Breaking Down Brazil's 1st Data Protection Law

By **Felipe Saraiva and Dean Forbes** (January 14, 2020)

Felipe Saraiva

Dean Forbes

After two years in the Brazilian Congress, the General Law of Data Protection was signed on Aug. 18, 2018, by then Brazilian President, Michel Temer, who also signed an executive order (Medida Provisória n. 869, from Dec. 27, 2018).

The executive order created the independent enforcement body for the LGPD, the National Agency of Data Protection and indicated that the new legislation would come into effect in August 2020, 24 months after its publication, after having been approved by Congress and sanctioned by the current Brazilian President, Jair Bolsonaro.

Today, the world's ninth biggest economy and the fourth largest internet user[1] still faces the remnants of a deep economic and political crisis, with the challenge of internal structural class inequality living side-by-side with a growing international investment flow and booming private and industrial sectors.

The coming into effect of the European Union's General Data Protection Regulation in May 2018 brought with it extraterritorial application and enhanced restrictions on international transfers of personal data, an important factor that has influenced the enactment of a Brazilian version of a comprehensive data protection law.

The LGPD

Before the LGPD, legislation regarding data protection in Brazil was sparse. The Brazilian constitution establishes that an individual's privacy, image and honor are broadly protected as fundamental rights. Other laws have focused on particular groups. The Access to Public Information Law is intended for public agencies and public entities in general and provides publicity and transparency to the general public. The internet law provides protection to internet users, and the Consumer Protection Code has the relationship between the consumer and the provider of services or goods in its scope.

The LGPD will operate in conjunction with these existing requirements and does not preempt them. After receiving contributions from different spheres of the Brazilian society, the protection of individual rights, the need for legal certainty and the necessity of stimulating economic growth were among the drivers of the Congress' mandate in drafting the new law.

LGPD Overview

The LGPD governs the protection of "personal data," defined as "information regarding an identified or identifiable natural person." The law also includes definitions of "sensitive personal data" (i.e., "concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person"), "data subject" (i.e., a "natural person to whom the personal data that are the object of processing refer to"), and several other terms that mirror those used in similar comprehensive laws,

including the GDPR, and that may not have existed in Brazilian laws.

As an example, the LGPD innovates by extensively defining the action of data "processing," meaning all acts related to the "collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storing, elimination, evaluation or control of the information, modification, communication, transfer, broadcasting or extraction."

As described further below, protections are broadly required for all personal data processing performed by individuals or legal entities, regardless of their nationality, when (1) processed in Brazil; (2) providing goods or services in connection with such processing in Brazil; or (3) collected in Brazil.

However, there are exceptions, such as where personal data is not being used for economic reasons, or for uses that are exclusively academic, artistic or journalistic. Moreover, the LGPD neither applies to the collection of personal data for public safety, nor for criminal investigation or restraint, clarifying that, for such uses, the protection of the public interest and the respect of due process is expressly required.

LGPD Principles

The LGPD establishes several principles for the processing of personal data:

- Purpose: legitimate, specific and explicit;

- Suitability: conformity with the purposes informed to the data owner;

- Necessity: processing only as much data as necessary for the achievement of the final purpose;

- Free access: facilitated and free access by the data owner in regard to the form and duration of the processing;

- Quality: accuracy, clarity, relevancy and actuality;

- Transparency: clear, precise and easily accessible information relating to the processing activities, as well as to the respective data processing agents;

- Security: use of technical and administrative measures to protect personal data from unauthorized accesses or accidental or unlawful destruction, loss, alteration, communication or dissemination;

- Prevention: measures to prevent the occurrence of damages due to the processing;

- Nondiscrimination: prohibition of unlawful or abusive discriminatory purposes; and

- Accountability: adoption of measures that are efficient and capable of proving the compliance with the personal data protection rules, including the efficacy of such measures.

Agents

The LGPD creates new legal agents and relationships. The controller is the natural individual or legal entity that makes decisions regarding the processing of personal data, whereas the operator will be the one to actually perform the processing. In case the latter doesn't follow the instructions provided by the former, or it violates the applicable data protection legislation, both agents will be deemed jointly and severally liable for any eventual breach. In case a number of controllers are directly involved in the data processing that caused damages to a data subject, these controllers will also be held jointly liable.[2]

Data Processing

As with the GDPR, "anonymous data" will not fall within the definition of "personal data," as it can't lead to the identification of an individual.

The law expressly allows the performance of data processing in certain specific situations[3]:

- Upon the data owner's consent; to comply with the controller's legal or regulatory obligations;

- By the public administration, when necessary to some public policies;

- In studies by research institutions;

- If necessary for the performance or preliminary measures related to contracts to which the data owner is a party, upon the data owner's request;

- For the regular exercise of legal rights;

- For the protection of the owner's life, physical condition or health, in procedures performed by health care professionals or sanitary surveillance agencies;

- For compliance with the controller's legitimate interest, but respecting the data owner's fundamental rights; or

- For the protection of credit.

Consent

In the Brazilian legal system, consent to an agreement may be express or implied. Here, the data owner's free and informed consent is the first requirement for the lawful performance of data processing,[4] and it must be express (i.e., in writing, or in any other way that expresses the owner's will).

To avoid issues related to unlawful consent, the written form is suggested. Further, such consent must be connected to the specified processing activity: The exact purpose and the scope of the processing must be clear. Additionally, when using written consent, such a statement must be included in an outstanding clause, separate from the rest of the agreement.

An important distinction is made regarding data concerning minors (i.e., individuals under 18 years old), where a parent's consent is required for data processing. However, the practicality of enforcing such a provision may be a concern, considering the dynamics of, and possible lack of parental supervision with, online transactions.

Data Portability

Another significant innovation is the portability of the data between controllers, upon the data owner's request and limited only in case of commercial and industrial secrets. A difference between the LGPD's data portability requirement and its GDPR counterpart is that the latter provides that data owners may themselves receive their data, not limiting the portability to the transfer between controllers.

In Brazil, this right may raise technological issues mostly related to the feasibility of the transfer of data among controllers. Interoperability will be a fundamental discussion, as the

necessary technology to guarantee the exercise of the owner's portability rights may have elevated operational costs. Unfortunately, standards related to the exercise of this right were not clarified by the legislator and must still be defined by the ANPD.[5]

Right to Explanation

Similarly to the GDPR, the LGPD grants the data owner the right to request a proper explanation in regard to, and a revision of, automated decisions — made by means of algorithms — in data processing that may have affected their interests.

Nonetheless, automated decisions may trigger another legal principle: the prohibition against discrimination. Algorithms are only as neutral as the programmer, and sometimes decisions may reaffirm the status quo, as the information used to feed such automation can come from data that is already biased.[6] Understanding and explaining exactly how machine learning algorithms reach a specific decision may be extremely complex, and concepts like "privacy by design" or "privacy by default" are possible paths to the compliance with the new legal requirements.[7]

International Transfers

Cross-border transfers are restricted by the LGPD to a listed number of circumstances. For instance, such transfers may be performed in case the foreign country confers an adequate level of protection to personal data as per Brazilian standards — still to be defined by the ANPD. In cases where such protection is not properly provided, the controller may guarantee it by means of contractual provisions, global corporate rules, or by certificates or codes of conduct. These provisions, rules, certificates and codes are expected to be regulated by the ANPD.[8]

Legal Effects and Compliance

Liability is established when damage is caused by a breach of data security, and the ANPD may enforce sanctions such as: a warning; a fine up to 2% of the company's income; a daily fine; the general publication of the underlying infraction; the freezing of the personal data to which the violation refers and the complete deletion of such data.[9]

Agents must adopt security measures in order to prevent breaches, according to standards still to be established by the ANPD. Regardless, these agents are obliged to inform the national authority, in a reasonable time, as defined by ANPD, about any breach or risk to the data owners, describing the nature of the affected data, providing information regarding the data owners, the measures used for data protection, the risks involved in such incident, the reasons for an eventual delay in such report and the measures that are being adopted to mitigate eventual damages.

The agency will then provide the agent with instructions on how to deal with such breach, which can involve the wide disclosure of the incident to the public and measures to mitigate damages.[10]

The agent's liability will be inferred if damage occurs. Possible defenses are: (1) that the agent did not perform that respective data processing; (2) that there was no violation of the applicable law; and (3) that the damage is exclusively the data owner's fault.

The law also provides for compliance guidelines, relevant in order to avoid liability in case of a breach. However, the current lack of clear local standards cause the correct measures to

still depend on the analogous interpretation of measures implemented around the globe.

Grace Period

As a matter of legal principle, the LGPD could not affect previously executed contracts nor rights acquired under the previous legal structure. Although not expressly dictating how it is going to regulate its effects on data acquired before its publication, the LGPD establishes a grace period of 24 months, ending in August, 2020 — time that industry agents must use to conform with the new provisions.[11]

The "Encarregado"

As under the GDPR, the controller will have to appoint a person to serve as the data protection officer, here named encarregado in Portuguese, or "the one in charge." This person will be the communication link between the controller, the ANPD, and the data subjects and shall be responsible for accepting complaints and communications, providing explanations and adopting measures and providing orientation to employees and contractors regarding best practices.

As part of its legal duties, the encarregado will be responsible for training the company's personnel in regard to data security and for keeping in place a system to monitor, document, report and communicate incidents related to data breach.

Data Protection National Agency

The ANPD was granted regulatory powers to enforce the provisions of the LGPD. It also has the scope of providing the industry with best practices and strategic guidelines, interpret the law, create the necessary rules, and sanction those players that violate the LGPD or the rules enacted by the ANPD.[12]

Despite having been legally created, the agency has not yet started its works or issued any enforcement agenda. Therefore, gaps naturally left by the LGPD's text or best practice standards will be pending until filled by the ANPD.

Critical Sectors

The greatest impact of the LGPD will be on companies that process consumers' data in its daily activities, such as technology and marketing companies. Those companies that process less consumer data, but do not have the required infrastructure to provide legal protection, may also be in a critical position.

Health Care

The health care sector is one of the most sensitive areas. Clinical analysis and drug development activities must pay special attention, especially concerning digital systems containing patients' and employees' information — weight, blood type, medical history, etc.

This data may only be processed in compliance with more restrictive measures, such as the data owner's specific consent and public policy-related factors. Maybe most importantly, health-related sensitive data will not be allowed to be transferred for profit between controllers, except when (1) related to the aforementioned portability rights or (2) its transfer is necessary to guarantee adequate supplemental health care services.

Employment

Employers usually ask for the employees' or prospective employees' general personal data, also maintaining a database with resumes and personal documents. Job application processes, internal policies and general documents signed by employees would have to be reviewed, and a screening of who has access to employee's data will have to be implemented for training and control purposes.

Small Businesses

Businesses will be required to allow their clients to discretionarily access and alter the information being processed. Hence, small companies may be the most affected by this new legislation, due to the necessary investments in technological resources and new business platforms. Simple customer-relationship-management-related activities, or information for fidelity programs and discounts, for instance, will have to be reviewed in respect to the suitability and necessity principles.

Credit Scoring

The LGPD grants data owners rights to access their own information, creating an obligation to credit protection agencies to provide access and allow the correction of incomplete or inaccurate data.

As previously mentioned, the right to explanation will require some companies to understand and provide explanation to data owners about automated decisions. Therefore, credit-scoring agencies will have to be prepared for such requirement, and to requests related to the anonymization and deletion of information, for example.

Next Steps

Agents shall implement a series of privacy and data protection measures by August 2020. The influence of the GDPR in the new Brazilian law eases this process; however, the ANPD is still to become active in its regulatory functions and to provide businesses with needed clarity in regard to such compliance issues.

In addition to the appointment of an encarregado, companies will have to understand their data processing activities and data flows, maintaining the appropriate records. This includes all personal data that is being processed by the controller and by third-party operators on behalf of the controller, as such details may in the future be demanded by the national authority.[13]

Therefore, agents will have to screen all of their current data processes, evaluating current databases in light of the LGPD principles. The LGPD does not force agents to maintain such impact reports, as the GDPR does, but the ANPD may request those in the future.

Upon such mentioned screening, the collected data must be classified as per the different levels of protection conferred by the LGPD, e.g. personal data, sensitive data and anonymous data. Accordingly, appropriate privacy compliance policies would be recommended. In addition, in order to mitigate legal exposure in the event of a data breach, putting in place a written information security policy and a data incident response plan should be strongly considered.

Current contractual provisions should likely be revisited, and the agents will have to obtain

the relevant consent for the processing of previously acquired data. Suppliers and other contractors will also have to go through a due diligence process to guarantee their compliance, considering the possibility of joint liability.[14]

The GDPR requires the controller to execute an agreement with the operator and lists mandatory provisions to be included in it. Despite the absence of a similar provision in the LGPD, such an agreement is recommended to avoid misinterpretations in regard to the controller's instructions regarding the use of the collected data.

Until more concrete guidance is provided by the ANPD, agents should observe the plain text of the law and consult with appropriate legal counsel for advice on compliance activities that are specific to their organizations.

Felipe Saraiva is an international lawyer and Dean Forbes is counsel at Sidley Austin LLP.

[1] Brazil's Rio Times publication cites to the Brazilian Statistics Institute (IBGE). See L. Alves, "Number of Internet Users in Brazil Grows by Ten Million in One Year," Rio Times (Dec. 20, 2018) https://riotimesonline.com/brazil-news/rio-business/number-of-internet-users-in-brazil-grows-by-ten-million-in-one-year/. See also J. Elhres, "Latin America: An ecommerce economy on the rise," Mobile Payments Today (June 6, 2019) https://www.mobilepaymentstoday.com/blogs/latin-america-an-ecommerce-economy-on-the-rise/.

[2] LGPD, Article 42, §1, I.

[3] LGPD, Article 7.

[4] LGPD, Article 7, I.

[5] Frazao, Ana; Nova LGPD: Direito a Portabilidade (2018); https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direito-a-portabilidade-07112018.

[6] Ferrari, Isabela; Becker, Daniel; Wolkart, Erik N.; Arbitrium ex machina: framework, risks and the governance of decisions informed by algorithms; vol. 995; Revista dos Tribunais (2018); p. 635.

[7] Ferrari, Isabela; Becker, Daniel; Inovação e Inteligência Artificial; vol. 1; Revista do Direito e as Novas Tecnologias (2018).

[8] LGPD, Articles 33 and 34.

[9] LGPD, Article 52.

[10] LGPD, Article 48, §2.

[11]MP 869, Article 65.

[12] LGPD, Chapter 9, Section I.

[13] LGPD, Article 10, §3, and Article 32.

[14] Humberto de Sá Garay, Dicas de compliance para adequação à Lei de Proteção de Dados, Estadão Newspaper, October 9, 2018, https://politica.estadao.com.br/blogs/fausto-macedo/dicas-de-compliance-para-adequacao-a-lei-de-protecao-de-dados/.