Carácter Privado²⁷ provides broadly over which data can be processed establishing sanctions on organizations that fail to comply with such provisions.

20. EUROPEAN COMMISSION. Adequacy of the protection of personal data in non-EU countries. Available at < https://ec.europa.eu/info/law/law-topic/data-protection/datatransfers-outside-eu/adequacy-protection-personal-datanon-eu-countries_en >. Accessed Aug. 19, 2018.

21. FERNANDEZ, Diego. Argentina’s new Bill on Personal Data Protection. Available at <<https://iapp.org/news/a/argentina-new-bill-on-personal-data-protection/>>. Accessed Aug 19, 2018.

22. CHILE. Ley n° 19628, of Aug. 28, 1999. Protección de datos de carácter personal. Available at < <http://www.oas.org/es/sla/ddi/docs/CH3%20Ley%2019628%20Proteccion%20de%20Datos%20de%20Car%3%A1cter%20Personal.pdf> >. Accessed Aug. 19, 2018.

23. COLOMBIA. Ley Estatutaria N° 1581 of Oct. 17, 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Available at <<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>>. Accessed Aug. 19, 2018.

24. PERU. Ley n° 29733, of July 3, 2011. Ley de protección de datos personales. Available at: <<http://www.oas.org/es/sla/ddi/docs/P6%20Ley%2029733%20de%20proteccion%3%B3n%20de%20datos%20personales.pdf>>. Accessed Aug. 19, 2018.

25. URUGUAY. Ley n° 18.331 of Aug. 18, 2008, Protección de datos personales y acción de “habeas data”. Available at <<http://www.oas.org/es/sla/ddi/docs/U4%20Ley%2018.331%20de%20Proteccion%3%B3n%20de%20Datos%20Personales%20y%20Acci%3%B3n%20de%20Habeas%20Data.pdf>>. Accessed Aug. 20, 2018.

26. EUROPEAN COMMISSION. Adequacy of the protection of personal data in non-EU countries. How the EU determines if a non-EU has an adequate level of protection. Available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>. Accessed Sept. 28, 2018.

27. PARAGUAY. Ley n° 1682, of Jan. 16, 2001. Que reglamenta la información de carácter privado. Available at <http://www.redipd.org/legislacion/common/legislacion/paraguay/Ley_1682_de_2001.pdf>. Accessed Aug. 20, 2018.

1.2. From Public Consultation to Presidential Decree (2010-2018)

Realizing about the need to build a debate agenda on data protection in Brazil, the Ministry of Justice drafted a Bill for Data Protection (“APLPD”) which was offered for public consultation and comments in 2010, when a blog was created on data protection and a Public Consultation on the matter made available, both hosted on website “culturadigital.br”²⁸.

The consultation, which took four months, received comments from the different sectors of society, thus forming a multisectoral quota of contributions. It is worth mentioning that at that time this draft was closely associated with the public discussion about the Marco Civil of Internet, which was still in the process of debate, sometimes referred to as the “Legal Framework for Data Protection”²⁹. With the first comments on the APLPD, an outline of what was to become the future text of the LGPD was made eight years later.

Two years after such first public consultation, on June 13, 2012, Congressman Milton Monti proposed in the Chamber of Representatives Bill 4060 of 2012³⁰ (“PL 4060/12”), which provided for the processing of personal data as well as other measures, with the public consultation promoted by the Ministry of Justice as its primary source of inspiration.

28. Link to access website: <http://culturadigital.br/dados-pessoais/blog/2010/12/15/marco-normativo-de-privacidade-e-protecao-de-dados-pessoais-esta-em-debate-participe/>

29. CULTURA DIGITAL. Guidelines for Discussion on the Normative Framework of Privacy and Data Protection. Available at < <http://culturadigital.br/dadospessoais/diretrizes-e-terminos-de-uso/> >. Accessed Aug. 20, 2018.

30. BRASIL. Câmara dos Deputados. Bill no. 4060 of 2012. Provides on data protection and amends Law no. 12.965 of April 23, 2014. Available at <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066> >. Accessed Aug. 20, 2018.

PL 4060/12, which was filed in the Chamber without much fanfare, was only given course in 2013³¹, when systems analyst Edward Snowden denounced a series of irregularities and surveillance practices on a global scale promoted by the National Security Agency (NSA), an entity connected to the US government³². The repercussion of the case was enormous involving both mass surveillance of network users and heads of state of other countries - a situation by which even Brazil was forced to speak internationally on the matter³³. In view of such circumstance and the PL 4060/12 being unique on data protection in the country at the time, it ended up for debate by the Parliamentary Commission of Inquiry on Espionage in the Federal Senate³⁴.

At the Commission, public hearings on the matter were held³⁵, indicating that such was one manner to promote citizens’ privacy and data protection, as well as a way to avoid state vigilance practices by other countries. After year 2013, the matter of data protection ended up not progressing significantly. The agenda was resumed in 2015 when the Ministry of Justice promoted the second public consultation on the bill on data protection,

31. *Ibidem*

32. GIDDA, Mirren. Edward Snowden and the NSA files – timeline. *The Guardian*. Aug. 21, 2013. Available at < <https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline> >. Accessed Aug. 20, 2018.

33. NAKAGAWA, Fernando; GUIMARÃES, Mariana. International Press highlights “Dilma’s heavy attack on USA espionage. O Estado de São Paulo. Sept. 24, 2013. Available at: <<https://politica.estadao.com.br/noticias/geral,imprensa-internacional-destaca-duro-ataque-de-dilma-a-espionagem-dos-eua,1078297> >. Accessed Aug. 20, 2018.

34. BRAZIL. Federal Senate. Available at: <<https://legis.senado.leg.br/comissoes/comissao;jsessionid=779DDBC-421C9E4637D209B7050309322?0&cod-col=1682> >. Accessed Jan 4, 2018.

35. BRAZIL. Câmara dos Deputados. Bill no. 4060 of 2012. Provides personal data protection and amends Law no. 12.965 of April 23, 2014. Available at <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066> >. Accessed Aug. 20, 2018.

also on the “culturadigital.br”³⁶ platform.

In this second consultation, the contingent of contributions was much larger as well as the suggestions for changes in the wording of the text by different sectors of society³⁷. Based on these recommendations, the Ministry of Justice, following the end of the first term of President Dilma Rousseff, filed the Bill, which then was given number 5276/16 (“PL 5276/16”).

With a more complete text, the PL 5276/16³⁸ ended up moving forward faster than the others. This completeness was due to the volume of public hearings held to hear and debate the matter with representatives of all sectors of the Brazilian society, as well as international players invited to lecture on the matter.

Invigorated by the entry into force of the GDPR on May 25, 2018³⁹, the Chamber and the Senate decided to join forces so that the text of PL 5276/16, considered the most complete, were to be submitted in lieu of PL 4060/12. Which, in the case, had priority of procedure in the House for having been proposed four years before PL 5276/16. Once they were joined, the new version was put on the agenda in the plenary of the Chamber of Representatives on May 29, 2018 being approved unanimously in 20 minutes⁴⁰. After approval of the text in the Chamber, it was taken to the Federal Senate where it was given an ID by the Bill of Rights of the Chamber 53 of 2018 (“PLC 53/2018”)⁴¹.

On July 3, 2018, the text was placed on the agenda of the Committee on Economic Affairs (“CAE”) of the Federal Senate, being given a report from Senator Ricardo Ferraço, then rapporteur of PLS 330/2013, a general bill that was at the same time in course at the Federal Senate⁴². With some requests for amendment with a few substantial changes to the text, it was considered in good standing for vote.

In the same session, approved and received was an urgent request for inclusion in the

36. BRAZIL, Emanuelle. Public Consultation will be base for bill on personal data protection. Câmara dos Deputados. Jan. 28, 2015. Available at <<http://www2.camara.leg.br/camara-noticias/noticias/ADMINISTRACAO-PUBLICA/480920-CONSULTA-PUBLICA-SERA-BASE-PARA-PROJETO-DE-LEI-SOBRE-PROTECAO-DE-DADOS-PESSOAIS.html>>. Accessed Aug 20, 2018.

37. MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: A contextual detailed analysis. Jota. July 14, 2018. Available at <<https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>>. Accessed Aug 20, 2018.

38. BRASSCOM - ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES. Contributions to the Special Commission – Personal Data of Câmara dos Deputados on Law for Processing Personal Data. June 2017. Available at <<http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/Brasscom.pdf>>. Accessed Aug. 20, 2018.

39. GOMES, Helton Simões. Law of European Union protecting persona data enters into force and reaches the whole world; understand it. G1. May 25, 2018. Available at <<https://g1.globo.com/economia/tecnologia/noticia/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo--entenda.ghtml>>. Accessed Aug. 20, 2018.

40. MENDES, Laura Schertel; DONEDA, Danilo. Law of data protection cannot perish at the seashore. FOLHA. Available at <<https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml>>. Accessed Aug. 24, 2018.

41. BRAZIL. Câmara dos Deputados. Bill of the Chamber no. 53 of 2018. Provides on personal data protection and amends Law no. 12.965, of Apr. 23, 2014. Available at <<https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>>. Accessed Aug. 24, 2018.

42. BRAZIL. Federal Senate. Bill of Senate no. 330 of 2013. Provides on protection, processing and use of personal data as well as other provisions. Available at <<https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>>. Accessed Aug 24, 2018.

agenda of the plenary of the Federal Senate⁴³. On July 10, 2018, after strong pressure from the civil society and other sectors, the PLC was scheduled at the plenary of the Federal Senate floor, where it was voted and unanimously approved⁴⁴.

After that, it was sent for approval by the President and held on August 14, 2018 with some vetoes⁴⁵, mainly regarding articles 55 to 59 that constituted and organized the National Data Protection Authority (“ANPD”) and the National Council for the Protection of Personal Data and Privacy on the grounds that there was a flaw of initiative, that is, the entity could not be created by a law of initiative of the legislative power, but it would have to be created by normative initiative originating in the executive power.

Finally, on December 27, 2018, Provisional Measure no. 869 (“MP no. 869/18”), published in the Official Gazette of the Union on December 28, 2018, which promoted changes in the text approved and created the ANPD as well. Provisional measures have immediate application, but they depend on the approval of the National Congress for definitively becoming law and subsequent presidential approval if content is altered, which will be better developed later.

This historical construction of the data protection laws in the world, specifically in the European and South American continents between 1970 and 2018 demonstrates some important points. The first of which is the development of a specific right for the

protection of data subjects, covering online and offline means. The second demonstrates the volume of already-existing laws, as well as the fact that the first law was approved in 1970 in Germany, evidencing the almost 50 years of legislative delay on the subject in the Brazilian territory.

After 48 years of the existence of the first data protection law in the world, Brazil has now its own general data protection law. With the approval of the LGPD, there is some strong expectation of a greater promotion of rights and guarantees for citizens, both online and offline, in order to hopefully safeguard individual rights and foster innovation by establishing clear, harmonious and transparent rules.

1.3. Objective

In order to describe the process and the result of the creation of a normative structure in the Brazilian context, we will analyze how the LGPD conciliates with the already-existing sectoral norms on data protection in the country.

We will also address the main pillars and relevant points of the LGPD in order to clarify its importance and what it has an impact on.

Finally, considering that the GDPR also came into force in 2018, we will superficially address some points of contact between both norms.

43. BRAZIL. Federal Senate. Senators approve the urgency for proposal that changes transportation apps taxation. Available at < <https://www12.senado.leg.br/noticias/materias/2018/05/23/senadores-aprovam-urgencia-para-proposta-que-muda-tributacao-de-aplicativos-de-transporte> >. Accessed Aug. 24, 2018.

44. MENDES, Laura Schertel; DONEDA, Danilo. Law of data protection cannot perish at the seashore. FOLHA. Available at <<https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml>>. Accessed Aug. 24, 2018.

45.

Data Protection: The Construction of a Right

2.1. Has an eight-year-long debate turned into a good law?

The eight years that separate the publication of the first public consultation and the approval of the LGPD were marked by intense debating, in which members of the most diverse sectors of society participated. The concern to improve the law can be observed in the fact that the discussions for the development of the wording of PLs 4060/12 and 5276/16 had two public consultations and 13 public hearings⁴⁶. During the same period, another senate Bill, PLS 330/13, was in progress. It was given only two public hearings and was then filed⁴⁷.

46. BRAZIL. Câmara dos Deputados. PL 4060/12 - Processing and Protection of Personal Data – Previous Meetings. Available at <<http://www2.camara.leg.br/atividadelegislativa/comissoes/comissoes-temporarias/especiais/55alegislatura/pl-4060-12-tratamento-e-protecao-de-dadospeessoais>>. Accessed July 23, 2018

47. BRAZIL. Senate. Bill of Senate no. 330 of 2013. Provides on protection, use and processing of personal data as well as other provisions. Available at www25.senado.leg.br/web/atividade/materias/-/materia/113947 >. Accessed Aug 24, 2018.

These years of debating and the legislative construction demonstrate that the whole process was a great process of maturation on the subject of data protection in Brazil⁴⁸.

Public hearings played an important role in this scenario. Such events were attended by academicians, representatives of the third sector, the private sector, the government and even representatives of the European Union, who were invited to talk about their experience in the legislative process that resulted in the approval of the GDPR. The presence of such representatives made it possible for the parliamentarians who were responsible for the bills in question to lead with very rich information⁴⁹.

These discussions allowed parliamentarians to produce various reports on the subject, as well as amendments to the bills dealt with (11 amendments only to PL 5276/16⁵⁰), which generally allowed for a quite complete law and along with high standards of quality tacitly imposed by the international discussion on the subject. However, the changes brought about by subsequent MP no. 869/18 may have weakened certain points of the LGPD when compared to international standards, as we shall see below.

Strongly inspired in the GDPR, as has been found in many of the various reports presented during the proceedings of PL 4.060/12 in the Chamber and later in the

.....
48. BIONI, Bruno. 2010 through 2018: a Brazilian discussion on a general data protection law. Jota. Available at <<https://www.jota.info/opiniao-e-analise/columnas/agenda--da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a--discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018>>. Accessed July 23, 2018

49. CÂMARA DOS DEPUTADOS. PL 4060/12 - Processing and Protection of Personal Data - Previous Meetings. Available at <<http://www2.camara.leg.br/atividadelegislativa/comissoes/comissoes-temporarias/especiais/55aleislatura/pl-4060-12-tratamento-e-protecao-de-dadospessoais>>. Accessed July 23, 2018.

50. BRAZIL. Câmara dos Deputados. Bill no. 5276 of 2016. Provides on processing of personal data for guaranteeing the free development of the personality and the dignity of the natural person. Available at <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>>. Accessed July 23, 2018.

Senate⁵¹, the text in its 65 articles attempted to approach, in its own way, the European legislation. The Brazilian law innovates by bringing into the legal context of the country issues not satisfactorily addressed by other preexisting sectoral data protection laws in Brazil. For example, a more precise definition of the concept of personal data, an explicit provision of the legal basis authorizing the processing of such data, a provision of public data processing, the creation of a Domestic Data Protection Authority, sanctions, etc. In the following items, we will detail the main innovations brought about by the LGPD.

2.2. Then, what about the Sectorial Laws over Data Protection in Brazil?

The concern with privacy and data protection in Brazil arises in an embryonic stage with the entry into force of the Penal Code in 1940. In its article 151, the code provides for the prohibition of violating third-party mail. Although it does not deal exactly with data protection, the article is a milestone for dealing, for the first time in a legal text, with the right to privacy.

The Federal Constitution of 1988 was also somehow concerned with the subject by providing, in its article 5, paragraph X, the inviolability of intimacy and privacy, also ensuring the right to indemnity for material or moral damage resulting from such violation. The constitution also guarantees the inviolability of communications in transit, which can only be intercepted by means of a court order.

The first Brazilian law to actually deal with data

.....
51. BRAZIL. Senate. Bill of Senate no. 4.060 of 2012. Provides on the protection, processing and use of personal data as well as other provisions. Available at <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?-codteor=1001750>. Accessed Sept 26, 2018.

protection and related rights is the Consumer Defense Code, Law no. 8.078, of September 11, 1990 ("CDC"). The norm regulates the relations between consumers and suppliers, establishing obligations and rights for both sides. Consumer data are the matter of Article 43, which gives consumers the right to access and correct information relating to themselves, among other provisions. The CDC was complemented by the Positive Registration Law, Law 12.414/2012, which created a data protection microsystem in the context of consumer relations, more specifically credit compliance and credit modeling, and deals with topics such as the principle of purpose, necessity, and even automated decision review. Several sectoral laws that addressed, in some way, the protection of data, were created in the Brazilian legislature. Such laws deal, for instance, with data relating to health, the financial market, criminal law and even the activities of the public sector.

In the field of health, we point out Resolution no. 1.821/07 of the Federal Medical Council, which provides for electronic medical records and medical data protection, and the Resolution of the National Health Surveillance Agency - ANVISA of Collegiate Board no. 44/2009, which provides for good pharmaceutical practices when rendering these services, including the use of data.

In the financial market, we can observe Complementary Law no. 105 of January 10, 2001, which deals with the secrecy of operations in financial institutions, and Administrative Rule no. 5/2002 of the Secretary of Economic Law of the Ministry of Justice which turned clauses in consumer contracts abusive as they authorize the sending of personal data without prior consent. In the area of Criminal Law, the main example is the recent law, Law no. 12.737, of November 30, 2012, known as the Carolina Dieckmann Act, which made a crime out of the invasion of computer devices. Another important example is Law no. 9.296 of July 24, 1996, which made telephone

interception unlawful.

In the public sector, the main highlight is Law no. 12.527 of November 18, 2011 ("the law of Access to Information"), which is extremely important in guaranteeing citizens access to public data in the three government spheres.

In the world of Internet, Law 12.965 of April 23, 2014 ("the Marco Civil of Internet"), which establishes principles, guarantees, rights and duties for the use of the Internet in Brazil, is considered, along with Decree 8.771/2016, which regulated it, a microsystem of data protection in the context of data processing through the Internet. The Marco Civil, for example, has express consent as a sole legal basis for the processing of personal data, conceptualized by the decree.

In addition to sectoral laws such as those mentioned, there already exists in Brazil a municipal law and a specific municipal law on data protection. The main example is Complementary Law no. 161 of July 12, 2018, in the municipality of Vinhedo, São Paulo. There also are bills in Campinas and São Paulo with the same objective - to guarantee the protection of the data of the citizens of these municipalities. With the entry into force of the General Law of Data Protection, much is questioned about the status of such data protection laws in Brazil. In this scenario, the LGPD can be seen as a general directive for data protection in Brazil. This means that the new law seeks not to replace those that currently exist, but to establish general rules and principles so that they can be met in a more beneficial manner for the subjects of personal data. Of course, if contradictions are found between these laws and the LGPD, the classical rules for decision-making between legal contradictions should be applied.



/ The Scope of the General Law on Data Protection in Brazil

After analyzing the European and South American history on data protection, we will specifically explore the most important provisions in our General Law on Data Protection.

First and foremost, emphasis must be placed on the fact that the LGPD has cross-border application⁵², that is, even entities without physical presence in Brazil, may be subject to it. These factors determine the incidence of the LGPD, as a general rule, (i) that the processing takes place in the domestic territory; or (ii) the purpose of this processing is to offer goods or services or, simply, to give information about individuals located in the domestic territory; or, finally (iii) that the personal data to be processed have been collected in the domestic territory⁵³.

52. The exceptions are described in items of Article 4 of Law 13.709 of Aug. 2018.

53. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 3, items I, II and III.

3.1. Personal Data and Categories of Data"

Our legislation defines personal data as "information relating to a natural person, either identified or identifiable⁵⁴. That is, any information which, separately or associated with some other, allows for the identification of a natural person. The scope of the definition attempts to frame more information into this category by increasing the scope of law enforcement.

Sensitive personal data are within one of the data categories present in the law. The LGPD indicates that sensitive personal data are those about "racial or ethnic origin, religious belief, political opinion, trade union membership or religious, philosophical or political organization, health or sexual life, genetic or biometric data, when connected to a natural person⁵⁵".

The "sensitive" nomenclature stems from the fact that this information may subject an individual to discriminatory practice and, therefore, the processing of such data must comply with more stringent legal bases and higher safety standards.

The third and final category covered by the law is that of anonymized data. These are data related to a subject "who cannot be identified through reasonable technical means and available at the time of processing"⁵⁶.

Anonymized data would not be subject to the rules of law if they could not be reidentified⁵⁷, encouraging innovations such as the internet of things and artificial intelligence. We will discuss the anonymization process in more detail later on.

54. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 5. Item I.
55. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 5. Item II.
56. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 5. Item III.
57. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 12, caput.

3.2. Legal Basis

The LGPD has ten legal basis for collecting and processing data. The legal basis are hypotheses by which the law allows the processing of personal data. Before, in Brazil, there were few legal basis expressly provided by law, such as: consent, the public interest and legal obligation.

With the LGPD, the range of legal basis increased, making data processing possibly more flexible than those based on domestic laws only.

In order to process personal data in a legitimate and lawful manner it is necessary to observe the general principles⁵⁸ and specific legal basis, which depend on the category of data in question.

The LGPD presents 10 hypotheses that allow the processing of personal data, consent of data subject being merely one of those. Such consent shall be provided in writing or by other means demonstrating the subject's intention of expressing it⁵⁹. It is also worth noting that, when it comes to written consent, such should be clearly stated in a clause in the contract⁶⁰ and that the obligation of proof of consent lies with the controller⁶¹. In addition, the data

58. The principles are found in the caput, the ten items of Article 6 of the LGPD, namely: good faith, purpose, adequacy, necessity, free access, data quality, transparency, security, prevention, non-discrimination and accountability.

59. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 8, caput.

60. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 8.

61. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 8, §2.

subject is entitled to revoke consent⁶², free of charge and in a facilitated manner.

The legal basis are: (i) consent of the subject⁶³; (ii) compliance with a legal or regulatory obligation by the controller⁶⁴; (iii) implementation of public policies⁶⁵; (iv) conducting studies⁶⁶ by research agencies⁶⁷; (v) the execution of a contract to which the subject is a party⁶⁸; (vi) the regular exercise of right in judicial, administrative or arbitration proceedings⁶⁹; (vii) the protection of life⁷⁰; (viii) the protection of health⁷¹; (ix) the legitimate interest⁷²; and, finally, (x) credit protection⁷³.

It is important to note that the legal basis of the legitimate interest of the data controller is present in the legislation. Therefore, the controller can base the data processing for legitimate purposes observed in concrete situations, regardless of the subject's consent, since all legal basis are independent from each other and none prevails over the other⁷⁴.

For sensitive personal data, the rules are more restrictive compared to "common" personal data. In the case of consent of the data subject, it must be made in a specific and prominent manner for the purposes of processing described⁷⁵, except when processing without consent, only when this information is indispensable for the execution of the activities pointed out in the law⁷⁶.

62. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 8, §5.
63. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 7, item I.
64. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 7, item II.
65. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 7, item III.
66. BRAZIL. Law no. 13.709, of Aug. 14, 2018. Article 7, item IV.
67. The definition of the research entity can be found in Article 5, XVII.
68. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item V.
69. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item VI.
70. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item VII.
71. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item VIII.
72. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item IX.
73. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item X.
74. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 10, items I and II.
75. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 11, item I.
76. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 11, item II, items a, b, c, d, e, f and g.

Another data category with a legal basis is the personal data of children who are up to 12 years of age. Consent for processing their data should be specific and prominent and granted by a parent or legal guardian⁷⁷. The processing of personal data of adolescents, that is, those above 12 years of age, must be conducted in their best interest, respecting the legal bases and principles relating to personal data.

3.3. Anonymization vs Pseudonymization

Another point present in the LGPD is the differentiation between anonymized and pseudonymized data. As previously noted, anonymized data are those that cannot identify the subject using reasonable technical means available at the time of their processing. For this reason, they are not considered personal data and such impossibility of identification removes the anonymous data from the scope of the LGPD.

On the other hand, pseudonymized data are those subject to processing which makes them impossible to associate to an individual, except for the use of information kept separately by the controller⁷⁸.

In our LGPD, pseudonymized data can only be used to perform research in public health, observing the rules of article 13 and its paragraphs.

In this case, we can point out that anonymized data, if it is not possible to reidentify an individual under reasonable means, can be widely used, whereas pseudonymized data can only be used for scientific purposes quite restricted.

In addition, the law does not require anonymization, but only indicates it be done where possible, which means that if "A" is a

77. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 14, §1
78. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 13, §4.

company that operates its services on CPF bases, and needs this identifier in order to generate a target, or perform data enrichment, for example, it will not be able to anonymize its database because it would make its services unfeasible, but it could just pseudonymize and encrypt the data in order to mitigate risks associated with possible incidents.

Therefore, it is important to measure this difference in order to understand technically and within the scope of the law, the context of the database of a public entity or company and thus outline actions on how to implement technical measures of pseudonymization.

3.4. Data Sharing

The LGPD defines the shared use of data as:

“... communication, broadcast, international transfer, interconnection of personal data or shared processing of personal databases by public entities and agencies in the fulfillment of their legal competencies, or between these and private entities, reciprocally, with specific authorization, for one or more processing modalities permitted by these public entities, or between private entities;”⁷⁹.

For sharing personal data, a legal basis appropriate to the context of the processing is needed⁸⁰. It is important that the controller have traceability of the personal data that they transfer to their partners, since the data subjects have the rights to know with whom and for what purposes their data are being shared⁸¹, as well as that their demands for correction, elimination, anonymization or

.....
79. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 5, item XVI.
80. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, §5. Despite the fact that this paragraph provides on specific consent, and its exemption afterwards, there was some legal incapacity here. Sharing can take place on any of the legal basis in the referred to Article.
81. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 9, items V and VII, and Article 18, item VII.

blocking be replicated to those who obtain their data shared.

It is important to note that the Public Authorities have greater freedom in the area of data sharing among public administration entities. For example, greater freedom to share sensitive data⁸², structuring personal data for shared use⁸³, among others. However, it should be pointed out that the Public Authority can only share data by means of a specific legal provision which presents the specific purposes for such sharing, taking into account the principle of purpose and legality, as is the case of the Law of Money Laundering, Law to Combat Criminal Organizations and Law of Access to Information. Always respecting the principle of necessity and proportionality at the time of data collection.

With the new wording given to the LGPD by Provisional Measure No. 869/18, the sharing of sensitive health data is also possible for the provision of supplementary health services, such as health plan operators⁸⁴.

Finally, in addition to the rules already established in the LGPD, the Domestic Authority of Data Protection (“ANPD”) may establish complementary norms on the shared use of personal data⁸⁵. As will be better explained in paragraphs 3.11 and 3.12, the ANPD will have the function to supervise compliance with the provisions of the LGPD, as well as to apply the applicable sanctions in case of infringement of one or more of them⁸⁶.

3.5. Hypotheses of Data Deletion

“Deletion” is a term defined in the LGPD as

.....
82. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 23, caput.
83. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 24, Sole paragraph.
84. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 11, Paragraph 4, item II.
85. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 30, caput.
86. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 52, caput.

“exclusion of data or set of data stored in a database, regardless of the procedure used”⁸⁷. In addition, the term elimination is used as a modality of data processing⁸⁸.

The subjects of personal data have the right to demand, at any time and upon request, the elimination of unnecessary, excessive or data non-conforming with the LGPD⁸⁹ and may even request the deletion of data originally processed with their consent⁹⁰. In addition, the personal data must be eliminated by the controller, after the end of its processing⁹¹. This term is observed in the following hypotheses of items in Article 21 of the LGPD:

*“ I – inspect the achievement of the purpose or that the data are no longer necessary or pertinent to the targeted purpose;
II – end of the processing period;
III – communication to data subject, even during the exercise of their right to revoke consent pursuant to provision § 5º of Art. 14 of this Law, safeguarding the public interests;
or IV – determination of the domestic authority upon breaching the provision of this Law.”⁹²*

The right to exclusion of personal data, however, is not absolute. The exclusion, or data requested by the data subject is based on the revocation of consent⁹³. If there is a legal basis, other than consent, authorizing that the data be kept, the company may continue processing such until the purpose of this other legal basis is reached.

That is, since the storage of data is a hypothesis of their processing, it is necessary to have a legal basis for it, either consent or

some other of those provided for in the LGPD. Other exceptions that authorize keeping the personal data are the use for law enforcement or regulation; for a study by a research entity; for transfer to third parties respecting the provisions of the LGPD; and for the exclusive use by the controller, provided that the data are anonymized⁹⁴.

3.6. Rights of Data Subjects

The LGPD seeks to ensure to all natural persons the ownership of their personal data, as well as guarantee their fundamental rights of freedom, intimacy and privacy⁹⁵. In addition, there are a number of specific rights indicated throughout articles 18 and 20 of the law. Among which, we can first classify the one that is known as “direitos ARCO”, which guarantees data subjects: (i) access; (ii) rectification; (iii) cancellation (here referred to as elimination); and (iv) opt-out, i.e. opposing to the processing of personal data (article 18, items II, III, VI and §2).

In addition to these rights, the LGPD also guarantees data subjects: (v) confirmation of the existence of processing; (vi) anonymization, blocking or elimination of unnecessary, excessive or data processed in disagreement with the provisions of the LGPD; (vii) data portability; (viii) information of the public and private entities with which the controller has shared use of data; (ix) information about the possibility of not granting consent and the consequences of refusal; and (x) revocation of consent (articles 18, I, IV, V, VII, VIII and IX).

Besides these rights, it is possible to infer another one in article 20, which is about: (xi) the automated decision review which, with the changes brought about by MP No 869/18 in LGPD, does not have to be performed by

87. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 5, item XIV.

88. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 5, item X.

89. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 18, item IV.

90. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 18, item VI.

91. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 16.

92. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 15.

93. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 15, item III.

94. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 16, items I, II, III and IV.

95. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 17.

natural person⁹⁶.

In this sense, what follows is a brief explanation and examples of some of those rights:

Request for access to personal data. This right allows the data subject to request and receive a copy of their personal data.

Request for correction of personal data. This right allows the data subject at any time to request the correction and/or rectification of their personal data if they identify any incorrectness.

Request for the exclusion of personal data. This right allows the data subject to request the exclusion of their personal data. All data collected should be excluded, unless there is any other reason for keeping them, such as any legal obligation to retain data or the need to preserve them for the rights of the operator or controller.

Opposition to data processing. The data subject has the right to contest where and in which context processing agents are processing their personal data for different purposes. And data subject may object to one purpose or all. In some cases, it is possible to demonstrate that agents have legitimate grounds for processing personal data, which may override the rights of the data subjects, as in such cases they may be essential for the supply of the product and/or service.

Restrict the processing of personal data. This right allows the data subject to ask the processing agents to suspend the processing of their personal data in the following scenarios: (a) if the data subject wishes the agents to establish the accuracy of the data; (b) where the subject specifies that the data be kept even if the agents no longer need them, as necessary, to establish, exercise or

.....
⁹⁶. It is important to bear in mind that the MP 869/18 brought some other significant changes in this Article 20 of the LGPD, removing: (i) the possibility for the data subject to request information on the criteria and procedures used for automated decisions; and (ii) the possibility that the ANPD perform audits to inspect possible discriminatory aspects performed by algorithmic processes; changes that directly impact the principle of transparency and the right to explanation.

defend legal claims; or (c) in cases where the data subject has objected to the use of their data, but the agents need to verify that they have legitimate grounds for using them.

Data subject requests the portability of personal data for themselves or for third parties. Allowing the subject to request that their data be made available in a structured format and interoperable system to facilitate the transfer to other suppliers of products or services, in a similar way as already happens between telephone operators in Brazil, through Resolution 460/2007 of Anatel.

Right to withdraw consent at any time. The subject has the right to withdraw their consent, however, this will not affect the legality of any processing performed before that happens. Depending on the context, if the data subject withdraws their consent, it may not be possible that processing agents provide certain products and services. And if this is the case, they need to warn the subject at the time this occurs.

Request by subject to review decisions. Another important data subject right is to request the review of decisions taken solely on the basis of automated processing of their personal data that affect their interests, including decisions to define personal, professional, consumer and credit profiles and/or aspects of their personality⁹⁷. With the changes brought about by MP 869/18 in the LGPD, such a review no longer needs to be performed by a natural person.

3.7. Cross-border Processing

International data transfer is the transmission of data to a foreign country or an international organization of which the country is a

.....
⁹⁷. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 20, caput.

member⁹⁸; international transfer is also a form of processing personal data⁹⁹. International transfer is only permitted when performed for countries or international organizations that provide an adequate degree of personal data protection¹⁰⁰. The adequacy will be evaluated by the ANPD¹⁰¹ and will take into account, for instance, the general and sectoral rules of the legislation in force at the destination, the nature of the data, compliance with the principles and rights of GPLP subjects, the adoption of security measures provided for in regulation, among others.

International transfer authorization is given when the controller offers and demonstrates guarantees of compliance with the principles, rights of the data subject and the protection regime set forth in the LGPD in various ways, such as specific or standard contractual clauses, global corporate standards or seals, certificates and codes of practice¹⁰².

The transfer may also occur when it is necessary for international legal cooperation, essential to protect the life of the data subject or of third parties, authorized by the ANPD, for international cooperation commitments, for the execution of public policies, provision of specific consent for international transfer, which should be given prominently to the data subject¹⁰³, among others¹⁰⁴.

3.8. Incident reporting

In the event of a security incident with personal data that may lead to risk or damage to the subjects, such as data leakage or improper use

.....
98. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 5, item XV.
99. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 5, item X.
100. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 33, item I.
101. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 34, caput.
102. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 33, item II.
103. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 33, items III through VIII.
104. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 33, item IX and Article 7, items II, V and VI.

of the data, the controller shall communicate and the ANPD¹⁰⁵ will establish a reasonable deadline to report the incident, which should contain at least¹⁰⁶:

- I - a description of the nature of the personal data affected;*
- II - the information on the data subjects involved;*
- III - technical and security measures used for data protection,*
- observing the trade and industrial secrets;*
- IV - risks related to the incident;*
- V - the reasons for the delay, if the communication was not immediate; and*
- VI - the measures that have been or will be adopted to reverse or mitigate the effects of the incident"*

The ANPD, taking into account the seriousness of the incident, may determine - to controller - measures such as the wide diffusion of the occurrence or the adoption of measures that mitigate or reverse the incident¹⁰⁷.

3.9. Information Security Standards

Decree no. 8771, of May 11, 2016, regulates the Marco Civil of Internet and presents in its article 13 guidelines for developing security standards that should be observed by connection and application providers. These guidelines are: establishing strict control over data access, provision of a record authentication mechanism, creating detailed access inventory, and using anti data tampering techniques.

The LGPD introduces new rules on information security standards. Processing agents must adopt technical and administrative security measures to protect personal data

.....
105. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 48, caput.
106. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 48, §1.
107. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 48, §2.

processed¹⁰⁸.

These standards must be adopted from the initial design stage of the product or service. The regime of “privacy by design”, which was consecrated internationally through the GDPR, ends up finding, through this provision, its implementation into our legal system.

The ANPD plays important roles in this area. It will be able to provide minimum standards of privacy according to the nature of the information processed¹⁰⁹, it will be able to provide on standards and techniques for the anonymization process¹¹⁰, to suggest the adoption of standards and good practice for the processing of personal data by the Public Authority¹¹¹, among others.

It is important to mention that the private initiative can also establish good practice and information security standards¹¹². When developing these standards, the LGPD sets forth the minimum items that must be observed, determining that whoever wishes to present initiatives:

“a) demonstrates the controller’s commitment adopting internal processes and policies that ensure the comprehensive compliance with standards and good practices regarding the protection of personal data;

b) it is applicable to the whole set of personal data under its control, regardless of the manner it was collected;

c) is adapted to the structure, scale and volume of its operations, as well as to the sensitivity of data processed;

d) establishes appropriate policies and safeguards based on a process of systematic evaluation of impacts and risks to privacy;

e) has the objective of establishing a relationship of trust with the data subject, through transparent action to ensure mechanisms of participation;

f) is integrated into its overall governance structure and establishes and implements internal and external supervision mechanisms;

g) has incident response and remedy plans; and

h) is constantly updated on the basis of information obtained from continuous monitoring and periodic evaluations;”

It should be kept in mind that these are the minimum requirements. Of course, companies can adopt more rigorous safety standards, or even seek to comply with international standards such as the GDPR.

.....
108. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 46, caput.
109. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 46, §1.
110. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 12, §3.
111. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 32, caput.
112. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 50.

3.10. Sanctions

The LGPD provides for a series of administrative sanctions which must be applied by the ANPD. Such as¹¹³:

- I – warning, indicating the deadline for the adoption of corrective measures;*
- II – simple fine of up to 2% (two percent) of the revenue of a legal entity of private law, group, or conglomerate in Brazil in their last year, excluding taxes, limited to the total amount of R\$ 50,000,000.00 (fifty million reais) per infraction;*
- III – daily fine, observing the total limit that item II refers to;*
- IV – publishing the infraction after duly ascertained and its occurrence verified;*
- V – blocking the personal data to which the infraction refers, until the regularization of the processing activity by controller;*
- VI – elimination of the personal data that the infraction refers to;”*

In order to define the applicable sanction, the ANPD will use as a parameter¹¹⁴ the seriousness and nature of the infractions and personal rights affected, the good faith of the offender, the advantage gained or intended by the offender, the economic condition of the offender, the recidivism, the extension of the damage, the cooperation of the offender, proof of the use of mechanisms capable of minimizing damages, the adoption of policies of good practice and governance and the prompt adoption of corrective measures.

Finally, the ANPD may, by its own regulation, define the methodologies that will guide the calculation of the basic value of administrative penalties related to infractions to the LGPD, which should be subject to public consultation¹¹⁵.

113. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 52.

114. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 52, §1, items I through X.

115. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 53, caput.

3.11. Data Protection Authority

As already briefly mentioned in the bill approved by the National Congress, the ANPD would be an autarchy connected to the Ministry of Justice. However, the articles referring to its creation¹¹⁶, present in PLC 53/2018, were vetoed in the presidential approval stage. The central justification for this veto was that the institution of the ANPD through the LGPD had an initiative flaw, due to the fact that its creation would be the competence of the Executive Power¹¹⁷, according to Michel Temer¹¹⁸.

Thus, on December 27, 2018, President Michel Temer issued MP no. 869/18, published in the Official Gazette of the Union on December 28, 2018, which, in addition to promoting certain changes in the approved text of the LGPD, also created the ANPD as a direct federal public administration entity and directly connected to the Presidency of the Republic^{119 120}.

According to the text of Provisional Measure no. 869/18, the ANPD will consist of six departments, most notably the Directing Council, the National Council for the Protection of Personal Data and Privacy, the legal advisory body and specialized units¹²¹, which are likely to be distributed across the country.

116. BRAZIL. Câmara dos Deputados. Bill of the Chamber no. 53 of 2018. Article 55 and subsequent.

117. Vetoed - lei geral de proteção de dados. Senado Notícias. Aug. 15. 2018. Available at <<https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais>>

118. Ibidem.

119. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 55-A.

120. The MP 870/2019, which sets forth the basic organization of the agencies of the Presidency of the Republic and of the Ministries, also the ANPD as an integral agency of the Presidency of the Republic, in its article 2, item VI.

121. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 55-B.

The Board of Directors shall consist of five directors, one of whom shall be the Director President¹²². The members of the Council shall be appointed directly by the President of the Republic for commission positions¹²³, and objectively selected¹²⁴. In addition, the term of office of the members of the Board of Directors will be 04 years¹²⁵, with the first appointments having differentiated terms according to what is established in the Appointment Act¹²⁶.

On the other hand, The National Council for the Protection of Personal Data and Privacy will consist of 23 members, with a multisectoral composition¹²⁷.

Basically, the National Council will be an advisory body, with no sanctioning or investigative power, an accessory to the ANPD, which will assist in the elaboration of the National Policy for the Protection of Personal Data and the performance of the ANPD. The National Council should prepare reports to ascertain the actions of the National Policy, and may also conduct studies, debates and public hearings on issues related to privacy and data protection, and circulate knowledge to the general population¹²⁸. With regard to the competencies of ANPD¹²⁹, we highlight the zeal for the protection of personal data, to inspect and apply sanctions, among several other functions previously mentioned¹³⁰. In short, it is a regulatory body with regulatory, inspecting, sanctioning and disciplinary functions that will have a comprehensive action, dealing with public and private bodies that process personal data.

.....
122. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 55-D, caput.

123. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 55-D, §1.

124. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 55-D, § 2.

125. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 55-D, § 3.

126. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 55-D, §4.

127. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 58-A

128. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 58-B, items I through V.

129. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 55-J, items I through XVI.

130. The ANPD is mentioned in our items related to International Data Transfer, Notification of Incidents, Security Standards of Information and Sanctions.

Finally, it is worth remembering that the Provisional Measures have immediate application, but they depend on the approval of the National Congress for definitively becoming law and subsequent presidential sanction if its content is changed. Thus, such changes brought about by MP 869/18 in the LGPD may lose effectiveness if rejected by the National Congress or lose validity if the term expires before becoming law of the MP by the National Congress.

3.12. Data Protection Impact Assessment

The data protection impact assessment is defined in the LGPD¹³¹ as the controller document that aims to map all processes on personal data processing performed by the organization that may pose risks to civil freedoms and fundamental rights, as well as measures, safeguards and mechanisms to mitigate these risks. The LGPD provides that the ANPD may request the controller to prepare, present and publish the impact report on data protection at different times¹³²¹³³. And from the construction of the report it is possible to visualize the company data map and identify the existing risks in the data flow. Thus, the document becomes an important stage in the process of demonstrating compliance with the Law.

In view of the temporary absence of a Brazilian authority, which, in addition to the inspection role, aims to contribute to the improvement of the data protection ecosystem in Brazil, it is difficult to prepare an impact report, without the authority indicating which are the methodologies and standards that should be used at the time of its elaboration.

.....
131. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 5, item XVII.

132. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 10, paragraph 3 and Article 38, sole paragraph.

133. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 38.

Thus, in the absence of recommendations, companies and organizations that wish to start the process of compliance with the LGPD can use the methodologies approved by foreign data protection laws and authorities while this subject is not yet defined in Brazil.

Given that the LGPD was very much inspired in the GDPR's European legislation, it is possible to seek methodologies and formats already adopted in the European scenario as a parameter for structuring and applying the impact report to data protection.

The idea of developing an impact report on data protection emerged in the 1995 European Union Directive with the Privacy Impact Assessment ("PIA"). The PIA sought to address risks and mitigators regarding individuals' privacy, however, it did not address specific data protection issues. This changed with the entry into force of the GDPR, which introduced the Data Protection Impact Assessment ("DPIA"), bringing methodologies and requirements for the elaboration of the document, besides making its elaboration compulsory in several hypotheses as in the case of data processing on a large scale and when there is public access monitoring.

With the creation and constitution of the ANPD, the data protection impact report will possibly gain form and design, in order to structure defined methodologies and establish minimum criteria for their elaboration. While the ANPD is not set up, it is still necessary to use the best models in the international scenario so that the assessment is made possible and prepare the report demonstrating compliance with the law.

The DPIA has then become an instrument that allows a photograph of the status of the regulatory compliance of the regime of data protection laws, including the LGPD, the GDPR and sectoral laws. After this photograph, you can identify what needs to be done to achieve compliance. This may include reviewing processes, drafting policies, revising contracts, appointing supervision teams, and applying data protection methodologies from the time of conception, known as privacy by design.

/ GDPR vs LGPD: what changes with the new Brazilian legislation?

The comparison between the GDPR and the LGPD is a matter of great practical value. It is worth mentioning that the GDPR can be applied to Brazilian companies, considering that their territorial scope covers data collected from natural persons that are in the European Union¹³⁴. Therefore, the question arises: is it possible to be in agreement with both laws?

To answer this question, it is necessary to compare the main elements in both legal texts. After all, do laws have irreconcilable standards or is it possible to comply with both regulations?

134. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 3.

4.1. Legal Bases

The LGPD presents 10 legal bases¹³⁵ for the legitimate processing of personal data, while the GDPR is limited to 6¹³⁶. We will compare the bases provided in both laws. Consent is a legal basis found in both regulations^{137 138}. On this point, the norms present some similarities, such as: written consent should be included in a clause apart from other clauses^{139 140}; the proof of consent is an obligation to the controller/person in charge^{141 142}, among others. An important difference between the norms is that the GDPR does not characterize consent as “free” when it appears as a requirement for the provision of a service¹⁴³, while the LGPD only notes that the personal data subject should be informed when data processing is a condition for obtaining a product or service¹⁴⁴. In turn, the processing of personal data for the exercise of functions of public interest^{145 146} has important differences.

The first of these is that GDPR, in its recital 31¹⁴⁷, states that processing based on this legal basis does not imply that the authorities

can share them among themselves; while the LGPD allows such sharing in the same paragraph that deals with this legal basis¹⁴⁸, provided that the specific purposes of implementing public policies under Article 26 are met. Also, with the amendments brought about by MP no. 869/18 in the LGPD, the list of exceptions to the sharing of personal data by the Public Authorities with private entities has been expanded, being possible to carry out such transfer when¹⁴⁹: (i) there is a decentralized execution of public activity that requires the transfer; (ii) the private entity has appointed a person in charge; (iii) when there are legal provisions or administrative legal instruments; (iv) where the transfer is for the purpose of fraud prevention, security and integrity of the data subject; and (v) data are publicly accessible.

Another important point on this subject is that the LGPD allows the data processing by the public administration to be backed by contracts, covenants and similar instruments, giving greater openness than the GDPR. The controller’s legitimate interest is a legal basis in both norms, limited by the rights and fundamental freedoms of data subjects¹⁵⁰¹⁵¹. However, there are also divergences. The LGPD does not allow the processing of sensitive data of children and the international transfer based on the legitimate interest. Moreover, the LGPD does not make any further consideration as to whether this legal basis could be applied to public entities in the context of their activities, and there is no

135. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7.

136. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 6.

137. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 6, 1.

138. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item I.

139. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 7, 2.

140. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 8, §1.

141. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 7, 1.

142. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 8, §2.

143. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 7, IV.

144. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 9, §3.

145. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 6, 1 e).

146. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item III.

147. The considerations within a legal norm look to present the prerogatives for better interpretation of the articles of any given law.

151. However, there are also divergences.

The LGPD does not allow the processing of sensitive data of children and the international transfer based on the legitimate interest. Moreover, the LGPD does not make any further consideration as to whether this legal basis could be applied to public entities in the context of their activities, and there is no

148. Furthermore, while on this topic, Article 25 of the LGPD states that “personal data processed by the Federal Government should be kept in an interoperable format and structured for shared use ...”. BRAZIL. Law no. 13.709 of Aug. 14, 2018.

149. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 26, §1º, items I through VI.

150. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 6, 1 f).

151. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item IX.

express limitation, as in the GDPR¹⁵².

It is worth mentioning that the LGPD presents some specific rules on processing based on the legitimate interest. In this case, the personal data must be strictly necessary for the intended purpose when processed by means of the legitimate interest, and the transparency of the data subjects must be guaranteed by this legal basis¹⁵³. It is necessary to apply a proportionality test that takes into account the legitimacy of the purpose, the possibility of a more appropriate legal basis, beyond the expectations of the data subject, within the processing context, and the need to apply safeguards aimed at mitigating possible damages to data subjects.

On the legal basis below there is no substantial difference between the regulations: execution of a contract in which the data subject is a party^{154 155}, for compliance with a legal obligation by the controller^{156 157}, protection of the vital interests of the data subject or third parties^{158 159}.

Having exhausted the legal basis present in the GDPR, it is still necessary to observe whether it, in any way, refers to the other four legal basis present in the LGPD, namely: (i) conducting studies by a research entity, (ii) regular exercise in judicial/administrative process, (iii) for the protection of health in procedures

.....
152. "The first paragraph, line (f), shall not apply to the processing of data conducted by the public authority in the performance of their tasks by electronic means." EUROPEAN UNION. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016. General Data Protection Regulation. Article 6.

153. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 10, §1 and 2.

154. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item V.

155. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 6, 1b).

156. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item II.

157. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 6, 1c).

158. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 7, item VII.

159. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 6, 1 d).

performed by health professionals and health care providers; and (iv) credit protection.

In the context of conducting studies by a research entity, the GDPR determines that the Member States should reconcile the rules guaranteeing academic freedom of expression with the right to the protection of personal data and may create exceptions to ensure the balance of these fundamental rights¹⁶⁰. The law also provides that the data subject has the possibility of limiting consent to specific categories or research projects¹⁶¹. The GDPR treats the exercise or defense of a right in a judicial proceeding as a hypothesis in which the processing of personal data may be less restricted, although not in itself a legal basis. The rights of the data subject to demand that their data be erased or rectified, or the processing of it limited, may be reduced if the processing is necessary for the defense or exercise of rights in a judicial proceeding¹⁶². This hypothesis may also allow personal data to be transferred to third countries or international organizations whose level of data protection is not ensured by the European Commission¹⁶³.

The GDPR does not consider health protection within procedures performed by health professionals and sanitarians as a legal basis for data processing, but addresses the issue in addressing sensitive data, since health data are part of such special category of data as we have seen, require a higher standard of security. Member States may also impose new limits and conditions for the processing

.....
160. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Recital (153).

161. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Recital (33).

162. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Recital (65) and Article 18, 2.

163. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 49, 1e).

of data related to health¹⁶⁴.

Finally, there are no specific considerations in the GDPR about a legal basis that has the protection of credit as a purpose. The ground in the European legislation would probably be the legitimate interest or execution of a contract.

4.2. Data Protection Officer

The Data Protection Officer (“DPO”) in the GDPR or the “person in charge” in the LGPD is the person responsible for assisting the controller in complying with legal data protection obligations, through monitoring, counseling, etc.^{165 166}. It is also worth noting that both norms allow regulatory authorities to submit new regulations on incumbents^{167 168}.

Also, following the changes introduced by MP No. 869/18 in the LGPD, the person in charge no longer needs to be a natural person, opening space for nominating legal entities, or committees, or working groups, that can perform such functions. Thus, currently, both norms allow the DPO and/or person in charge to be an employee of the company (natural person) or a third-party service provider (legal entity)^{169 170}.

Even if such exists and performs similar functions in both regulations, several differences can be pointed out. The GDPR

presents more tasks for the DPO. For example, they will manifest themselves in the incident notification^{171 172}, in the development of DPIA¹⁷³ and in prior consultations with the data protection regulator¹⁷⁴.

In addition, the GDPR presents specific concerns about the role of the DPO within the governance of the controller where it operates. The DPO cannot receive instructions on the exercise of their functions, nor can they be removed or penalized on their behalf. The DPO should report directly to the highest level of responsibility for data processing within the company’s organizational structure¹⁷⁵.

Finally, a very important difference between the two norms is the need for a DPO. While the GDPR points to several activities that require the performance of a DPO in the company¹⁷⁶, the LGPD points out that each and every controller should appoint a person in charge in a generic manner¹⁷⁷.

Thus, while the GDPR presents clearer marks of when to appoint a DPO, the LGPD makes the obligation generic, so that it will probably be applied to controllers of all sizes, a hypothesis that may be subject to subsequent regulation by the National Authority of Data Protection, which may even lead to exemptions.

164. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 9.

165. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 41, §2.

166. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 39.

167. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 41, §3.

168. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 47, 1h).

169. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 5, item VIII (Drafted as per MP 869/18).

170. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 37.

171. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 13, 1b) and Article 14, 1b).

172. In the LGPD, the identification of the DPO is compulsory under the terms of Article 41, §1.

173. The DPIA is a provision present in the GDPR, in Article 35 more precisely. It consists of an analysis of the risks of the implementation of a new data-processing technology to the rights and freedoms of data subjects. The participation of the DPO in this procedure is provided for in Article 35, 2.

174. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 36, 3d).

175. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 38, 3.

176. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 37.

177. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 41.

4.3. Consent

Consent is a legal basis in both regulations¹⁷⁸¹⁷⁹, and the definitions used¹⁸⁰¹⁸¹ by each are very similar. Other characteristics that are very similar in both regulations, due to which they do not deserve further consideration, are: the controller's obligation to demonstrate the data subject's consent¹⁸²¹⁸³, the need for written consent to be outstanding in a specific contractual clause¹⁸⁴¹⁸⁵, the right of withdrawal of consent¹⁸⁶¹⁸⁷, consent for the processing of children's data being granted by their parents or tutors¹⁸⁸¹⁸⁹ and consent being one of the few legal bases for processing sensitive personal data¹⁹⁰¹⁹¹.

A relevant point presented by the GDPR relates to individual decisions automated. Data subjects have the right not to be subject to decisions made solely on the basis of

automated processing that significantly affects them¹⁹². This rule shall not apply where the processing takes place on the basis of the data subject's consent to such processing in cases where it is necessary for the execution of a contract in which the data subject is a party or processing is authorized by a Member State of the EU¹⁹³.

The LGPD, on the other hand, guarantees the data subject the right to have their data reviewed when processed by automated means¹⁹⁴, regardless of the legal basis that authorizes the processing - with no exceptions present in the GDPR. It is also worth noting that, with the changes brought about by MP no. 869/18 to the LGPD, it is no longer necessary that the review of automated decisions be made by natural person.

4.4. Retention Period

Both GDPR and LGPD set limits and restrictions on the storage and processing of personal data connected to the attainment of their purpose. In the GDPR, these limits are present under Article 5, which establishes that the data processing will be limited to the purpose for which they were collected¹⁹⁵. As regards the maximum retention period, the European law makes no mention of a specific period, making it only clear that such a period should be limited to the time needed to achieve the purpose for which the data were collected.

Like the GDPR, the LGPD is concerned with limiting retention of data only to what is strictly necessary for its processing. The LGPD does not have a fixed period for the retention

178. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 13, item I.
179. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 6, 1a).
180. The consent granted by the data subject is a free, specific, informed and explicit manifestation of their will, by which the data subject accepts upon a declaration or their unequivocal positive act, that the personal data concerning him are processed; “;. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 4, 11.
181. “XII - consent: free, informed and unequivocal statement through which data subjects agree with the processing of their data for a determined purpose”. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 5, item XII.
182. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 7, 1.
183. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 8, §2.
184. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 7, 2.
185. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 8, §1.
186. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 7, 3.
187. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 8, §5.
188. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 8, 1.
189. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 14, §1.
190. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 9, 2 a).
191. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 11, item I.

192. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 22, caput.
193. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 22, 2a), b) and c).
194. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 20, caput e §1
195. EUROPEAN UNION. Regulation 2016/679 of the European Parliament and Council of April 27, 2016. General Data Protection Regulation. Article 5, 1 b).

of the data processed either, but it establishes under its Article 16 that “personal data will be eliminated after the end of their processing, within the scope and technical limits of the activities.”

Therefore, we see that the data retention period in the LGPD is conditioned upon the necessity of purpose as stated by the controller and, once such purpose is achieved, the data should be excluded from their servers.



/ Conclusion

The historical progress of the data protection laws all over the world (mainly in the European and South American continents between 1970 and 2018) shows that the development of the specific right to data protection is not a recent phenomenon, despite having hit the news after the approval and entry into force of the GDPR.

In addition, the laws in force today, which were created from 1970 onwards after the passing of the first one in Germany are surprisingly voluminous. This shows that although the approval of the Brazilian LGPD was a necessary step, it happened almost 50 years later.

This approval has given rise to strong expectation of a greater promotion of rights and guarantees for citizens in the online and offline environments in order to positively safeguard individual rights and foster innovation by establishing clear, harmonic and transparent rules, following the worldwide trend of protecting these rights. The eight years of debating and the legislative construction demonstrate that all this course was a great process of data protection growth in Brazil, noteworthy because it was during this period that several different bills were evaluated before becoming part of the foundations of the LGPD.

These events were attended by scholars, representatives of the third sector, the private sector, the government and even representatives of the European Union, who were invited to lecture on their experience in the legislative process that ended up in the approval of the GDPR. The presence of such representatives made it possible for the parliamentarians who were responsible for the bills in question to lead with very rich information.

The LGPD can be seen as a general directive for data protection in Brazil. That means that the new law seeks not to replace those that currently exist, but rather to establish rules and general principles that can be fulfilled more beneficially for the citizen. Naturally, in the event of disparities between these laws and those of the LGPD, the classical rules for decision-making upon legal contradictions should be applied.

The Brazilian law was innovative as it provided the domestic legal scenario with issues not satisfactorily addressed by other sectoral data protection laws in Brazil. For instance, as we have discussed, the more accurate definition of the concept of personal data, an explicit provision of the legal basis for data processing, a provision of public data processing, sanctions and even the creation of a National Data Protection Authority. Data, which was made at a later date through the publication of MP no. 869/18 in the Official Gazette of the Union on December 28, 2018.

The LGPD has ten legal basis for collecting and processing data, which was an important innovation as there were in Brazil few legal basis expressly provided by law, such as: consent, the public interest and legal obligation. With the LGPD, the range of legal basis has widened and become more flexible than other general data protection laws in the world.

Among other important innovations is the fact that for processing personal data in a legitimate and lawful manner, it is necessary to observe general principles and specific legal basis, which depend on the category of data in question. Another point present in the LGPD is the differentiation between the terms anonymized and pseudonymized data. We can then point out that the anonymized data have a greater range of use whereas pseudonymized data can only be used for very restricted scientific purposes, different from what happened previously.

Another relevant point of the norm is that international data transfer is now authorized, essentially with international agencies providing an adequate degree of personal data protection or when such is necessary for cross-border legal cooperation. In other situations, it is necessary to observe the appropriate legal provision for a specific kind of transfer.

Finally, the comparison between the GDPR and the LGPD is a matter of great practical value. It should be noted that the GDPR may be applied to Brazilian companies in view of the fact that its territorial scope covers any data collected from natural persons in the European Union. Therefore, many of the similarities found help companies that are adjusted in the scopes of both the GDPR and the LGPD to be compliant.

The GDPR has only six legal basis whereas the LGPD has ten, which means that more protection is provided by the Brazilian legislation. Even though much of the LGPD was based on the GDPR, we can say that the GDPR is more complete and detailed as it comes with an introductory text, for instance, which provides assistance in interpreting the norm a lot more intensely.

Although the LGPD will only enter into force 24 months after its publication, i.e. on August 16, 2020¹⁹⁶, the number of changes it proposes poses an important challenge to the sector in Brazil, especially regarding the adequacy of data collection and processing. In addition to the ethical aspect connected to the method which companies process data with, it is important to bear in mind that sanctions in case of noncompliance with the norm are quite high, thus the importance of the legal interest being protected and the requirement that the sector players prepare for a new regulatory reality.

To assist in the compliance process, public and private entities can make use of several methodologies, among which the Data Protection Impact Report, also known as DPIA, which despite being an instrument for measuring the impact of data-processing practices on data subjects, has become an important tool providing a snapshot of the institution's regulatory compliance status with the data protection laws, including the LGPD, the GDPR and sectoral laws. With this snapshot you can identify what needs to be done to be fully compliant. This may include reviewing processes, drafting policies, reviewing contracts, appointing inspection teams, and applying data protection methodologies from conception, known as privacy by design.

In addition, compliance with the LGPD can be seen as a major competitive edge, since one of the possible consequences of the process is the strengthening of the data subject's trust with the entity that processes them. This can lead to the enhancement of the image and reputation of the company seen by the market as a public entity in society.

In view of all this, it is possible to sustain that the Lei Geral de Proteção de Dados as the GDPR, will have more impact on society as a whole

than the laws before due to their straight and crosswise nature. It is important to remember that while the law aims to guarantee the data subject with greater protection when using their personal data, it fosters economic, technological and innovation development. Such outlook is relevant in the thorough interpretation of law. It is only through this that the interests of the lawmakers and the society will be met.

.....
¹⁹⁶. BRAZIL. Law no. 13.709 of Aug. 14, 2018. Article 65 (Drafted as per MP 869/18). It should be pointed out that in what concerns the ANPD, the Law enters into force on Dec. 28, 2018.



About Baptista Luz Advogados

With more than a decade in the business we come up with effective solutions and innovative ideas for the legal issues of our clients, partners and entrepreneurs.

With professionalism and experience our firm offers high quality legal advice in a personalized manner through which our client is given all the necessary support with precision and lucidity.

Follow us on social media

f in

BRAZIL

São Paulo

Rua Ramos Batista, 444 / 2º Andar
Vila Olímpia / São Paulo / SP / Brasil
tel +55 11 3049 7950

Florianópolis

Rodovia SC 401, Km 4 / Saco Grande /
Florianópolis / SC
tel +55 48 3036 0294

Londrina

Rua Ayrton Senna da Silva, 300 /
Sala 1801, Torre 1 / Gleba Palhano
Londrina / PR
tel +55 43 3367 7050

USA

Miami

78 SW 7th Street Suite 500
Miami / FL 33130 / US
tel +1 (786) 622 2002

Acesse nosso site:
en.baptistaluz.com.br

