Panor. Braz. law - Year 6 -Numbers 9 and 10 - 2018 - pp. 82 - 100.
ISSN 1075-1343 (print)
ISSN 2318-1516 (online)
DOI: http://dx.doi.org/10.17768/pbl.y6.n9-10.p82-100

PRIVACY AND DATA PROTECTION - FROM EUROPE TO BRAZIL

Christian Perrone

Ph.D. Candidate and Fulbright Scholar. LL.M. Cambridge University (UK); Diploma EUI on International Human Rights. Former Secretary for the Inter-American Juridical Committee (OAS) and Human Rights Specialist at the Inter-American Commission on Human Rights. Currently Public Policy Consultant, specialized in International Law and crossborder data-protection.

Sabrina Strassburger

Ph.D. in Legal Studies Bocconi University Milan; Post graduate Studies - International Trade, Instituto Universitario di Studi Europei. Currently Legal Counsel for Fiat Chrysler Automobile (Italy), specialized in data protection and European cross border issues.

Received: 2018-11-12. Accepted:2019-06-21

Abstract: The European General Data Protection Regulation ("GDPR") has entered into force in May 2018. It is the result of many years of debate on how to update privacy and data protection normative within the States members if the union. The discussion that lead to its adoption has served as a platform for legislation reform across the globe. Brazil was not immune to it. This papers uses comparative side-by-side analysis to understand how similar or dissimilar the recently approved General Data Protection Law (Lei Geral de Proteção de Dados Pessoais - "LGDP") is to its European counterpart. Systematically the paper is divided in two parts: one exposing the GDPR and another underscoring it to the LGDP. The six main axes used are: a) criteria in order to lawfully collect and process data; b) its major principles; c) obligations for the companies of having privacy by design and by default; d) data protection authorities; e) possible sanctions for breaches; and f) extraterritoriality of their application. It concludes that the Brazilian regulation has only minor differences from its system across the Atlantic and may even be said to be a "GDPR à la Brasileira".

Keyword: GDRP - LGDP - Data Protection - Privacy

I. THE GDPR AS A TEMPLATE FOR BRASIL

The European model of data protection is certainly considered as one of the most advanced in the field.[1] It entered into force in May 2018. It substituted a regime of more than 20 years based on the European Union Directive 95/46/EC.

The framework in Europe has at its core the fundamental rights of intimacy, privacy and private live, and the protection of data. They are enshrined in the Convention 108, European Convention on Human Rights and the Human Rights Charter of the European Union. All this creates a cluster of rights that need to be protected by the States within the European Union.

The GDPR is the next level in this field. As a EU Regulation, it acts as a general piece of legislation with direct effect on the whole European legal environment. Envisioning data as a transborder matter, these rules go beyond the European space and provide for a continuous protection even beyond the territorial limits of the EU. In other words, they are designed to have extraterritorial effect.

It is in this context that Brazil has drafted its new General Data Protection Legislation ("LGPD" in its original acronym). This legislation has benefited from the many years of discussion on the matter in Europe and in many countries around the world, including Latin America.[2] To a certain extent, the GDPR ended up as a basis for the Brazilian legislation recently approved.

The LGPD recognizes as well that privacy and data protection are a matter of fundamental rights. It also acts as a general regulation for the field. Furthermore, it extends the protection of data collected in Brazil to storing and processing outside the country.

The present article intends to present the Brazilian legislation through the lenses of the GDPR. In this sense, it will be divided in two parts: i) the GDPR exposed and ii) the LGDP compared. Both parts will cover 6 relevant axes: a) criteria in order to lawfully collect and process data; b) its major principles; c) obligations for the companies of having privacy by design and by default; d) data protection authorities; e) possible sanctions for breaches; and f) extraterritoriality of their application.

1 DE HERT, P., & PAPAKONSTANTINOU, V. The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. In.: Computer Law & Security Review , 28, 130-142, 2012.

2 CARSON, Angelique. Consent Is King in Latin America: Navigating the Eight Existing DPAs with a Look to the Future. Available at: https://iapp.org/news/a/2013-06-03-consent-is-king-in-latin-america-navigating-the-eight-existing/

The logic of the paper is to explore the extent of which the Brazilian legislation is similar and at the same time relatively different from its European sister. As a matter of conclusion we will state that the LGPD can be seen as GDPR with a Brazilian flavor.

II. REGULATION IN THE EUROPEAN UNION (GDPR)

The new General Data Protection Regulation ('GDPR')[3] sets the processing of personal data relating to individuals in the European Union. When an individual, a company or an organization intends to process personal data in connection to a professional or commercial activity - for business purposes, socio-cultural or financial activities for example - then the GDPR has to be respected. As a EU Regulation, it is distinguished from the previous data protection Directive: EU Regulations are legal acts of the European Union that become immediately enforceable as law in all Member States at the same time, while Directives, in principle, need to be enacted into domestic law[4].

Personal data is defined broadly by the GDPR as "any information" relating to an "identified or identifiable natural person" and the natural persons under this protection are referred to as "data subjects". EU data protection laws uses the term "data controller" to define the entities that determine how and why data is processed and the term "data processors" referring to entities that process personal data on behalf of a data controller. As an example, the data controller could be a car manufacturer that uses its customers personal data to offer car parts, accessories and after-sales services whereas the data processor could be the third party vendors processing personal data on behalf of the car manufacturer.

The GDPR aims to protect all EU citizens[5] from having its personal or even sensitive information released to an untrusted environment and in that regard, it establishes how data controllers and data processors should perform activities such as collection, recording, storage, use, disclosure, erasure of data subjects personal data.

2.1 Art. 6 - Consent and other lawful means of acquiring and processing personal data:

3 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. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679 Consulted on November 1, 2018.

4 FOLSOM, Ralph H., LAKE Ralph B., NANDA, Ved P. European Union Law After Maastricht: A Practical Guide For Lawyers Outside the Common Market. The Hague: Kluwer. 2012, p. 5.

5 Its scope of protection encompass as well all residents of the EU.

The main rule, since the beginning of EU personal data protection normative, concerns the fact that individuals must give consent to the processing of their personal data for one or more specific purposes. As a practical matter, whenever an individual provides its personal data for a certain purpose such as opening a bank account, filling for a job application, buying clothes online or attending a doctor's appointment, the data subject must be informed about the purposes for the collection of its personal data and after, he or she must as well provide specific consent in relation to that data processing. In most cases, it means to sign a document authorizing the data to be processed for those pre-determined informed purposes or opt-in by ticking a box expressing consent on a website.

Nevertheless, consent is not the only lawful basis established by Art. 6. Potentially, the same amount of personal data is collected on the grounds of "legitimate interests" of the controller or on grounds that the data was "necessary to fulfill a contract" entered into by the data subject.[6]

Art. 6 of the GDPR establishes data processing should be lawful in one of the following cases: (a) after the data subject's consent; (b) for the performance of a contract; (c) to comply with legal obligations of the data controller; (d) to protect the vital interests of the data subject; (e) when is necessary for the public interest or the exercise of official authority; (f) when is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2.2. Principles of protection:

One of the GDPR's objectives is to provide individuals with a stronger control on their personal data, with the aim to help restore consumers' trust in the digital economy. To pursue this objective, the new Regulation renewed some of the principles set out by Directive 95/46/EC and brought up some new ones, reinforcing data subjects rights in relation to their own data.[7]

The list of key principles in the GDPR's Article 5 is more detailed than the previous Directive. The GDPR principles begin by determining that the information should be: (a) "processed lawfully, fairly and in

6 EDWARDS, Lilian, VEALE, Michael. Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. 16 Duke L. & Tech. Rev. 18. December 4, 2017. P. 32.

7 POST, Robert C. Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. 67 Duke Law Journal. February 2018.

a transparent. manner" (lawfulness, fairness, and transparency); the information should also be (b) "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (purpose limitation). The GDPR Principles continue with requirements of (c) data minimization; (d) data accuracy; (e) limited storage; (f) integrity and last is the accountability for the data controller.[8]

2.3 Privacy by Design and Privacy by Default:

Prior to the GDPR, compliance with personal data protection laws consisted on the creation of policies, structuring of contractual terms, requesting of authorizations, auditing systems and processes, etc. The GDPR introduced new requirements by asking organizations to take one step further and develop products taking privacy already into consideration. This will require a closer collaboration from different departments within an organization in order to develop policies, procedures and systems simultaneously with product development, all bearing in mind GDPR compliance. This concept is what is known as "privacy by design or privacy by default"[9]

Privacy by design means building systems and infrastructure with privacy at its core, fostering personal data protection and having in mind its principles before and during the system creation and construction. The concept of privacy by design already existed but the provisions of Article 25 of the GDPR are a novelty in terms of legislative requirement. These provisions do not give individuals rights, but try "to provide a societal framework for better privacy practices"[10].

2.4. The Data-privacy authorities:

The GDPR establishes that each EU Member State shall create internally a supervisory authority: a public institution which will act independently on monitoring and enforcing the application of the GDPR. Article 57 of the GDPR determines the tasks each supervisory authority shall develop on its territory, which includes: the promotion of public awareness and understanding of data processing risks and rules, advising

8 SCHWARTZ, Paul M., PEIFER, Karl-Nikolaus. Transatlantic Data Privacy Law. 106 Geo. L.Journal. November 2017.

9 PETERSEN, Kyle. GDPR: What (and why) you need to know about EU data protection law. 31 Utah Bar Journal. July/August, 2018.

10 EDWARDS, Lilian, VEALE, Michael. Slave to the algorithm? why a 'right to an explanation' is probably not the remedy you are looking for. 16 Duke L. & Tech. Rev. 18. December 4, 2017. P. 23.

other national institutions with regard to data processing, promoting the awareness of controllers and processors of their obligations under the GDPR, providing information to and handling complaints lodged by data subjects concerning the exercise of their privacy rights, conducting investigations on the application of the Regulation, giving advice, encouraging the creation of codes of conduct and the establishment of data protection certification mechanisms, among others.

One important prerequisite assigned to the data-privacy authority concerns data breaches: in case of a personal data breach, data controllers have the obligation to notify the supervisory authority "without undue delay". Such notification to the data-privacy authority should contain the description of the nature of the breach, the numbers of data subjects and personal data records involved and its likely consequences (whenever possible), the description of the measures taken or to be taken to address or reduce the impact of the breach, documenting all the breaches in order to allow the supervisory authority to verify compliance[11].

Each EU member country has its own supervisory authority and in trans-border data-breaches, for example, they should collaborate and work together. With the GDPR the supervisory authority is no longer required to approve each single data processing agreement or data transfer based on the Model Contract Clauses, however, data controllers have to follow internal record keeping requirements and appoint a Data Protection Officer ("DPO") whenever its operations require monitoring data subjects on a large scale or use of sensitive data. Data controllers have a great amount of work (in terms of data transfer agreements, technical measures related documentation, security measures, among others) that needs to be done in order to comply with the GDPR requirements in that regard.

2.5. Sanctions:

Infringement of this new data-protection regulation can be extremely expensive: administrative fines can reach up to 20 million euros or, in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is greater.

Those penalties are applicable to both controllers and processors which means that cloud services are also subject to GDPR enforcement.

Data protection authorities of each member state have the prerogative to carry out investigations, determine when entities have to undertake remedial measures for deficiencies and last but not least, to

11 VOSS, W. Gregory. Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation. 50 R.J.T. 783, 2016.

impose those administrative fines.[12]

2.6. Extraterritorial application

The territorial scope of EU data protection laws has been increased with the GDPR as the jurisdiction has been extended to be applicable to companies processing personal data of individuals residing in the European Union no matter where the company is actually located. With the past data protection laws, this matter was unclear and the topic has been discussed in court several times; now with the GDPR, this subject has been clarified.

It is the Article 3 of the Regulation that makes its applicability clear: it is applicable to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR is also applicable to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU.

If a company outside the EU is reached by the GDPR's extraterritorial application, an European representative has to be designated to serve as a contact point for EU regulators and consumers. This representative can be a natural or legal person established in any EU country where one of its data subjects reside. Such representative must have access to all the company documentation related to GDPR compliance and in case of failure to comply with the GDPR rules, the European representative may also be subject to enforcement proceedings[13].

III) THE GENERAL DATA PROTECTION LAW IN BRASIL

The LGPD (Brazilian General Data Protection Law) intends to have a similar effect as the GDPR. It was drafted to have a wide scope on and off line, even if on such matters what first comes to mind is social media and data breaches. Furthermore, it aims at data collected and or held by both private and public sectors. The logic is to have a unified system in order to move beyond the sectorial specific regulations of today.

To have an idea, the LGPD touches upon at least 40 different

12 FACCIPONTI, Joseph P., MCGRAIL, Katherine. GDPR Is Here — What If You Didn't Prepare? Law 360. May 24, 2018.

13 FRANCKE, Glory. Time To Update Your Privacy Statement For GDPR. Law 360, September 26, 2017.

pieces of regulation scattered throughout different areas such as the health sector, the banking system and consumer protection.[14] The LGPD is not suppose to dispose of these laws and regulations, it seeks to held them together and provide a common framework.[15]

3.1. Consent and other lawful means of acquiring and processing personal data:

"Consent is king."[16] For long the logic of collecting and processing personal data was focused on consent. It was seen as being a formal key or a substancial necessary criteria. Behind it, there is a contactual rationale. Private data is an individual property and can be contracted; hence, the necessity of an agreement on the collection and processing of such information.

The US, for instance, has maintained from its inception a "notice and consent" approach.[17] It is focused on disclosures made through "privacy policies". These are statements disclosing what data is to be collected and how it will be treated. Individuals, then, have the choice to opt for the service under such conditions or not.

In Europe, as we have seen above, the system maintained a focus on consent but moved beyond it. The individual assent to have his or her personal data collected is seen as an insufficient criteria. On the one hand, it is necessary to be freely given, informed and specific. This creates a strong burden for companies to comply with. On the other hand, big data and many other positive usages of data might not be compatible alone with such a framework. The lawful means for processing information have concentrated in the mentioned six main basis present in art. 6 of the GDPR.

The LGPD has followed a similar path, rejecting the more broad US system. The Brazilian legislation (in art. 7) has included not only the six GDPR basis: (a) consent; (b) necessary for the performance of a contract; (c) necessary for compliance with a legal obligation;

14 For an overall proposal of how the framework acted, see: http://baptistaluz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf.

15 Such a situation may create unexpected opposition. During the Presidential Assent there were claims that the law should leave space for some exceptions related to national security, banking and a few others. Failing to have that, the President should vetoed certain parts of it. It would have killed the unifying principle that inspired the legislation in the first place.

16 It has become a common frase to describe the relevance of consent to the data-protection field.

17 SLOAN, R. H. and WARNER R. Beyond Notice and Choice: Privacy, Norms, and Consent. In.: Suffolk University Journal of High Technology Law, No.: 2013-16, 12 Apr 2013. Available at SSRN: https://ssrn.com/abstract=2239099.

(d) necessary for the protection of vital interests; (e) implementation of public policies by the public administration; (f) legitimate interest. But also, four more: (g) research by public study entities; (h) exercise of rights in legal proceedings; (i) health protection; (j) protection to credit. Perhaps the last two are the most important addition. They might be subsumed under other headings but it is relevant that they were explicitly mentioned.

Some authors have pointed out the presente of the aforementioned specific criteria may be the result of discussions of other relevant domestic legislations. This may be actually true. There has been a debate on the Positive Credit History Law (Lei do Cadastro Positivo - Lei N. 12.414/2011).[18] Besides, there is also a relevant tradition of protection of how doctors regulate their own procedures. The federal doctor's board (Conselho Federal de Medicina) has been the focal point in determining institutional health-related practices, including personal data.

- Consent

One consequence for opting for a more European as opposed to an American approach is that consent has to be understood in a much more robust way. Both the EU and Brazilian legislations are in consonance that it is necessary for the individual to be substantially informed and be able to freely consent. The burden is allocated within the person or company seeking to collect and process the data.

One difference, however, might be seen in how consent has to be established for international transborder transfers. Art. 49(1) of the GDPR mentions "explicit consent". Art. 33, VII, of the LGPD states that they may occur when "specific and highlighted consent" is provided. The difference in the language of the two may have on privacy policies (and perhaps contracts) are designed and brought before individuals.[19]

- Legitimate interests

This is an addition to the Brazilian legal framework. It is a regulation that has an open texture aiming at providing some degree of flexibility to the strict adherence to consent. As mentioned above, it

18 ARRUDA, D. S. and FRANCO, P. Nova lei do cadastro positivo beneficia consumidor?Porque nem tudo que reluz é ouro. In.: Jota, January 12, 2018. Available at: https://www.jota.info/opiniao-e-analise/artigos/nova-lei-do-cadastro-positivo-beneficia-consumidor-12012018.

19 It is also a slight departure from the language in other Latin American countries and what experts have seen as a hindrance to the flow of data. See: CARSON, Angelique. Consent Is King in Latin America: Navigating the Eight Existing DPAs with a Look to the Future. Available at: https://iapp.org/news/a/2013-06-03-consent-is-king-in-latin-america-navigating-the-eight-existing/.

provides a lawful basis for the usage of data for beneficial purposes and allows for big data processing, artificial intelligence and other forms of processing that may need large data-sets.

Due to its open-texture, the outer limits of what means legitimate interests will depend very much on its interpretation. This means a legal risk for any company processing data under such basis. It is necessary to document what the interests are and to conduct a balancing exercise between the "necessity of processing on the legitimate interests of the data controller and the rights and interests of the "data subjects".[20]

3.2. Principles, rights and duties:

The LGPD follows the example of the GDPR. It establishes a series of principles under which the whole system of privacy and data protection has to be analyzed. This may have its origin in fact that both pieces of legislation are to be understood as providing more concretude for fundamental rights. It is as well a normative methodology that allows for flexibility; particularly necessary in dealing with a fast paced and constant changing field.

The main lines in both regulations are similar: purpose of the collection and processing; adequacy and compatibility (between collection and processing); limitation and minimization of data collection; processing and storage; transparency; non-discrimination; and accountability.

In the US, there are certain obligations for minimization and to a certain extent a high degree of transparency. The latter guaranteed by "privacy policy" disclosures. These are enforced mostly by the Federal Trade Commission (FTC) mandate to police unfair and deceptive practices.[21]

The LGPD has chosen to establish a series of general obligations for data processing and rights to data subjects, similarly as the GDPR. The bedrock is found in purpose, adequacy and limitation. The logic is that collection, processing as storage has to be limited to the needs and purposes of the activity. An assessment has to be made as to why the data is collected and whether it is necessary. If does not have a purpose, it should not be collected in the first place, and if it was, it should not be stored. On the other hand, if it had a purpose, the processing has to de adequate and compatible.

Limitation means not only in quantity (how much and which data it to be collected). It should be understood as well within a time framework. When the purpose is finished and it is not to fulfill another

20 This proportionality exercise follows from the language of art. 7, IX, of the LGPD.

21 For an overall view, see: SOLOVE, D. and HARTZOG, W. The FTC and the New Common Law of Privacy. In.: Columbia Law Review, vol. 114, 2014, 583.

one, should be eliminated. The mentality of data storage in default has to be changed for one of data management.[22]

Right of portability:

Among the rights established in the Brazilian legislation is the right of portability. Every individual has a right to request the data controller to transfer his or her personal data to another controller. The right is not in and on itself new. However, they were not general rights. Resolution 460/07 from ANATEL (Brazilian Telecommunications Regulatory Agency) allows for the portability of certain telecom data sets from one telecom company to the other. In the banking system there is as well a certain possibility to transfer certain data sets from one bank to another.[23]

The novelty in the LGPD is the fact that it creates a general right. Data Controllers are mandated to create procedure to transfer data to other controllers, presumably the provides the same or similar service.

Right of review of automated decisions:

Automated decision-making services have become more widely available and with it the risks. The GDPR establishes a right to a "human review". In other words, people may not be subject solely to an automated decision-making system. There has to be an option to review by a human person with the criteria for the decision available.

The Brazilian system has already had similar right, however, they applied to a very narrow field, credit scoring. The Positive Credit History Law (Lei do Cadastro Positivo - Lei N. 12.414/2011) provides for a right of an "explanation" of the criteria for processing and the mechanisms used by the algorithm.[24] This system was translated to the LGPD with the addition that it is applicable to all data-processing.

Some authors are of the opinion that the LGPD has a broader scope are relatively more protective than the GDPR. They understood that in the Brazilian system, "the impact on the data subject is presumed when automated decision making is based on profiling, and there is no limitation to situations when the data was provided by consent."[25]

Notification:

22 MAYER-SCHÖNBERGER, V. Delete: The Virtues of Forgetting in the Digital Age. Princeton, 2011.

23 More information one can find in the Central Bank website: https://www.bcb.gov.br/pre/bc_atende/port/portabilidade.asp.

24 Some aspects of the procedure may be excluded such as trade secrets and protected intellectual property rights.

25 BIONI, B.; OLIVEIRA GOMES, M. C. and MONTEIRO, R. L. GDPR matchup: Brazil's General Data Protection Law. IAPP, October 4, 2018. Available at: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/.

Data breaches have become more common. Cyber security has risen to a very important preoccupation. Consonant with logic of both instruments, they have provisions that make the individuals aware of breaches to their personal data. The definition of a data breach and of which data is considered personal have an important impact on how many notifications does a company have to send, to whom and due to what.

The LGPD circumscribes the breaches to those that may create risks or relevant damage to data subjects (art. 48, caput LGPD). Other pieces of legislation only create rights of receiving notification to data subjects in very specific cases. In most US states that do have statutes on the matter, a data subject only has a right to a notification when the data involves his or her name.[26]

The Brazilian and European systems converge in that data subjects do have general notification rights and that data-protection authorities have to be notified. The amount of time after the breach occurred that it must happen in the Brazilian legislation is not set. It only states that it must be within a reasonable amount of time and that it will be defined by the data-protection authority (art. 48, para. 1, LGPD).

Right to a compensation:

Art. 42 and following provide a liability regime and the means to find compensation to damages occurred as a result of carrying out the activity of processing personal data. This is similar to the European system that adopted a logic that damages have to be compensated.

It commands a standard of analysis that seems to be different from the one in the United States, for instance. In the latter constitutionally in other to have standing in Court - and have access to remedies such as compensation - the plaintiff has to show "concrete damage", known as well as injury-in-fact.[27]

The language of the European and Brazilian legislations should lead to a different analysis, particularly relating to moral damages. It mandates actual/effective indemnification. It also establishes it as a joint obligation for the chain of data processing. The controller, however, receives the main brunt of obligation.

3.3. Privacy by Design and by Default:

26 See for instance: California Security Breach Notification Statute - Cal. Civ. Code §§ 1798.29, 1798.82; and Michigan Security Breach Notification Statute - Mich. Comp. Laws §§ 445.63, 445.72.

27 In light of the Spokeo Case, it seems that it is not very easy to establish the connection between a breach in data security and a specific damage. (Spokeo, Inc. v. Robins, U.S. Supreme Court, 2016).

Privacy by design and by default, as we have seen, intend to regulate all fases in the development of a new product or service. Even early stages, planing of products and services have to include a concern for data protection and individual privacy. This pre-launching regulation is a novel concept for the Brazilian regulatory environment.

We can draw parallels to environment and health concerns. In all of them there is a need to assess the impact an activity and or a product may have vis-à-vis a relevant value, a clean environment, population's health and now privacy and data protection.

However, for the latter, it goes beyond what may accidentally happen or a normal result of the action. The activity - service or product - has to be by default designed to protect individual's privacy and data. It is not enough to have contention plans. These only have an ex post facto effect. While, the law commands a proactive approach.[28]

The two concepts have a direct link with the principles established in the legislation. The most obvious are security, prevention and accountability (art. 6 VII, VIII and X, LGPD). However, in order to guarantee purpose, suitability/adequacy and necessity (art. 6 I, II and III, LGPD), for instance, the procedures for collection and treatment of data have to be assessed and designed ab initio having privacy in mind.

The Brazilian legislation, as much as the European one, has an important emphasis on ex ante instruments such as licenses and processing documentation.[29] It goes as far as mandating data processing impact assessments (DPIAs).[30] These are not mandatory for every specific data processing activity, however, they may be requested even from the public sector (art. 32, LGPD).

Their methodology and specifics are not specified. They were left for the data protection agency to develop through secondary legislation. As we will see, with the Presidential veto to the portion of the statute that contained the provisions of a Brazilian data protection agency, the

28 Vide: GELLERT, R. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. International Data Privacy Law , 5, 3-20, 2015; SPINA, A. A Regulatory Mariage de Figaro: risk regulation, data protection, and data ethics. European Journal of Risk Regulation , 8, 88-94, 2017.

29 For the relationship between a risk approach and ex ante documents see: ZANNATA, R. Proteção de Dados Pessoais como Regulação de Risco: uma nova moldura teórica? In.: Artigos Selecionados Rede de Pesquisa em Governança da Internet, 2017. Available at: https://www.researchgate.net/publication/322804864_Protecao_de_dados_pessoais_como_regulacao_do_risco_uma_nova_moldura_teorica.

30 See for instance, art. 10 para. 3: "The national authority may request of the controller an impact report on protection of personal data, when processing is based on her legitimate interest, being observed commercial and industrial secrecy." (Unofficial translation based on several unofficial translations available online. Just to mention one: https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf).

standards to be followed tend to be in the air.

Due to the similarities between the two norms, it is safe to say that following the European model should not be far fetch from the needs of the Brazilian standards. It is safe to say that in the future, when eventually a Brazilian data protection agency is established, the assessments will have to adapt to its normative cannons. Any data controller and processor should be aware of such needs.

3.4. Data-Privacy Authority - Presidential veto:

Another important feature similar to both systems is a central data-protection authority (DPA). As seen above, the EU system establishes a domestic data-protection and a European data-protection system. Each national DPA serves as a nerve point, focusing data-protection regulation and oversight in one administrative body.

This tends to facilitate the process for data-processing organizations. They have to respond to one organ. This does not eliminate completely the sectoral specific regulation, nor the level of protection from individuals in every particular country. Banking authorities, for instance, are able to regulate data-flows and issue specific norms. However, the framework of analysis has to be under the overarching rules in the general data protection regulation.

The regulatory strategy is based on a dialogue between the country DPA and the data-controller (entity controlling the processing activity). The LGPD was drafted so that there is a DPA (a governmental agency) in charged with regulatory and oversight powers (arts. 55 and ff).[31] It has an extensive impact in how the regulation should work. Excluding its specific mandated clauses, the authority is mentioned 49 times in the whole legislation.

It is certainly seen as part of the basis of the legislation. Again, in view of the open texture and the many regulatory procedures ex ante and ex post present in the regulation, the agency has a fundamental role to play. It will set the standards and clarify substantially the rigor of the privacy demands.

As the LGPD sought presidential approval, there were doubts about the constitutional statute of the legislation as it stands.[32] It has

31 For the history of the provision: Artigo 19. Proteção de dados pessoais no Brasil. Análise dos projetos de lei em tramitação no Congresso Nacional. November, 2016; and Internet Lab. O que está em jogo no debate sobre proteção de dados pessoais no Brasil? 2016. Available at: http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf and http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf.

32 The main argument was that the initiative of any legislation that intends to

lead to a presidential veto to some provisions, including the ones that establish the Brazilian data-protection authority (arts. 55 ff). It is expected that a new piece of legislation is proposed by the Executive in order to establish the authority. The form of proposition (through a new bill or a presidential decree - medida provisória) is up for debate.

This creates as well a possibility to reanalyze the structure of the agency and what are its main componentes. The original proposition stroke a balance between the many sectors involved and provided for an independent agency subject to the direct supervision of no other body.[33] Up until this moment, the proposal was not present to Congress and we cannot state that it will follow the same form. As understood from the EU model, it is important to guarantee that the authority is formally and substantially independent and has the authority to regulate the national data-protection policy.

3.5. Administrative Sanctions:

The Brazilian DPA, as per the approved legislation, no matter its format, will have the capacity to impose administrative sanctions. As the data-protection bill was proposed in 2011, it contained fines of up to 20% of the companies annual turnover. After the consultation period, the legislators found it proper to reformulate the sanctions system.

As much as the GDPR, it is as well an escalated system. It starts with a warning and ends with a fine of up to two percent (2%) of revenues in Brazil, capped to a maximum of fifty million reais (R$ 50,000,000.00) per infraction. It should be noted that differently from Europe the penalties, when monetary, are calculate in accordance with the domestic turnover (in Brazil) as opposed to worldwide. Furthermore, the cap is not the minimum and the percentage the maximum, it is established with the contrary logic.

Another aspect is that it does not have the same two tiered system for ordinary breaches versus more fundamental ones. However, the Brazilian legislations permits a certain leeway and proportional escalation. The methodology itself is not defined in the regulation. It is suppose to be established by the national authority after public consultation (art. 53, para. 4, LGPD).

The law prescribes the necessity of having administrative procedures with full defense for the aggrieved parties available (art.

create an executive organ has to come from the Executive Branch itself. The agency, as part of the federal public administration system, had to have been proposed by the Executive. Any doubts as to the initiative could be fatal to its existence and any decisions made could be questioned under the same basis.

33 Arts. 58 and 59, LGPD, vetoed as well by the President, established a multi-sectoral advisory body, which could be revised.

52, para.1). Moreover, it indicates some of the criteria that should be taken into consideration such as the severity and nature of the breach, the economic condition of the offender and its degree of cooperation. What is more important is that includes a clear obligation to respect a proportionality analysis (art. art. 52, para.1, XI).

3.6.Extraterritorial Effect:

Both the GDPR and the LGPD have a broad base scope. The option was to protect the data of all individuals resident in their territories. In Brazil, it was not different. Art. 3, in consonance with the Brazilian Internet Bill of Rights (Marco Civil da Internet, Lei 12.965/14), states that the law is applicable no matter the means employed or where data is located or the company has its headquarters. What is relevant to engage the obligations is: the processing operation being carried out in the country; the data collection done within the territory; or the purpose of the processing activity is to target (offer goods, services) to or based on data of individuals located in the national territory.

In this sense, it expanded the degree in which the domestic legislation is applicable. As much as the GDPR created what is called a "bubble of protection" for personal data of EU residents, the Brazilian legislations also extends to activities that may not occur within national territory. For instance. if personal data is collected under the aforementioned circumstances, it has to be protected no matter where it is stored, or being processed or even who is actually processing it. The obligation for the company continues and, remember, the company can be called to repair in a jointly and severely fashion.

IV) CONCLUSION - GDPR À BRASILEIRA

The GDPR updated European legislation on the matter for the 21st century. The Brazilian General Data Protection Legislation (LGPD) certainly has followed in its footsteps. Instead of continuing in a piecemeal type of sectorial regulation as has happened so far in countries such as the United States, Brazil has opted for a strong general system.

It is important to understand that the LGPD is not a precise copy of the GDPR. It differs in its granular application. It has to be highlighted that their constitutive principles have a similar basis and are intended to create a rights-based regulation with an open textured aimed to be further regulated and enforced by a central data-protection authority. [34]

34 The Presidential veto in Brazil makes this as a matter of fact possibly up for discussion. The structure, of the regulation, however, is based on the need of a data protection

As a matter of legal basis to acquire and process data, both follow a method of emphasis on freely given, informed consent. However, they open up, including the legitima interests of the controllers. Brazil goes even further including health and credit protection. Arguably, they could also be subsumed under other headings in the GDPR.

The two systems converge as well in prescribing privacy as matter of default and design. From the start the interests of privacy of data subjects have to be taken into consideration. They also establish very steep sanction mechanisms even if in the European case they mean analyzing the worldwide annual revenue of the companies and in Brazil the domestic.

Finally, the Brazilian data-protection system emulates the European in its notion that data may circulate, however, the standards of protection have to be maintained. The two regulations share the concept that its own regulation is from the of-set applicable wherever data collected of its citizens or residents is. It goes beyond the mere territorial approach to a extraterritorial one.

The LGPD, then, adds up a certain "Brazilian flavor" to the GDPR regulation. They do, however, share the same model, logic, even structure. It may allow an easier case for a free flow of information between the country and Europe and hopefully they may fulfill their mandates to protect individual's privacy and personal data.

REFERENCES

DE HERT, P., & PAPAKONSTANTINOU, V. The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. In.: Computer Law & Security Review , 28, 130-142, 2012.

CARSON, Angelique. Consent Is King in Latin America: Navigating the Eight Existing DPAs with a Look to the Future. Available at: https://iapp.org/news/a/2013-06-03-consent-is-king-in-latin-america-navigating-the-eight-existing/

FOLSOM, Ralph H., LAKE Ralph B., NANDA, Ved P. European Union Law After Maastricht: A Practical Guide For Lawyers Outside the Common Market. The Hague: Kluwer. 2012, p. 5.

EDWARDS, Lilian, VEALE, Michael. Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. 16 Duke L. & Tech. Rev. 18. December 4, 2017. P. 32.

POST, Robert C. Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. 67 Duke

authority, as seen above.

Law Journal. February 2018.

SCHWARTZ, Paul M., PEIFER, Karl-Nikolaus. Transatlantic Data Privacy Law. 106 Geo. L.Journal. November 2017.

PETERSEN, Kyle. GDPR: What (and why) you need to know about EU data protection law. 31 Utah Bar Journal. July/August, 2018.

DWARDS, Lilian, VEALE, Michael. Slave to the algorithm? why a 'right to an explanation' is probably not the remedy you are looking for. 16 Duke L. & Tech. Rev. 18. December 4, 2017. P. 23.

VOSS, W. Gregory. Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation. 50 R.J.T. 783, 2016.

FACCIPONTI, Joseph P., MCGRAIL, Katherine. GDPR Is Here — What If You Didn't Prepare? Law 360. May 24, 2018.

FRANCKE, Glory. Time To Update Your Privacy Statement For GDPR. Law 360, September 26, 2017.

SLOAN, R. H. and WARNER R. Beyond Notice and Choice: Privacy, Norms, and Consent. In.: Suffolk University Journal of High Technology Law, No.: 2013-16, 12 Apr 2013. Available at SSRN: https://ssrn.com/abstract=2239099.

ARRUDA, D. S. and FRANCO, P. Nova lei do cadastro positivo beneficia consumidor?Porque nem tudo que reluz é ouro. In.: Jota, January 12, 2018. Available at: https://www.jota.info/opiniao-e-analise/artigos/nova-lei-do-cadastro-positivo-beneficia-consumidor-12012018.

SOLOVE, D. and HARTZOG, W. The FTC and the New Common Law of Privacy. In.: Columbia Law Review, vol. 114, 2014, 583.

MAYER-SCHÖNBERGER, V. Delete: The Virtues of Forgetting in the Digital Age. Princeton, 2011.

BIONI, B.; OLIVEIRA GOMES, M. C. and MONTEIRO, R. L. GDPR matchup: Brazil's General Data Protection Law. IAPP, October 4, 2018. Available at: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/.

GELLERT, R. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. International Data Privacy Law , 5, 3-20, 2015;

SPINA, A. A Regulatory Mariage de Figaro: risk regulation, data protection, and data ethics. European Journal of Risk Regulation , 8, 88-94, 2017.

ZANNATA, R. Proteção de Dados Pessoais como Regulação de Risco: uma nova moldura teórica? In.: Artigos Selecionados Rede

de Pesquisa em Governança da Internet, 2017. Available at: https://www.researchgate.net/publication/322804864_Protecao_de_dados_pessoais_como_regulacao_do_risco_uma_nova_moldura_teorica

Artigo 19. Proteção de dados pessoais no Brasil. Análise dos projetos de lei em tramitação no Congresso Nacional. November, 2016. Available at: http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf

Internet Lab. O que está em jogo no debate sobre proteção de dados pessoais no Brasil? 2016. Available at: http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf.