sciendo

ICLR, 2022, Vol. 22, No. 2.

Personal Data Protection in Brazil: How Much Europeanization?

Ondřej Filipec
Palacký University Olomouc, Czech Republic
ondrej.filipec@upol.cz (corresponding author)

Malu Paiva Alves
University of São Paulo, Brazil
malupaivaalves@usp.br

Leonardo Nochang Heck
University of São Paulo, Brazil
leonardo.heck@usp.br

Gustavo Delvaux Parma
Federal University of Rio de Janeiro, Brazil
parmagd@gmail.com

FILIPEC, Ondřej; PAIVA ALVES, Malu; NOCHANG HECK, Leonardo; DELVAUX PARMA, Gustavo. Personal Data Protection in Brazil: How Much Europeanization? *International and Comparative Law Review*, 2022, vol. 22, no. 2, pp. 81–104. DOI: 10.2478/iclr-2022-0016

Summary: In this article, we are assessing the impact of GDPR on the adoption of the Brazilian LGPD regulation. The assessment is done in the context of Europeanization. After the introduction of key concepts, the article is providing deeper insight into the LGPD creation, revealing historical and teleological perceptions of the influence: Moreover, a separate chapter is provided on the comparative dimension. Overall, with the adoption of the GDPR EU created a comprehensive regulatory regime, which was reflected by Brazilian lawmakers, who found strong inspiration in the EU regulation and who have decided to converge in order to avoid losses associated with a potential difference between the EU and Brazilian data market. As a result, LGPD is very similar to the GDPR and in many parts is taking the same attitude..

Keywords: GDPR, LGPD, Europeanization, Data Protection, EU, Brazil.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

1 Introduction

On the 25th of May 2018 the famous GDPR[1] entered into force, causing an unprecedented revision of personal data protection in the EU. The adoption and implications of the GDPR were broadly discussed and are also well documented in the scientific literature. However, GDPR is also having a significant normative dimension that is going beyond the EU borders. By adopting the GDPR, it was not the first time that the EU has set relatively high regulatory standards, which have become a source of inspiration for other countries outside the EU. This article focuses on GDPR's influence on the revision of personal data protection in Brazil.

The main aim of the article is to reveal how much the Brazilian regulation (the Brazilian General Data Protection Law, in Portuguese "Lei Geral de Proteção de Dados Pessoais" or LGPD) was influenced by the EU GDPR. The influence over Brazilian regulation will be put into the context of Europeanization, which offers a vital concept for analyzing the transfer of norms, processes and values within a political and legal context. Hopefully, the article will contribute to the exploration of the convergence between Brazilian and EU regulation, but also to the assessment of the broader context in which Europeanization took place, including the identification of supportive intervening variables. The research is also put into the broader context of Europeanization literature. Therefore, the main research question is "How much Europeanization there in Brazilian personal data regulation?" And second: "How was the Europeanization conducted?". Finding answers to these questions will contribute to a better understanding of how the EU can influence countries outside its jurisdiction, which might have potential implications for the Europeanization concept.

The aims are reflected within the structure of the article which is divided into four parts. In the first part, a short introduction to Europeanization is provided, especially in relation to legal analysis and the EU's influence beyond its jurisdiction. The second part presents the main features of the GDPR. This is necessary for identifying the content of Europeanization and distinguishing it from other phenomena, including globalization or simply modernization. The Third part examines the original state of the affairs in Brazil to map domestic conditions that enabled Europeanization. Finally, the last part discusses similarities and differences between the GDPR and the Brazilian regulation, as we expected a certain level of divergence due to the influence of path dependency logic. Similarities are debated in the context of causality, as the appearance of the same provisions at the same time may be caused by other factors, rather than the influence of the EU.

1 In full Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

From the early beginning, it was evident, that GDPR would have a global impact, which was the subject of many studies.[2] Unlike any other complex regulation, the GDPR is under assessment and interpretation by authorities inside and outside the EU.[3] Moreover, its impact is multidimensional, penetrating related regulations areas which must accept the existence of the norm. This is also the case with newly emerging regulations.[4] Despite GDPR effects being a relatively well-researched topic, discussion on the impact of GDPR beyond Europe are still relatively rare. Hopefully, this article will help to explore part of the GDPR's impact on regulatory updates in Brazil within the context of Europeanization.

2 Europeanization of law

The concept of Europeanization is well established in European studies, offering various perspectives including history, political science or law. From the historical perspective, Europeanization was seen similarly to "Americanization" or "Sovietization", referring to the adaptation of structures to external entities merely in the context of the Cold war. Later on when the bipolar division was over, a new space in Europe appeared, allowing its own way of institutional settings associated mainly with the development of the EU.[5] However, this attitude is somewhat limited in comparison to the concepts developed within political science by (today) "classical authors" such as Claudio M. Radaelli, Tanja Börzel, Thomas Risse, Simon Bulmer, Martin Burch, Ian Bache, Johan Olsen, and many others.[6] At the beginning of the 2000s, the Europeanization literature was

2 ALBRECHT, Jan Philipp. How the GDPR Will Change the World. *European Data Protection Law Review*, 2016, vol. 2, no. 3, pp. 287–289; GODDARD, Michelle. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 2017, vol. 59, no. 6, pp. 703–705; RYNGAERT, Cedric, TAYLOR, Mistale. The GDPR as Global Data Protection Regulation? 2020, *AJIL Unbound*, vol. 114, pp. 5–9; sa SAFARI, Beata, A. Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard For Personal Data Protection. *Seton Hall Law Review*, 2017, vol. 47, no. 3, pp. 809–848.

3 PAVELEK, Ondřej, ZAJÍČKOVÁ, Drahomíra. Personal Data Protection in the Decision-Making of the CJEU Before and After the Lisbon Treaty. *TalTech Journal of European Studies*, 2020, vol. 10, no. 1, pp. 167–188.

4 ANDRAŠKO, Jozef, MESARČÍK, Matúš. Those Who Shall Be Identified: The Data Protection Aspects of the Legal Framework for Electronic Identification in the European Union. *TalTech Journal of European Studies*, 2020, vol. 10, no. 1., pp. 3–24; KOCHARYAN, Hovsep, VARDANYAN, Luisine, HAMUĽÁK, Ondrej and KERIKMÄE. Critical Views on the Right to Be Forgotten After the Entry Into Force of the GDPR: Is it Able to Effectively Ensure Our Privacy? *International and Comparative Law Review*, 2014, vol. 14, no. 2, pp. 96–115; VARDANYAN, Lusine, KOCHARYAN, Hovsep. The GDPR and the DGA Proposal: are They in Controversial Relationship? European Studies. *The Review of European law, Economics and Politics*, 2022, vol. 9, pp. 91–109.

5 BORNEMAN, John, FOWLER, Nick. Europeanization. *Annual Review of Anthropology*, 1997, vol. 26, pp. 488.

6 See for example RADAELLI, Claudio M. Europeanization: Solution or problem? *European*

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

growing, which was reflected in the broadness of understanding and problems to define what is exactly behind the term. Different understandings soon resulted in several distinctive conceptualisations: for example Johan P. Olsen is referring to five big categories, and Robert Harmsen and Thomas M. Wilson have about eight categories, but there are studies going beyond this number.[7]

In line with the concepts within political science a legal perspective on Urbanization was also developed, reflecting a very similar attitude to Europeanization, which was understood as a political process. For example, Christina Ferreira defines Europeanization as 1) the creation of a supranational system of norms (*corpus iuris*); 2) A state in which there are norms and concepts influencing national legal orders in the areas that were predominantly national; or 3) a state, in which EU models (rules, principles, concepts or arguments) go beyond EU borders and find its place among EU non-member states.[8] This division reflecting different jurisdictions is logical, as Europeanization has a different nature for the EU member states (creation and implementation of the EU law), for candidate countries that are adopting *acquis Communautaire*, and for the rest of countries where Europeanization is merely a voluntary phenomenon. However, even individual categories have a variety of modifications, as Europeanization might be direct or indirect, enforced or voluntary, comprehensive or partial.

A division implementing two different aspects is brought by Michal Bobek who distinguishes between the normative vs. empirical nature of Europeanization, combined with the scope of analysis.[9] As a result, there are three options including 1) a limited empirical approach; 2) a wider empirical approach and 3)

---

integration online Papers, 2004, vol. 8, no. 16, pp. 1–26; BÖRZEL, Tanja. Towards Convergence in Europe? Institutional Adaptation to Europeanization in Germany and Spain. *Journal of Common Market Studies*, 2002, vol. 39, no. 4, pp. 193–214; BÖRZEL, Tanja, RISSE, Thomas. When Europe Hits Home: Europeanization and Domestic Change. *European Integration online Papers*, 2000, vol. 4, no. 15, pp. 1–14; BULMER, Simon, BURCH, Martin (1998) Organizing for Europe: Whitehall, the British State and the European Union. *Public Administration*, vol. 76, no. 1, pp. 601–628. BACHE, Ian. *Europeanization and Multilevel Governance*. New York: Rowman and Littlefield Publishers, 2008, 206 pp; OLSEN, Johan P. The Many Faces of Europeanization. *Journal of Common Market Studies*, vol. 40, no. 5, pp. 921–952.

7 Compare: OLSEN, Johan P. The Many Faces of Europeanization. *Journal of Common Market Studies*, vol. 40, no. 5, pp. 923–924; HARMSEN, Robert, WILSON, Thomas M. Introduction: Approaches to Europeanization. *Yearbook of European Studies*, vol. 14, pp. 13–26; DANČÁK, Břetislav, FIALA, Petr, HLOUŠEK, Vít. Evropeizace: pojem a jeho konceptualizace. In. DANČÁK, Břetislav, FIALA, Petr, HLOUŠEK, Vít (eds.). *Evropeizace. Nové Těma politologického výzkumu*. Brno: IIPS, pp. 11–25.

8 FERREIRA, Christina. The Europeanization of Law. In: OLIVEIRA, Costa Jorge, CARDINAL, Paolo (eds.) *One Country, Two Systems, Three Legal Orders – Perspectives of Evolution*. Berlin: Springer, pp. 171–190.

9 BOBEK, Michal. Europeanization of Public Law. IN. BOGDANDY, A. et al. (eds.) T*he Max Planck Handbook of Public Law in Europe. Vol. I: Ius Publicum Europeanum*. Oxford: Oxford University Press, 2016, p. 28.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

a wider normative approach. By using the first approach the researcher is usually trying to find features of Europeanization (elements, fragments) within national legislation. The analysis is conducted in order to reveal the scope of Europeanization and uses mainly a "top-down" perspective. The second option is a more complex analysis employing also a "bottom-up" perspective as it understands Europeanization as an interactive process between a national and EU domain. Here a diagonal logic is also applicable, as Europeanization may also affect other levels and actors. It opens the door for a legal pluralism and multicentric conception of law.[10] Finally, in the normative approach, the researcher is trying to find "how the final result shall look like" and discover a sort of "misfit" between the actual state of law and the desired state.[11]

Unlike in political science, "misfit" has a significant legal dimension and there might be various kinds of misfits. Misfit may be simply associated with a transposition deficit, which might have different scope and nature. As a result, "misfit" may range from missing transposition to incomplete transposition or wrong transposition. Misfit may also have a significant normative dimension, going beyond the scope of transposition deficit as in some cases transposition is not required and much softer tools are used.[12] This is also the case of Brazil, which does not have legal obligation to implement EU rules[13], might as well be inspired by the EU regulation due to the fact that Brazil is facing similar issues in data protection and Europe is acting as a soft power – in the terms of culture, political ideals or solutions, which are perceived by others as legitimate.[14] There are various examples where the EU provided a source of inspiration for Brazil and Mercosur cooperation.[15]

The EU's influence beyond its borders has been conceptualized in the work of Frank Schimmelfenning (2009) who distinguished eight ideal types of Europeanization, based on different logic (the logic of consequences and logic of appropriateness) and different channels, which might be intergovernmental or trans-

10 VEČEŘA, Miloš. The process of Europeanization of law in the context of Czech law. *Acta univ. gric. et. silvic. Mendel. Brun*., vol. LX, no. 2, p. 462.

11 BOBEK, Michal. Europeanization of Public Law. IN. BOGDANDY, A. et al. (eds.) T*he Max Planck Handbook of Public Law in Europe. Vol. I: Ius Publicum Europeanum*. Oxford: Oxford University Press, 2016, p. 38.

12 GOMBOS, Katalin. Europeanisation effects in the court jurisprudence. *International and Comparative Law Review*, 2019, vol. 19, no. 1, pp. 262..

13 Look at the issue of extraterritorial application of the EU law: FALALIEIEVA, Liudmyla. Modern Approaches to the Extraterritorial application of the EU law. *European Studies – The Review of European Law, Economics and Politics*, 2014, vol. 1, no. 1, pp. 103–110.

14 NYE, Joseph. *Soft Power: The Means to Success in the World Politics*. New York: Public Affairs, 2004, p. 11.

15 See for example BOAVENTURA, Amorim Elisa, STEHLÍK, Václav. The Human Rights Protection in the EU-Brazil Relations: Structural Considerations and Current Legal Developments. *European Studies – The Review of European Law, Economics and Politics*, 2019, vol. 6, no. 1, pp. 141–156.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

national.[16] In the following parts, we look at Europeanization in Brazil in the area of personal data protection and extend the above concepts to this particular case. In the analysis, we go beyond the "limited empirical approach" as described by Bobek, because we add focus also on the procedural aspects of Europeanization and the involvement of Brazilian institutions. In line with the Schimmelfennig, we are also assessing channels of transfer.

3 The GDPR as a source of Europeanization

This section presents the structural features of GDPR in order to enable a comparison between it and the Brazilian data protection law to be carried out in the following sections. As Europeanization refers to the change or a transfer of norms, it is necessary to reveal the content of Europeanization. However, it is out of the scope of this article to discuss the details of the GDPR, which is why the following text is dedicated only to the most distinctive features of the EU regulation.

GDPR was introduced in 2016 after a years-long complicated discussion on proposed changes to EU data protection law. It was in 2009 that the Commission introduced a consultation about the theme, and it further formalized it in 2012, when a legislative proposal was proposed to be discussed by the European Parliament and the Council of the EU.[17] Its main aim was to modernize and uniformize EU Data Protection Law, substituting the former legal regime which had been instituted in 1995 by the Data Protection Directive (95/46/EC).

As opposed to directives – EU norms that have to be transposed by each member state into its own national legal system – regulations such as GDPR are immediately valid and applicable in all EU member states. This favours harmonization and consistent enforcement across countries.[18] Under the Directive, the member states had much more discretion to shape the specifics of their own data protection regime through statutes that internalized the Directive's norms.[19] This created complexity and increased the costs for stakeholders operating in multiple members of the EU which had to comply with many different regimes.[20]

16 SCHIMMELFENNING, Frank. Europeanization beyond Europe. *Living Reviews in European Governance*, 2012, vol. 7, no. 1, p. 8.

17 European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2018, p. 30.

18 Jan Philipp Albrecht. How the GDPR will change the World. *European Data Protection Law Review*, 2016, vol. 2, n. 3, p. 287–289.

19 But *see* Recital 10 GDPR allowing states to "maintain or introduce national provisions to further specify the application of [GDPR] rules".

20 Simon Davies. The Data Protection Regulation: A triumph of pragmatism over principle? *European Data Protection Law Review*, 2016, vol. 2, n. 3, p. 293–296.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

The process that led to the later adoption of GDPR had also another product: Directive 2016/680, which is applicable to police and judicial authorities in the specific context of law enforcement operations.[21] This is one of the fields to which GDPR does not apply, alongside data processing related to national security, data processing by EU institutions[22] and the data processing carried out by natural persons for personal or household activities (i.e., not associated with commercial activities).[23]

GDPR entered into effect on 25 May 2018 and introduced a fundamental rights-based approach whose aim is to improve the possibility of data subjects to decide how their own data are to be used by private and public institutions.[24] GDPR in this sense implements and regulates the right to protection of personal data guaranteed by article 8 of the Charter of Fundamental Rights of the EU[25] and article 16 of the Treaty on the Functioning of the European Union (TFEU). The incorporation of this right in TFEU lays down the legal basis for EU legislation on data protection in all fields of EU competence. In other words, the Lisbon Treaty, which instituted TFEU, paved the way for the adoption of GDPR.[26]

Article 4 of GDPR presents a large number of definitions used throughout the Regulation. For our purposes, the most important are the ones of "personal data", "processing", "controller", "processor", and "consent". Further definitions may be presented or clarified when necessary. According to Article 4:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

21 Directive (EU) 2016/680 of the European Parliament and of the Council of 26 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the reduction of criminal penalties, and on the free movement of such data.

22 Data processing by EU institutions is governed by Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, OJ L 295.

23 *See* Recitals 16–20 and Article 2 GDPR.

24 Michelle Goddard. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 2017, vol. 59, no. 6, p. 703.

25 As stated by Article 1(2) GDPR. *See* also Article 52 (1) of the Charter (on the standards for limiting rights granted by it).

26 European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European Data Protection Law*, p. 28–9.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; …

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

From these definitions, we can extract some observations about the scope and application of GDPR. First, it protects exclusively the data of "natural persons": legal persons, such as companies, do not enjoy the rights granted by the regulation. Furthermore, only living people are protected by it. The processing of data of deceased persons is to be regulated by the Member States.[27] This definition further excludes from the scope of GDPR the processing of anonymized data, that is, data that has been altered in order to preclude the possibility of connecting it to a specific person.[28] On the other hand, data that has been merely pseudonymized – that is, data that may be attributed to an identifiable individual with the use of some further information – falls under GDPR.[29]

Second, any operation conducted with personal data, starting with its collection up until its destruction, falls under the definition of 'processing', which means that GDPR applies to a large range of behaviors. It covers both manual and automated processing, so human intervention in processing is not relevant to define whether GDPR applies. On the other hand, it is applicable only to pro-

27 *See* Recital 27 GDPR.

28 Recital 26 GDPR. *See* Sanjay Sharma, *Data Privacy and GDPR Handbook*. Hoboken: Wiley, 2020, p. 50.

29 On the implications of this for scientific research, mainly in countries where pseudonymized data had been exempted from data protection laws, *see* Mahsa Shabani and Pascal Borry. Rules for processing genetic data for research purposes under the new EU General Data Protection Regulation. *European Journal of Human Genetics*, 2018, vol. 26, p. 149–156. *See* also Recital 33 GDPR.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

cessing operations regarding data contained or intended to form part of a filing system.[30]

Finally, GDPR institutes a relatively demanding conception of consent, which must be expressly and specifically asserted regarding each particular purpose of processing activities. Consent must be informed and freely given, meaning that the data subject must know at least who the controller is and must also have a genuinely free choice about whether to authorize the processing of her data. If consent may not be refused without detriment, it is not considered to be freely given.[31] As mentioned above the underlying idea is to empower data subjects to make adequate decisions about who may process their data, and how and for what purposes that may be done.[32]

The Controller and Processor are the agents entrusted with personal data and in charge of processing it. The definitions established by GDPR are clear. The Regulation determines that the relation between Controller and Processor must be established through a contract or 'other legal act under Union or Member State law', which must furthermore expressly determine the 'subject matter and duration of processing', its 'nature and purpose', 'type of personal data and categories of data subjects' and 'obligations and rights' of the Controller. The Controller shall only contract Processors who can provide sufficient guarantees that they are able to implement 'appropriate technical and organizational measures' that make processing compatible with GDPR requirements.[33]

One of the basic principles underlying GDPR is that the processing of personal data is only allowed when there are legal grounds for it. In other words, prohibition is the default.[34] Article 6 of GDPR defines the legal grounds that justify data processing. According to it, the processing is lawful only if: 1) the data subject has consented to it; or 2) it is necessary for performing a contract to which the data subject is party or for preparing a contract into which the data subject is willing to enter; or 3) it is necessary for the Controller to comply with a legal obligation imposed on them; or 4) it is necessary for protecting vital interests of the data subject or another natural person; or 5) it is necessary for securing the completion of a 'task carried out in the public interest or in the exercise of public authority vested in the controller'; or 6) it is necessary 'for the purposes

30 Recital 15 and Article 2(1) GDPR.

31 *See* Recitals 32, 42 and 43 GDPR.

32 The full importance of this can only be appreciated if we bear in mind that in modern society information has a great potential to change states of affairs and that to provide information is to empower the one who receives it. The case of Cambridge Analytica is probably the most illustrative example. *Compare* Sanjay Sharma, *Data Privacy and GDPR Handbook*, p. 1–18.

33 Article 28 GDPR.

34 Sahar Bhaimia. The General Data Protection Regulation: the next generation of EU data protection law. *Legal Information Management*, 2018, vol. 18, p. 21–28.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

of legitimate interests pursued by the controller or by a third party', provided that these interests are not overridden by fundamental rights of the data subject.

The lawfulness of processing is coupled with the requirement that it must also be *fair*. This comprises a principle of transparency, according to which it must be clear to the data subject that her data is being collected, stored, or otherwise processed, what the data will be used for, who is the controller, and what the risks, rules, safeguards, and rights regarding the processing.[35] Data processing is permissible when consent is given by a person over 16 years old. In case the data subject is younger than 16, consent must be given by the person who holds parental responsibility over the data subject. Article 8 (1) determines that the Member States might reduce the minimum age for providing consent to data processing but establishes that it cannot be reduced to less than 13 years old.

Another important feature of GDPR is that it identifies some "special categories of personal data" that are subject to stricter rules. These are data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership', 'genetic data, biometric data for the purpose of uniquely identifying a natural person', and data concerning health or sex life or sexual orientation of a natural person.[36]

As mentioned above, GDPR institutes a rights-based approach to data protection. Accordingly, its third Chapter enlists the rights of the data subject. Most relevant for our purposes – and beyond some ideas already presented such as transparency – this Chapter grants a right to access the data subject to information about whether her data is being processed and about the details of the processing activity (Article 15); a right to rectification of inaccurate data held by a controller (Article 16); a right to erasure (Article 17), which is related to but different from (are more restricted than) the right to be forgotten previously recognized by the Court of Justice of the European Union;[37] a right to restriction of processing (Article 18); and a right to data portability that consists in the right to obtain from the Controller the subject's data in a 'structured, commonly used and machine-readable format' in order to transmit the data to another Controller (Article 20). These rights of the data subject correspond to obligations imposed on Controllers and Processors.

35 *See* Recital 39 and Articles 5 and 12 GDPR. Article 12 is part of Chapter III GDPR, which states the 'rights of the data subject'.

36 Article 9 GDPR. On the definitions of genetic data and data related to health, *see* Recitals 34 and 35.

37 *See* Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014: 317. For discussion of the relation between the right to be forgotten and the right to erasure, presenting the conditions under which a data subject may require erasure, *see* Sanjay Sharma, *Data Privacy and GDPR Handbook*, p. 205 ff.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

Beyond these, GDPR also imposes some general obligations on Controllers, namely that they must implement technical and organizational measures 'to be able to demonstrate that processing is performed on accordance' with GDPR (Article 24) and that data protection is to be implemented by design and default (Article 25). This last obligation requires that Controllers adopt technical measures to ensure that the data processing will be, from the outset, minimally invasive.[38] Overall, the EU enacted very complex and ambitious regulation

4 Europeanization of Data protection in Brazil

Before the enactment of the Brazilian General Data Protection Law, the data protection framework in Brazil consisted mainly of sparse statutes that assured basic rights related to informational self-determination and information security within specific areas of law.

Federal Law No. 12,414/2011, for example, introduced new provisions on credit bureaus and their data processing procedures. Its aim was to create the Positive Credit Report, a database containing information about "good payers" (i.e., natural or legal persons that comply with their financial obligations) in order to allow them to be eligible for loans with lower interest rates.

Since its original redaction, the statute has brought data protection-related rights to those registered in the Positive Credit Report, such as the possibility for an individual to request full and free access to his or her own information stored on a platform, including information about who had recent access to the data; the right to request revisions, changes or corrections to the data displayed; and the right to obtain the exclusion of their records within a certain database.

The Code of Consumer Defense and Protection (1990) has also allowed consumers to obtain free access to their information in databases of suppliers of goods and services since its adoption. The statute also established that all data must be displayed accessiblyand that consumers have the right to request corrections or revisions to their own data.[39]

---

38 *See* Recital 78 GDPR and Sharma. *Data Privacy and GDPR Handbook*, p. 84 ff.

39 "Art. 43. The consumer, without penalty from what is said on article 86, will have access to information that exists in registries, forms, and personal consumption data that has been reported about him, as well as their respective sources.

§ 1. Consumer registrations and data must be objective, clear, truthful, and in a language that is easy to understand. It may not contain negative information referring to a date over five years prior.

[…] § 3. If the consumer finds inaccurate information about himself in a file or record, he may demand its immediate correction. The party maintaining the file or record will have five weekdays to communicate the change of this incorrect information to any parties involved." An official English translation of the Brazilian Code of Consumer Defense and Protection (2014 version) can be accessed by: < http://www.procon.rj.gov.br/index.php/publicacao/listar/5/1>.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

Even if the right to privacy is certainly not equal to the right to data protection, they are surely linked in many aspects.[40] Therefore, it is worth mentioning that the right to privacy is also protected by the Brazilian Constitution (1988).[41]

And in 2014 Civil Rights Framework for the Internet came into force. The law, widely regarded as a major landmark in Brazilian digital regulations, established personal data protection as an underlying principle of Internet governance and defined the "non-disclosure of their personal data to third parties, including connection logs and Internet application access logs, except with their free, express, and informed consent or in the cases provided for by law" as a right to every Internet user, among other provisions, such as the duty of data controllers to act diligently when processing personal data.[42]

But, even so, the aim of Brazil's Internet Bill of Rights was to regulate general rights and duties towards Internet access in the country. Even if it had (and still has) important data protection provisions, it cannot, by any means, be considered a law designed specifically to regulate personal data issues.

Therefore, by then Brazil still lacked proper legislation able to ensure strong safeguards for personal data processing. Throughout the years, this became a sensible issue, as nowadays everyone is susceptible to having their data misused by private or public institutions and, through the Internet, data breaches offer an unprecedented threat. Scandals such as the Cambridge Analytica case, in which data of millions of people was harvested to boost political campaigns without their consent,[43] showed the world how our data might be used to shape our behaviour without anyone's knowledge.

---

40 E.g.: KOKOTT, Juliane; SOBOTTA, Christoph. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 2013, vol. 3, no. 4, pp. 222–228.

41 "Article 5. All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms: […]

X – the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured; […]" The official English translation of the Brazilian Constitution, provided by the Brazilian Senate, can be accessed by: <https://www2.senado.leg.br/bdsf/item/id/243334>.

42 "Art. 10. Maintenance and disclosure of Internet connection logs and Internet application access logs contemplated in this Law, of personal data, and of the content of private communications must respect the privacy, private life, honor, and image of the parties directly or indirectly involved. […]

Art. 11. All operations involving the collection, storage, retention or processing of records, personal data, or communications by Internet service and applications providers must comply with Brazilian law and the rights to privacy, protection of personal data, and confidentiality of private communications and records, if any of those acts occur in Brazilian territory.". An unofficial translation of Brazil's Internet Bill of Rights, provided by the Institute for Technology & Society of Rio can be accessed by: < https://itsrio.org/en/publicacoes/understanding-brazils-internet-bill-of-rights/>.

43 CADWALLADR, Carole, GRAHAM-HARRISON, Emma. (2018, Mar 17). Revealed: 50

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

In this scenario, it is every country's duty to protect its citizens against the misuse of their data. But furthermore, since Directive 95/46/EC of the European Union (EU) came into force in 1995, the transfer of personal data to countries outside the EU became a sensible issue, as it would only be possible if the third country could provide an "adequate level of protection". Some exceptions to this rule were created, such as when the controller himself was capable of ensuring that the recipient would comply with the EU's data protection rules, e.g., through data protection contractual clauses.

When Directive 95/46/EC was revoked by the enactment of the GDPR, the same rule and exceptions were again applied in Chapter 5.

But this time things were different than they were in 1995: the GDPR impacted the world's digital economy on a scale rarely seen before,[44] and many countries started a worldwide run to comply with the regulation, as in today's economy data transfer is an indispensable need. Consequently, Brazil also needed to adapt its legal system in order to maintain economical and commercial relations with the EU. A secure path to provide an adequate level of protection according to the GDPR is to produce legislation similar to it. As it will be shown now, this was the option chosen by Brazil.[45]

While the bill that eventually became the Brazilian General Data Protection Law was being discussed in the National Congress (Brazil's federal parliament), the rapporteur chosen to present the proposed legislation in the Chamber of Deputies (the lower house of the National Congress) specifically addressed that the bill had a strong inspiration from the EU legislation. He also stated that it is "extremely pertinent" for a country's data protection legislation to be in line with European regulation, as this would indicate the country's commercial attractiveness in today's global digital economy.

It was also mentioned that a country able to comply with the GDPR would also be in condition to attract data processing from the EU, which could potentially lead to the opening of more branches of foreign companies in Brazilian territory. Therefore, according to the rapporteur's report, there was a need for Brazil to create a data protection law harmonic with the best international practices, such as the EU, while still preserving Brazilian specificities and sovereignty.

million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian* [online]. Available at: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> Accessed: 07.03.2022.

44 BRADFORD, Anu. *The Brussels Effect: How the European Union Rules the World*. 1 Edition. Oxford University Press 2020, p. 152.

45 Even after the Brazilian General Data Protection Law came into effect, Brazil is still not considered a country with an adequate level of protection by the European Commission, but nevertheless, it might also be considered an important step towards this goal. The list of countries recognized as providing adequate protection by the European Commission might be accessed through: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

Then, when the bill was discussed in the Federal Senate (the upper house of the National Congress)[46] the rapporteur from the senate wrote in his report[47] that the enactment of a Brazilian data protection law was an "inescapable need". Still according to the report, by then Brazil had already lost valuable opportunities of international financial investments due to its lack of an effective data protection law. Besides economic justifications, the senator also stated that there would be a social necessity for strong legal data protection safeguards to guarantee citizens' right to privacy and other fundamental rights. Hence, the creation of a data protection culture would benefit different sectors of society: from big tech companies to common citizens.

Similarly to the previous report, the one from the the senate also recognized that the bill was "strongly inspired by the European regulation within specific lines", as the GDPR is a regulation with expressive worldwide recognition. The document stated that the EU Regulation had a global effect, due to its extraterritoriality, and adopting this normative influence would be an expressive gain for Brazil.

Furthermore, it was also defended that the Brazilian society had a lot to gain from this international cooperation as many of the foreign inspirations for the bill had already been tested abroad, but only as long as Brazilian national characteristics were respected by the new data protection statute. Therefore, it was widely recognized during the legislative process behind the Brazilian General Data Protection Law that there was a strong influence on the GDPR. In other words, it is possible to conclude that the LGPD was a notorious case of Europeanization beyond Europe.

As already noticed in the legislative documents, there was strong economic and commercial reasoning to justify this influence, as the extraterritorial effects of the GDPR force many countries to comply with the European regulation as a requirement to receive data transfers from within EU member states and to consequently stay competitive in today's digital economy. But, beyond economic reasons, the adoption of European standards was also greatly based on social grounds, as specifically addressed in the rapporteur's report from the Federal Senate. That shouldn't be a surprise, as the GDPR is often regarded as a landmark privacy legislation when it comes to guaranteeing the subject's rights and information self-determination.

This is not, by any means, a new scenario. Nearly 120 countries have already enacted data protection laws, and most of them have some resemblance with the EU data protection legislation. This might happen not only because the GDPR is considered some kind of "gold standard" when it comes to data protection, but

46 Unlike many other countries, in Brazil's federal parliament every bill must be approved by both chambers.

47 The rapporteur's report might be accessed through (Portuguese only): https://www25.senado.leg.br/web/atividade/materias/-/materia/133486 [cited 2022-02-06].

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

also because most large corporations that operate within the EU already comply with the GDPR even when it is not applicable, as it was taken as a global business standard, and it is easier for companies to just apply the same standards everywhere they operate.[48]

Furthermore, as the proliferation of different privacy laws across the world that diverge too much from each other might also increase the operational costs of most big tech companies, they often lobby for countries outside the EU to also adopt the GDPR's "template", further collaborating for the standardization of privacy laws.[49] Even if there was no concrete evidence of this kind of lobby during the legislative process behind the LGPD, this hypothesis cannot be discarded, as lobbying activities are not regulated (although permitted) in Brazil, which makes them lack proper transparency, not to mention that they are often associated with a negative image.[50] Therefore, having stated that it is widely recognized that the LGPD got a strong inspiration from the GDPR, being a case in which EU models go beyond EU borders towards EU non-member states[51], now we shall analyze the main differences and similarities between both legal norms.

5 Assessing the GDPR elements within LGPD

The GDPR system is probably the most complete and advanced data protection legislation in the world.[52] Nonetheless, as already discussed, the LGPD is recent and has been directly influenced by the GDPR. Although LGPD and GDPR are quite similar in many aspects, there are also significant differences that directly impact their applicability. Both the GDPR and the LGPD are structured to correct information asymmetries between individuals and public entities or/and business corporations through legal and regulatory mechanisms capable of guaranteeing the effective exercise of informational autonomy.[53] The GDPR was also designed to promote the data protection equivalence among EU Member States and a secure environment for data flow in Europe.

48 BRADFORD, Anu, op. cit., p. 148.

49 Ibid., p. 149.

50 MIA-DE-VASCONCELOS, César Ricardo, CAVALCANTI-NOBREGA, Kleber and LACERDA-DE-PAULA, Gabriel. LOBBY AND INFLUENCE POWER FROM THE PUBLIC AGENTS. *Dimens.empres.* [online]. 2019, vol.17, no.4 [cited 2022-02-06], pp. 29–48. Available from: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-85632019000400029&lng=en&nrm=iso>. ISSN 1692-8563> Accessed: 09.03.2022.

51 FERREIRA, Christina, op. cit., loc. cit.

52 LORENZON NEVES, Lais. *Comparative Analysis between Personal Data Regulations in Brazil and the European Union (LGPD and GDPR) and their Respective Enforcement Instruments*, pp.5

53 PERES CAVALCANTE. Pedro. *Privacy and Personal Data Protection: A comparative analysis of the Brazilian and European regulatory frameworks*, pp. 24.

Both legislations are based on similar principles that influence data subjects' rights and legal obligations.[54] GDPR is based on principles that highlight the promotion of individual rights in provisions that were designed to deal with present and future digital situations. Article 5 of GDPR presents the following principles: (i) lawfulness, (ii) loyalty, (iii) transparency, (iv) purpose limitation, (v) data minimization, (vi) storage limitation, (vii) accuracy, (viii) integrity and (ix) confidentiality.[55]

The principles presented in LGPD are the following: (i) purpose, (ii) adequacy, (iii) necessity, (iv) free access, (v) quality of data, (vi) transparency, (vii) security, (viii) prevention, (ix) non-discrimination and (x) accountability.[56] LGPD

54 DE AGUILAR PEREIRA NEVE, Rebeca. *GDPR and LGPD: Comparative Study*. pp. 18.

55 See article 5 GDPR: "Personal data shall be: processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')."

56 See article 6 LGPD: "Activities of processing of personal data shall be done in good faith and be subject to the following principles: I – purpose: processing done for legitimate, specific and explicit purposes of which the data subject is informed, with no possibility of subsequent processing that is incompatible with these purposes; II – adequacy: compatibility of the processing with the purposes communicated to the data subject, in accordance with the context of the processing; III – necessity: limitation of the processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportional and non-excessive in relation to the purposes of the data processing; IV – free access: guarantee to the data subjects of facilitated and free of charge consultation about the form and duration of the processing, as well as about the integrity of their personal data; V – quality of the data: guarantee to the data subjects of the accuracy, clarity, relevancy and updating of the data, in accordance with the need and for achieving the purpose of the processing; VI – transparency: guarantee to the data subjects of clear, precise and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy; VII – security: use of technical and administrative measures which are able to protect personal data from unauthorized

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

is also based on the Brazilian Federal Constitution which established privacy as a fundamental right, as already mentioned,[57] and since its adoption it has been a milestone in data protection and privacy in Brazil. Furthermore, the statute established rights for data subjects and obligations to data Controllers and Processors.

Both the LGPD and the GDPR protect only the personal data of natural persons, excluding legal entities. Both legislations defined personal data as any information related to an identified or identifiable natural person, excluding from their scope the processing of anonymous data, unless the anonymization process can be reversed. The concept of personal data covers cookies, personal information, email address, IP address, browsing behaviour data, medical records, and biometric data, among others. Both laws also classify anonymous data as information that does not allow an identified natural person, however – differently from GDPR – LGPD sets that anonymous data can be classified as personal data in situations that it allows the data subjects' identification.

Both regulations are also applicable to businesses, public bodies, institutions, and non-profit organizations as data controllers and/or data processors.[58] Regarding the personal scope, there are small differences within the legal text itself, as the GDPR explicitly states that it is applicable to natural persons regardless to their nationality or place of residence, while LGPD does not clearly declare it. Even so, the LGPD can be interpreted in the same way as the GDPR through an integrated interpretation with the Brazilian Constitution.[59]

Considering the legal basis for data treatment, the LGPD establishes ten legal bases[60], while the GDPR provides only six.[61] Although some of them are similar, both legislations have differences in this regard as well. For example, LGPD allows processing of personal data for credit analyses (credit protection). In both

accesses and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination; VIII – prevention: adoption of measures to prevent the occurrence of damages due to the processing of personal data; IX – nondiscrimination: impossibility of carrying out the processing for unlawful or abusive discriminatory purposes; and X – accountability: demonstration, by the data processing agent, of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures."

57 BRAZIL. Constitution of the Federative Republic of Brazil 1988. Article 5: "*X – the privacy, private life, honor and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured; XII – the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts*."

58 Compare articles 3 and 4 GDPR with articles 1–5 LGPD.

59 BAPTISTA LUZ ADVOGADOS; ONETRUST DATAGUIDANCE (org.). *Comparing privacy laws: GDPR v. LGPD.* pp. 07.

60 See articles 7–13 LGPD.

61 See articles 5–10 GDPR.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

laws, the data processing must be based on one or more of the legal bases to be considered legitimate and lawful.[62]

Sensitive data is established in both LGPD and GDPR. Therefore, it is set that sensitive personal data is the information that allows us to make conclusions beyond data subject identification. The European and Brazilian legislators understood that the best way to protect them would be to bring clear examples of sensitive data – such as political opinions, racial origin, religious or philosophical beliefs, biometric, health-related data, others. Both legislations established that sensitive data should receive specific treatment.[63]

Under GDPR, the processing of sensitive data is more restrictive than in LGPD, since the Brazilian law sets that the consent of data subject for processing sensitive data should be specific, clear and for specific purposes. GDPR, on the other hand, expressly prohibits the processing of sensitive data, except for the purposes sets in Article 9 (1) and (2), such as when the data subject has given explicit consent to the processing of sensitive personal data for one or more specific purposes. To intensively protect data subjects' sensitive data, the GDPR is more restrictive for consent to process sensitive data, requiring that it must be freely given, explicit, unambiguous, informed and specific[64] – consent in LGPD is similar to the one present in GDPR.[65] Comparing both legislations, it is possible to establish some parallels between them – for example, a common concern regarding sensitive personal data related to health and protection of life. However, the GDPR provisions are not the same as those sets by LGPD, especially because GDPR is more extensive than the short statements presented by the Brazilian law.[66]

Regarding children's personal data, LGPD and GDPR present different regulations, being the GDPR more restrictive.[67] GDPR sets the minimum age of 16 years old for consent to process personal data – although EU Member States can set lower age, abiding by the minimum of 13 years of age. The parent or legal guardian consent must be given for processing children's data under 13 years of age in the EU. For its part, LGPD sets that the age for consent to be given is 13 to 18 years old[68] and the children's personal data process should be pursuing their

62 TEFFÉ, Chiara Spadaccini de and VIOLA, Mario. Processing of Personal Data according to LGPD: a Study about the Legal Basis. *Civilista.com (Revista Eletrônica de Direito Civil)*, vol. 9, no. 1, pp. 1–38.

63 Ibid., pp. 29.

64 MULHOLLAND SAMPAIO, Caitlin. *Sensitive Personal Data and The Protection of Fundamental Rights: An Analysis in Light of The General Data Protection Law (LAW 13.709/18)*.

65 Article 5 LGPD: "XII – consent: free, informed and unambiguous manifestation whereby the data subject agrees to her/his processing of personal data for a given purpose."

66 PERES CAVALCANTE. Pedro. *Privacy and Personal Data Protection: A comparative analysis of the Brazilian and European regulatory frameworks*. pp. 40

67 See Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75 GDPR

68 See article 14 LGPD.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

best interest. Brazilian legislation also states that parents or legal guardians must give specific and prominent consent for data processing in cases where children are under 13 years old. In addition, both legislations exclude from their scope the processing of anonymized data, although the LGPD sets that anonymized data can be considered personal when used to formulate behavioral profiles of an identified particular natural person.

It is important to note that both GDPR and LGPD set an obligation for data processors and data controllers to maintain a record of the processing activities under their responsibility, however, the LGPD is more general about it, while GDPR establishes in detail the information that needs to be recorded, as following for data controllers: (i) the name and contact details of the controller; (ii) the purposes of the processing; (iii) a description of the categories of data subjects and of the categories of personal data; (iv) the categories of recipients to whom the personal data will be disclosed; (v) international transfers of personal data, with the identification of third countries or international organizations, and the documentation of suitable safeguards adopted; (vi) the estimated time limits for erasure of the categories of data; and (vii) a general description of the technical and organizational security measures adopted. The data processors must record (i) the name and contact details of the processor; (ii) the categories of processing conducted on behalf of each controller; (iii) international transfers of personal data, with the identification of third countries or international organizations, and the documentation of suitable safeguards adopted; and (iv) a general description of the technical and organizational security measures adopted.[69] Under GDPR not all organizations must comply with article 30, meanwhile, LGPD sets that all organizations – regardless of their sizes, type or number of employees – must comply with the records processing obligations.

Both regulations set specific rights that may be exercised by the data subjects. The GDPR has established eight rights for the data subject[70], while LGPD has set nine main rights for the data subject.[71] Also, in both regulations data subject rights are similar For example, GDPR and LGPD set: (i) right of exclusion, data subjects can request the deletion of their personal information, except in exemptions provided for the two laws; (ii) access to information – based on the principle of transparency – the data subject can require to the data processor and/or data controller detailed information about the processing of their personal data; (iii) allow the holders of personal data to object to the processing of their data; (iv) recognize the data portability as a right of data subject; (v) others.

LGPD requires the data controller to carry out a data protection impact assessment (DPIA) to evaluate the risks of processing certain types of data. However, it does not set when DPIA is required and the Brazilian Data Protection

69 Ibid., pp. 27.

70 See articles 12–23 GDPR.

71 See article 18 LGPD.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

Authority (ANPD) is responsible for determining when such requirements are necessary. GDPR is more detailed about DPIA[72]. It establishes that a DPIA shall be conducted in specific circumstances and must contain safeguards to mitigate risks in the data processing. Also, when DPIA indicates that a certain data process represents a high risk – even if measures to mitigate it be taken into account – the controller must consult the supervisory authority prior to processing the data. Regarding the Data Protection Officer (DPO), LGPD requires the data controller to appoint a DPO, meanwhile, GDPR requires that both controllers and processors appoint a DPO, and – differently from LGPD – establishes when DPOs are not required.

Concerning data security, GDPR and LGPD are quite similar, as they include an obligation for controllers and processors to adopt security measures during the data process to protect personal data. GDPR requires the data controller to implement data security measures. LGPD determines that ANPD will issue guidelines about security measures, and GPPR sets the security requirements for data controllers and processors. Regarding data breaches, both data protection laws include an obligation to notify the supervisory authority as well as data subjects affected in certain circumstances. LGPD determines that ANPD and data subjects must be is informed in the event of a data breach, while GDPR requires the data controller to implement data security measures and to communicate with data protection authority within 72 hours after the data breach – in GDPR, not necessarily the data subjects will be informed of a data breach.[73] Furthermore, both laws established fines, sanctions, and civil lawsuits against data controllers and operators according to the type of event and severity of the data breach.

The LGPD is very similar to the GDPR in context, structure, purpose, and attitudes.[74] Therefore, both laws have: (i) several similar principles; (ii) broad concept of personal data; (iii) the need for any data processing to have a legal basis; (iv) exhaustive list of legal hypotheses for data processing; (v) detailed characterization of the data subjects' consent and concern about its manifestation; (vi) individuals' rights. The principles are the bases of data subjects' rights and the guidelines are ment to be observed in operations involving the processing of personal data by controllers and operators – even to public organizations. Also, both LGPD and GDPR set administrative and economic sanctions in case of non-compliance with legal requirements by processing agents.[75] It is evident, that the effect of GDPR goes beyond normative a dimension and has strong influence on the LGPD.

72 See articles 5, 24, 32–34 of recitals 74–77, 83–88 GDPR.

73 Ibid., pp. 35.

74 BIONI, Bruno Ricardo, MONTEIRO, Renato Leite, GOMES, Maria Cecília Oliveira. GDPR matchup: Brazil 's General Data Protection Law. 2018.

75 TEFFÉ, Chiara Spadaccini de and VIOLA, Mario. Processing of Personal Data according to LGPD: a Study about the Legal Basis. *Civilista.com (Revista Eletrônica de Direito Civil)*, vol. 9, no. 1, p. 38.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

6 Conclusion

This article analysed the EU GDPR as a source of Europeanization for the Brazilian General Data Protection Law (LGPD). There were two principal research questions dealt. First, "How much Europeanization is there in the Brazilian personal data regulation?" And second: "How was Europeanization conducted?". The answer to the first question was provided in the fourth chapter, which showed significant similarities in the context, structure and ultimate rational and at least six principal elements. These similarities are going beyond functional nature of the data protection and are purposefully present in the LGPD. This fact has been proven also in the answer on the second question.

Mapping origins of the Brazilian legislation, the EU influence was explicitly mentioned by the rapporteurs during the law-making process. Moreover, the adoption was also influenced by the pragmatic need to comply with EU rules in order to prevent negative economic impact stimulated by the absence of effective regulation (or by the enactment of a regulation supporting the divergence). In other words, the attractiveness of the EU market and the potential loss of EU companies created pressure for compliance. As a result, there is a strong influence of the GDPR on the LGPD, which may be shown in the comparative, historical or teleological interpretation.

Acknowledgment:

This article has been written with the generous support of the Institute for Czech-Brazilian Academic Cooperation (INBAC) and its high-level UNIGOU exchange program. Part of the research has been written under the grant scheme of Jean Monnet Network Project 611293-EPP-1-2019-1-CZ-EPPJMO-NETWORK "European Union and the Challenges of Modern Society (legal issues of digitalization, robotization, cyber security and prevention of hybrid threats" awarded in 2019 to the Faculty of Law, Palacký University in Olomouc.

List of references

ALBRECHT, Jan Philipp. How the GDPR will change the World. *European Data Protection Law Review*, 2016, vol. 2, no. 3, pp. 287–289.

ANDRAŠKO, Jozef, MESARČÍK, Matúš. Those Who Shall Be Identified: The Data Protection Aspects of the Legal Framework for Electronic Identification in the European Union. *TalTech Journal of European Studies*, 2020, vol. 10, no. 1., pp. 3–24.

BACHE, Ian. *Europeanization and Multilevel Governance*. New York: Rowman and Littlefield Publishers, 2008, 206 pp.

BAPTISTA LUZ ADVOGADOS; ONETRUST DATAGUIDANCE (org.). *Comparing privacy laws: GDPR v. LGPD.* [online] Available at: <https://baptistaluz.com.br/wp-content/uploads/2019/05/gdpr_v_lgpd_revised_edition-1.pdf> Accessed: 07.03.2022.

BHAIMIA, Sahar. The General Data Protection Regulation: the next generation of EU data protection law. *Legal Information Management*, 2018, vol. 18, pp. 21–28.

BIONI, Bruno Ricardo, MONTEIRO, Renato Leite, GOMES, Maria Cecília Oliveira. *GDPR matchup: Brazil's General Data Protection Law*. 2018. [online] Available at: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/#:~:text=The%20Brazilian%20General%20Data%20Protection,development%20of%20natural%20persons'%20personality> Accessed: 10.03.2022.

BOAVENTURA, Amorim Elisa, STEHLÍK, Václav. The Human Rights Protection in the EU-Brazil Relations: Structural Considerations and Current Legal Developments. *European Studies – The Review of European Law, Economics and Politics*, 2019, vol. 6, no. 1, pp. 141–156.

BOBEK, Michal. Europeanization of Public Law. In. BOGDANDY, Armin. et al. (eds.) *The Max Planck Handbook of Public Law in Europe. Vol. I: Ius Publicum Europeanum*. New York: Oxford University Press, 2016, p. 38.

BORNEMAN, John, FOWLER, Nick. Europeanization. *Annual Review of Anthropology*, 1997, vol. 26, pp. 487–514.

BÖRZEL, Tanja, RISSE, Thomas. When Europe Hits Home: Europeanization and Domestic Change. *European Integration online Papers*, 2000, vol. 4, no. 15, pp. 1–14.

BÖRZEL, Tanja. Towards Convergence in Europe? Institutional Adaptation to EUropeanization in Germany and Spain. *Journal of Common Market Studies*, 2002, vol. 39, no. 4, pp. 193–214.

BRADFORD, Anu. *The Brussels Effect: How the European Union Rules the World*. 1 Edition. New York: Oxford University Press, 2020, 404 pp.

BRAZIL. *Constitution of the Federative Republic of Brazil 1988.* [online] Available at: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/243334/Constitution_2013.pdf?sequence=11> Accessed: 07.03.2022.

BRAZIL. Law n.º 12.414/11. [online]. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm> Accessed: 07.03.2022.

BRAZIL. Law n.º 12.414/11. [online]. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Accessed: 07.03.2022.

BULMER, Simon, BURCH, Martin (1998) Organizing for Europe: Whitehall, the British State and the European Union. *Public Administration*, vol. 76, no. 1, pp. 601–628.

CADWALLADR, Carole, GRAHAM-HARRISON, Emma. (2018, Mar 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian* [online]. Available at: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> Accessed: 07.03.2022.

DANČÁK, Břetislav, FIALA, Petr, HLOUŠEK, Vít. Evropeizace: pojem a jeho konceptualizace. In. DANČÁK, Břetislav, FIALA, Petr, HLOUŠEK, Vít (eds.). *Evropeizace. Nové Téma politologického výzkumu*. Brno: IIPS, pp. 11–25.

DAVIES, Simon. The Data Protection Regulation: A triumph of pragmatism over principle? *European Data Protection Law Review*, 2016, vol. 2, no. 3, pp. 290–296.

DE AGUILAR PEREIRA NEVE, Rebeca. *GDPR and LGPD: Comparative Study*. UNICEUB Repository. [online]. Available at: <https://repositorio.uniceub.br/jspui/bitstream/prefix/15239/1/Rebeca%20Neves%2021750900.pdf> Accessed: 07.03.2022.

European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2018.

EUROPEAN UNION. Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012, pp. 47–390.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

EUROPEAN UNION. Directive (EU) 2016/680 of the European Parliament and of the Council of 26 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the reduction of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

EUROPEAN UNION. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).

EUROPEAN UNION. *Charter of Fundamental Rights of the European Union. Official Journal of the European Union C83*. Vol. 53. Brussels: European Union, 2010.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

EUROPEAN UNION. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (Text with EEA relevance).

FALALIEIEVA, Liudmyla. Modern Approaches to the Extraterritorial application of the EU law. *European Studies – The Review of European Law, Economics and Politics*, 2014, vol. 1, no. 1, pp. 103–110.

GODDARD, Michelle. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 2017, vol. 59, no. 6, pp. 703–705.

GOMBOS, Katalin. Europeanisation effects in the court jurisprudence. *International and Comparative Law Review*, 2019, vol. 19, no. 1, pp. 261–275.

KOCHARYAN, Hovsep, VARDANYAN, Luisine, HAMUĽÁK, Ondrej and KERIKMÄE. Critical Views on the Right to Be Forgotten After the Entry Into Force of the GDPR: Is it Able to Effectively Ensure Our Privacy? *International and Comparative Law Review*, 2014, vol. 14, no. 2, pp. 96–115.

KOKOTT, Juliane; SOBOTTA, Christoph. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 2013, vol. 3, no. 4, pp. 222–228.

LORENZON NEVES, Lais. *Comparative Analysis between Personal Data Regulations in Brazil and the European Union (LGPD and GDPR) and their Respective Enforcement Instruments*. vol. 1 (2021). [online]. Available at: <https://bibliotecadigital.fgv.br/ojs/index.php/rpdue/article/view/83423/79192> Accessed: 09.03.2022. (Portuguese only).

MIA-DE-VASCONCELOS, César Ricardo, CAVALCANTI-NOBREGA, Kleber and LACERDA-DE-PAULA, Gabriel. LOBBY AND INFLUENCE POWER FROM THE PUBLIC AGENTS. *Dimens.empres.* [online]. 2019, vol.17, no.4 [cited 2022-02-06], pp. 29–48. Available from: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-85632019000400029&lng=en&nrm=iso>. ISSN 1692-8563> Accessed: 09.03.2022.

MULHOLLAND SAMPAIO, Caitlin. *Sensitive Personal Data and The Protection of Fundamental Rights: An Analysis in Light of The General Data Protection Law (LAW 13.709/18)*. [online]. Available at: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf> Accessed: 09.03.2022.

NYE, Joseph. *Soft Power: The Means to Success in the World Politics*. New York: Public Affairs 2004, 191 pp.

OLSEN, Johan P. The Many Faces of Europeanization. *Journal of Common Market Studies*, 2002, vol. 40, no. 5, pp. 921–952.

PAVELEK, Ondřej, ZAJÍČKOVÁ, Drahomíra. Personal Data Protection in the Decision-Making of the CJEU Before and After the Lisbon Treaty. *TalTech Journal of European Studies*, 2020, vol. 10, no. 1, pp. 167–188.

PERES CAVALCANTE. Pedro. *Privacy and Personal Data Protection: A comparative analysis of the Brazilian and European regulatory frameworks*. [online]. Available at: <https://repositorio.ufpe.br/bitstream/123456789/34357/5/Monografia_PRIVACIDADE%20E%20PROTE%c3%87%c3%83O%20DE%20DADOS%20PESSOAIS%20-%20Uma%20an%c3%a1lise%20comparativa%20dos%20quadros%20regulat%c3%b3rios%20brasileiro%20e%20europeu%20FINAL.pdf> Accessed: 07.03.2022 (Portuguese only).

RADAELLI, Claudio M. Europeaniation: Solution or problem? *European integration online Papers*, 2004, vol. 8, no. 16, pp. 1–26.

RYNGAERT, Cedric, TAYLOR, Mistale. The GDPR as Global Data Protection Regulation? 2020, *AJIL Unbound*, vol. 114, pp. 5–9.

SAFARI, Beata, A. Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard For Personal Data Protection. *Seton Hall Law Review*, 2017, vol. 47, no. 3, pp. 809–848.

SHABANI, Mahsa, BORRY, Pascal. Rules for processing genetic data for research purposes under the new EU General Data Protection Regulation. *European Journal of Human Genetics*, 2018, vol. 26, pp. 149–156.

SHARMA, Sanjay. *Data Privacy and GDPR Handbook*. Hoboken: Wiley, 2020, 480 pp.

SCHIMMELFENNING, Frank. Europeanization beyond Europe. *Living Reviews in European Governance*, 2012, vol. 7, no. 1, pp. 5–27.

TEFFÉ, Chiara Spadaccini de and VIOLA, Mario. Processing of Personal Data according to LGPD: a Study about the Legal Basis. *Civilista.com (Revista Eletrônica de Direito Civil)*, vol. 9, no. 1, pp. 1–38.

VARDANYAN, Lusine, KOCHARYAN, Hovsep. The GDPR and the DGA Proposal: are They in Controversial Relationship? European Studies. *The Review of European law, Economics and Politics*, 2022, vol. 9, pp. 91–109.

VEČEŘA, Miloš. The process of Europeanization of law in the context of Czech law. *Acta univ. gric. et. silvic. Mendel. Brun.*, vol. LX, no. 2, pp. 459–464.

Published by Palacký University Olomouc, Czech Republic, 2022.
ISSN (print): 1213-8770; ISSN (online): 2464-6601