Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cybersecurity

Second Edition

Brazil

Kasznar Leonardos Intellectual Property

chambers.com

2019

Law and Practice

Contributed by Kasznar Leonardos Intellectual Property

Contents

1. Basic National Legal Regime p.3
- 1.1 Laws p.3
- 1.2 Regulators p.4
- 1.3 Administration and Enforcement Process p.4
- 1.4 Multilateral and Subnational Issues p.4
- 1.5 Major NGOs and Self-Regulatory Organisations p.5
- 1.6 System Characteristics p.5
- 1.7 Key Developments p.5
- 1.8 Significant Pending Changes, Hot Topics and Issues p.6

2. Fundamental Laws p.6
- 2.1 Omnibus Laws and General Requirements p.6
- 2.2 Sectoral Issues p.7
- 2.3 Online Marketing p.9
- 2.4 Workplace Privacy p.9
- 2.5 Enforcement and Litigation p.10

3. Law Enforcement and National Security Access and Surveillance p.11
- 3.1 Laws and Standards for Access to Data for Serious Crimes p.11
- 3.2 Laws and Standards for Access to Data for National Security Purposes p.11
- 3.3 Invoking a Foreign Government p.11
- 3.4 Key Privacy Issues, Conflicts and Public Debates p.11

4. International Considerations p.12
- 4.1 Restrictions on International Data Issues p.12
- 4.2 Mechanisms That Apply to International Data Transfers p.12
- 4.3 Government Notifications and Approvals p.12
- 4.4 Data Localisation Requirements p.12
- 4.5 Sharing Technical Details p.12
- 4.6 Limitations and Considerations p.12
- 4.7 "Blocking" Statutes p.12

5. Emerging Digital and Technology Issues p.12
- 5.1 Addressing Current Issues in Law p.12

6. Cybersecurity and Data Breaches p.13
- 6.1 Key Laws and Regulators p.13
- 6.2 Key Frameworks p.13
- 6.3 Legal Requirements p.13
- 6.4 Key Multinational Relationships p.14
- 6.5 Key Affirmative Security Requirements p.14
- 6.6 Data Breach Reporting and Notification p.14
- 6.7 Ability to Monitor Networks for Cybersecurity p.14
- 6.8 Cyberthreat Information Sharing Arrangements p.15
- 6.9 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation p.15

Kasznar Leonardos Intellectual Property provides tailored solutions to the most complex IP issues, both nationally and internationally, with a deep understanding and knowledge of different cultures and business industries, combined with technical and legal analysis. The firm provides advice on contractual matters, as industrial property agents with brand price trade-off and as lawyers, arbitrators and mediators in litigation and extrajudicial dispute resolution. Specialised in the management of intellectual assets, the team has 21 partners and more than 200 employees, with correspondents in every state of Brazil, as well as a broad international network. The data protection department is known for providing tailor-made services in connection with Brazilian and foreign data protection laws. Its academic background and continuing researches allow the team to provide concise and accurate advice on the creation of privacy policies and the assessment of risks.

Authors

Pedro Vilhena is head of the digital law practice and is a senior associate who is highly experienced in IP law, and digital and data protection law. He is a member of the International Association of Privacy Professionals (IAPP), a Data Protection Committee member of the International Trademark Association and an Internet Committee member of the Brazilian Intellectual Property Association. Pedro lectures on the Brazilian General Personal Data Protection Law (LGPD) in companies, unions, associations and chambers of commerce, and on its implications to the pharmaceutical industry in companies and unions. He also teaches data protection law on a graduate programme on IP and innovation at the Escola Superior de Advocacia in São Paulo.

Anderson Ribeiro is a partner in the life sciences department, Anderson has a wealth of experience in life sciences, patents, compliance, healthcare and regulatory law. He is a member of the Data Protection Task Group at Sindicato da Indústria de Produtos Farmacêuticos no Estado de São Paulo and lectures on the enactment of the LGPD and its implications to the pharmaceutical industry at the same organisation. Anderson also conducts training sessions at pharmaceutical and biotech clients concerning the impact of the LGPD within their activities.

Larissa Martins is an associate who specialises in IP law, and digital and data protection law. A member of the Brazilian Bar Association, she studied on a short-term intensive course about data protection at Fundação Getúlio Vargas Law in 2018 and speaks Portuguese, English and Spanish.

1. Basic National Legal Regime

1.1 Laws

The Brazilian Federal Constitution protects the fundamental right of privacy in Article 5, embracing the inviolability of private life and intimacy (item X) and the secrecy of correspondence and of telegraphic, data and telephone communications (item XII). The rights of privacy, honour and image are inviolable. In addition, the Brazilian Civil Rights Framework for the Internet ('Internet Act') also protects privacy and personal data, according to Article 3, section II, Article 8 and 11, which determine respect for the Brazilian legislation and to the right of privacy, data protection and secrecy of private communications. The Internet Act also demands the security of data and network functionality.

Brazil is experiencing a key change in its legislation. The Brazilian General Personal Data Protection Act (Law No 13,709/2018, the 'LGPD') was enacted on 14 August 2018. The LGPD was complemented by Provisional Measure No 869/2018, which created the Data Protection National Authority (ANPD). The Articles regarding the creation of the ANPD and the Brazilian Advisory Board on Privacy and Data Protection came into force on 28 December 2018. However, the Provisional Measure postponed the application of the remaining Articles of the LGPD to 15 August 2020. The aim of this Regulation is to protect personal data, which is defined as information regarding an identified or identifiable natural person (Article 5, Section I).

Heavily inspired by the European model of data protection, the LGPD also has provisions in the case of data breach (Article 48). The controller must send the notification to the ANPD and the data subjects, informing them about the occurrence of the incident that may create risk or relevant damage to the data subjects in a reasonable period.

The administrative penalties for infringement of data subjects' rights range from warnings to fines, depending on the degree of the infringement and recidivism of the controller. Administrative penalties do not prevent civil liability, which can be sought by data subjects, both individually or collectively, in courts.

1.2 Regulators

Currently, as the ANPD is not yet established, the main regulators are the National Telecommunications Agency (ANATEL) for data protection issues relating to telecommunication services, the National Consumer Protection Secretariat (SENACON) for the protection of consumers' personal data protection, and the Administrative Council for Economic Defense (CADE) for data protection matters that may undermine antitrust efforts. In addition to these administrative bodies, public prosecutors are also responsible for investigating data breaches and filing lawsuits against controllers or processors. In such cases, an inquiry is initiated upon the prosecutor's request and the investigation is followed by a judicial proceeding.

Once the LGPD is in force, the key regulator will be the ANPD, a body directly linked to the Presidency of the Republic, with technical autonomy. The ANPD has no powers to audit controllers or processors, but to request information through administrative proceedings. It will also be responsible for applying penalties to any infringing entities. The ANPD's jurisdiction will cover any processing operation carried out:

- in Brazil;
- abroad, if the purpose of the processing activity is to offer or provide goods or services or the processing of data of individuals located in Brazil; or
- abroad, if the personal data being processed were collected in Brazil.

1.3 Administration and Enforcement Process

Currently, all regulators are bound to follow general rules for administrative procedures in Brazil. By law, such procedures may be initiated by a complaint or ex officio and the investigated entities are entitled access to all documents and to present their defence. Once a decision is rendered by the corresponding authority, an appeal may be filed and must be analysed and ruled by or on behalf of the president or governing body of such authority. All decisions in administrative procedures in Brazil are subject to revision by a Federal Court.

Once in force, the LGPD will concentrate all such processes under the ANPD. The data protection authority will also be bound to the rules on general administrative procedures, but some specific provisions will apply. The acts of monitoring and sanctioning will be conducted through an administrative proceeding, ensuring that the investigated party will have the right to a prior hearing, full defence and the right to appeal (Article 55-J, Section VI).

Penalties can be imposed under the criteria in Article 52, paragraph 1, which are the:

- severity and the nature of the infractions and of the personal rights affected;
- good faith of the infringer;
- advantage realised or intended by the infringer;
- economic condition of the infringer;
- recidivism;
- level of damage;
- cooperation of the infringer;
- repeated and demonstrated adoption of internal mechanisms and procedures capable of minimising the damage, for secure and proper data processing, in accordance with the provisions of the law;
- adoption of a good practice and governance policy;
- prompt adoption of corrective measures; and
- proportionality between the severity of the breach and the intensity of the sanction.

1.4 Multilateral and Subnational Issues

Currently, Brazil is not considered by any foreign national data protection authority a country providing adequate levels of data protection. Brazil is not a member of any regional or global bilateral or multilateral system of data protection. Once in force and if correctly applied, the LGPD's provisions are expected to increase the level of data protection in this jurisdiction, which will certainly ease relations between Brazil and other relevant systems.

As a Federated State, Brazil may have national, state-level and city-level laws. According to the Federal Constitution, the Federal government is the only level competent to rule on civil law. Some precedent attempts of regional laws on data protection have already been ruled unconstitutional based on such disposition.

Notwithstanding, the State of São Paulo has a pending bill of law (No 598/18) aiming to rule data processing operations in its territory, as a state-level general data protection law. The State of Rio Grande do Sul had a more specific bill (No 293/2017) regarding data processing by the public administration, which was filed away. Rio de Janeiro has a bill (No 375/2015) on the protection of data subjects' rights, which is still pending.

At city-level, there are ongoing discussions about data protection in Campinas (Bill of Law No 297/2017), Recife (Bill of Law No 182/2018) and São Paulo (Bill of Law No 807/2017). The city of Vinhedo enacted its municipal data protection law on 11 June 2018 (Law No 12/2017).

1.5 Major NGOs and Self-Regulatory Organisations

The most noteworthy self-regulatory organisation in Brazil for data protection matters is the Brazilian Data Marketing Association (ABEMD), which upholds the technical and professional development of data marketing and applies the Self-regulation Code of Data Marketing, developed in 1997. The main concern of the ABEMD is the protection of users in email marketing practices, determining that every company needs to have an opt-out option for commercial emails. This Code is not binding, but is widely recognised by consumers and marketing companies.

At least two Brazilian NGOs have been very active in every discussion on data protection during recent years, including public consultations on the bills of law of the Internet Act and of the LGPD.

The Institute of Technology and Society of Rio de Janeiro (ITS) has as its mission to ensure that Brazil responds creatively and appropriately to the opportunities provided by technology in the digital age, and that its potential benefits are widely shared by society. ITS Rio is an independent and non-profit research institute. Its team has more than ten years of expertise, analysing matter of several areas and providing independent opinions in partnership with universities, civil society, private sector and government agencies. Recently, in partnership with the Center of Law, Internet and Society (CEDIS) of the Brazilian Institute of Public Law (IDP), ITS joined an expert team in privacy and data protection to teach a short-term course about data protection and privacy.

The Internet Lab is a centre of interdisciplinary research, which sponsors academic debate and knowledge production on legal and technology areas. Constituted as a non-profit research institute, the Internet Lab acts as a point of connection between academics, civil society parties and the private sector, stimulating the development of projects that address the creation and implementation of public politics in new technologies, namely involving privacy, freedom of speech and gender and identity matters. Supporters include entities such as Google, the Ford Foundation and the Open Society Institute.

1.6 System Characteristics

Brazil's current regulation on data protection is similar to the US model, with several fragmented rules applicable to specific situations (consumer-protection matters, internet users' rights, etc). This fragmented model will be converted into a centralised model upon the entry into force of the LGPD, a general law inspired by the European Union model (and specifically by the text of 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).

The upcoming Brazilian system is very similar to the EU model, but the LGPD is less detailed and refined than the European General Data Protection Regulation (GDPR).

Similarities between the Brazilian and EU systems include:

- processing of personal data must be done on a legal basis;
- the controller bears the burden of proof of consent;
- data subjects are granted extensive rights over their personal data;
- administrative penalties and civil liabilities are cumulative;
- obligation of appointment of a data protection officer, as a rule; and
- international data transfers are allowed for countries that ensure adequate levels of data protection, among other possibilities.

While the general functioning of both systems is similar, some differences are noteworthy, including:

- the GDPR provides more detail about the identifiable natural person (Article 4), while the LGPD only mentions it (Article 5, Section I);
- while the LGPD does not detail each data considered as sensitive (Article 5, Section II and Article 11), GDPR has definitions for health, biometric and genetic data (Article 9);
- the GDPR provides that the consent for processing children's data can be given by themselves upon the age of 16. In Brazil, the LGPD is more severe and follows the Civil Code and the Child and Adolescent Statute, which determine that the legal age is 18 years (Article 14 of the LGPD);
- unlike the GDPR, the LGPD waives data processing agents' liability when damage is exclusively caused by the data subject's or third-parties' fault (Article 42);
- the GDPR provides that the relationship between controller and processor needs to be formalised by an agreement or other legal act (Article 28, paragraph 3), while the LGPD has no such specification (Article 39);
- the data-protection impact assessment report is more detailed in the GDPR than the LGPD; and
- the term for a data-breach notification under GDPR is 72 hours (Article 85), while the LGPD determines that breaches must be notified in a reasonable period (Article 48).

1.7 Key Developments

The enactment of the LGPD is certainly the most important legal development since the Internet Act (2014). As the law is not yet in force, additional information is provided below.

Since the early discussions of the LGDP bill, a great deal of attention has been dedicated to data protection, including extensive media coverage of major breaches and an increas-

ing number of lawsuits, both private and public. Most of those cases are initiated by public prosecutors, especially those at the Federal District, whose extensive knowledge of current and upcoming data protection rules is remarkable.

An important decision [Writ to the Superior Court No 55019/DF] was recently rendered by the Superior Court of Justice, stating that a court order is sufficient to allow access to data collected on the internet and stored in a country abroad (application of Article 10, paragraph 1 of the Internet Act). Based on this decision, local subsidiaries of multinational companies must comply with any court orders requesting access to a database in a foreign country. It also consolidates the Brazilian practice of speeding up data-provision measures, without the need of rogatory letters.

1.8 Significant Pending Changes, Hot Topics and Issues

Considering that the LGPD will be in force as of August 2020, the next 12 months are expected to be crucial to public and private entities' compliance plans. Aside from general compliance efforts seen in other countries, Brazilian companies will have a greater need for awareness programmes and training sessions, considering that data protection is very new to the Brazilian legal system and to the country's culture in general.

Another important hot topic will be the establishment of the ANPD and commencement of its operations. The ANPD is expected to issue several regulations before August 2020 to fulfil some gaps in the LGPD, including criteria to determine which companies will need to appoint a data-protection officer and the validation of sectorial data security practices proposed by specific industries. From a political perspective, the nomination of the ANPD's board of directors by the President of the Republic will certainly be the subject of public analysis, mainly by specialist media.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Currently, there is no legal obligation to appointing a data protection officer in companies that process personal data. This requirement will be applicable after August 2020, in compliance with the LGPD, but the ANPD is authorised to waive this requirement under certain criteria.

The Internet Act predicts the possibility of processing internet users' data only with the consent of the data subject. In some cases, it is also possible to justify the processing operation when there is a court order authorising the procedure (Article 7, Sections II and III).

As of August 2020, under the LGPD, data processing operations will be legal in any of the cases listed in Article 7, which are:

- fulfilment of a legal or regulatory obligation of the data controller;
- execution of public policies by the public administration;
- fulfilment of an agreement of which the data subject is a party, upon the data subject's request;
- protection of the data subject's or of a third-party's life or health integrity;
- conducting studies by public or non-profit research agencies;
- regular exercise of rights in lawsuits, administrative or arbitration proceedings;
- credit protection; and
- controllers' legitimate interests.

There is no direct concept of 'privacy by design' or 'by default' in the legislation, but there are provisions that imply these concepts. The Internet Act requires the information of the purpose and the express consent to collect, use, store or process personal data. This requires mapping which data will be collected and for what purpose (Article 7, Sections VI and VIII).

The LGPD maintains this scenario. There is no definition of these terms, but its provisions require that data-processing agents undertake data-mapping and consider the whole process of obtaining personal data and the reasons for processing it before it is collected, as well as taking privacy and data-protection issues into account throughout the development of new goods and services.

Currently, there is no need to conduct a privacy impact analysis. According to Article 38 of the LGPD, applicable from August 2020, the ANPD can determine that the controller prepares a data-protection impact assessment report referring to its data-processing operations. The report must contain a description of the types of data collected, the methodology used for the collection, and the analysis of controllers regarding adopted measures, safeguards and mechanisms of risk mitigation.

The adoption of external privacy policies is needed to obtain the consent of data subjects in an express, free and informed way, according to Article 7, Section IX of the Internet Act. While adopting internal privacy policies is highly recommended, there is no legal obligation concerning this matter.

While the LGPD does not impose the adoption of internal or external policies, it is unlikely that any processing agent will be compliant with all legal obligations without very structured privacy policies, both internal and external. The adoption of an internal privacy policy is considered 'good

practice' under Article 50 and may mitigate risks and sanctions, in the case of data breaches.

Currently, the most extensive list of rights concerning data protection is laid out in the Internet Act, including:

- inviolability of intimacy and private life, safeguarding the right for protection and compensation for material or moral damages resulting from their infringement;
- inviolability and secrecy of the flow of users' communications through the internet, except by court order, as provided by law;
- inviolability and secrecy of a user's stored private communications, except upon a court order;
- clear and full information entailed in the agreements of services, setting out the details concerning protection to connection records and records of access to internet applications, as well as on network management practices that may affect the quality of the service provided;
- non-disclosure to third parties of users' personal data, including connection records and records of access to internet applications, unless with express, free and informed consent;
- expressed consent for the collection, use, storage and processing of personal data, which must be specified in a separate contractual clause;
- the definitive elimination of the personal data provided to a certain internet application, at the request of the users, at the end of the relationship between the parties, except in the cases of mandatory log retention;
- the publicity and clarity of any terms of use of internet connection-providers and internet applications-providers; and
- application of consumer protection rules in the consumer interactions that take place on the internet.

Further rights are established in the Consumer Protection Code, the Access to Information Act, the Tax Code, the Bank Secrecy Act and the Compliant Debtors List Act, each applying to the corresponding data protection dispositions.

With the application of the LGPD from August 2020, data subjects will have additional rights (Articles 17 to 22), including:

- confirmation of the existence of the processing;
- access to the data;
- correction of incomplete, inaccurate or out-of-date data;
- anonymisation, blocking or deletion of unnecessary or excessive data or data processed contrary to the LGPD;
- portability of the data to another service or product-provider, by means of an express request and subject to commercial and industrial secrecy, pursuant to the regulation of the National Authority on Data Protection;
- deletion of personal data processed with the consent of the data subject (unless the law provides otherwise);
- information about public and private entities with which the controller has shared data;
- information about the possibility of denying consent and the consequences of such denial; and
- revocation of consent under paragraph 5 of Article 8 of the LGPD.

Currently, there is no provision over the anonymisation, de-identification or pseudonymisation of personal data.

Under the provisions of the LGPD, the anonymised data shall not be considered personal data, except when the process of anonymisation to which the data were submitted has been reversed, using exclusively its own means, or when it can be reversed applying reasonable efforts. In such cases, use of data is legal. The use of pseudonymised data is only legal if made by public or non-profit research bodies for public-health studies purposes only.

Currently, there are no legal provisions relating to automated decision making, online monitoring or tracking.

Article 20 of the LGPD, applicable from August 2020, establishes that data subjects have the right to request a review of decisions taken solely on the basis of automated processing of personal data that affects its interests, including decisions intended to define its personal, professional, consumer or credit profile or aspects of its personality. The ANPD is yet to define the reach of automated decisions and the procedures for their revision.

Currently, data protection provisions are not directly connected to the concept of 'injury' or 'harm.' The wording of the LGPD is also very data-centred and does not refer to injury or harm in any way. However, one of the criteria for determining the sanction to be applied by the ANPD is the gravity and the nature of the personal rights affected by the breach. In this sense, data breaches that may cause any type of harm, injury or embarrassment are subject to higher sanctions.

2.2 Sectoral Issues

Sensitive data is not defined by the existing legislation.

From August 2020, the LGPD's definition of sensible data will be applicable – applying to racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organisation membership, health or sex life and genetic or biometric data (Article 5, item II).

The special issues applied are a restriction on processing sensitive data, requirements of special separate consent and a requirement for the controller to provide prior information to the data subject regarding the operational risks of processing data (Article 11).

Financial data
Currently, the Federal Constitution and Bank Secrecy Act protects the financial data and the secrecy of bank operations, so financial institutions shall maintain confidentiality in their active and passive operations and services rendered. Financial data is not listed as sensitive by the LGPD.

Health data
Health data, by its turn, is under protection by several rules and regulations.

Currently, Rule No 124/2006 of the National Supplementary Health Agency determines that private healthcare companies cannot share data subjects' personal data with third parties without consent, under penalty of BRL50,000 (Article 72).

From August 2020, health data will be treated as sensitive according to the LGPD (Article 5, Section II) and will need to be processed under the special conditions imposed by this regulation.

In addition, the Code of Medical Ethics of the Federal Medicine Council sets forth a duty to the healthcare professional to protect patients' data (Articles 73-79).

Law No 13,787/2018, enacted in December 2018, addresses the digitalisation, retention, storage and handling of patients' records. The law establishes that the physical files of all patients need to be digitalised and then disposed of, unless the documents have a historical value. The digitalised records may be deleted after 20 years of the last registration.

Also in December 2018, the Federal Medicine Council adopted Resolution no 2,227/2018, regarding online medical services. Patients need to authorise the transmission of their personal data by informed and free consent. This Resolution is temporarily suspended for public consultation.

Furthermore, within clinical trials, ANVISA's Board of Directors' Resolution – RDC 09/2015 (Article 6, Section II) – and Resolution 466/2012 of the National Council of Health (Item IV.3, e) provides that the data and privacy of clinical trials' participants shall be protected.

Communications data
The Brazilian Constitution sets out that communications and privacy are fundamental rights, with special degrees of protection. The Internet Act also grants the inviolability of the user's communications through the internet, except in cases where there is a court order.

The Brazilian Telecommunications Act (Law No 9,472/1997) also provides that users of telecommunications services are protected by the inviolability of its communication and privacy (Article 3, Section V and IX), unless otherwise determined (Article 72).

The LGPD does not list the communications as sensitive data, unless the communication contains some of the specific matters considered as sensitive and listed in Article 5, Section II.

Currently, other categories of data (including union membership, sexual orientation, political or philosophical beliefs, etc) do not configure a special kind of protection. Sexual orientation, political and philosophical, religious, genetic and biometric data will be considered sensitive data after the application of the LGPD, according to Article 5, Section II.

Voice Telephony
Voice communications are included in the fundamental right of privacy of communications granted by the Federal Constitution. In this sense, Law No 9,296/1996 regulates the final part of Article 5, Section XII of the Constitution, which permits a breach in communication in cases where this information is needed to help with a criminal investigation.

Text Messaging
By analogy, text messages have the same protection as private communications.

Privacy policies are not required explicitly under the law but are a practical way to inform the data subject about the data processing and other provisions involving its privacy.

The use of tracking and behavioural technologies implies the storing of data to offer customised information to the user. However, according to the Internet Act, this kind of processing demands the consent of the data subject and, in order to do that in a practical way, companies use such technologies as cookies (with a warning on the initial screen of their website), beacons, etc. The same need for consent or other requirement for processing personal data will be applied under the LGPD after August 2020.

The same applies to "do not track" considerations, and consent required for behavioural advertising.

Video and Television
In light of the growing importance of internet-based video and smart TVs, under current and upcoming data protection rules, it is fundamental for controllers to obtain consent from viewers, especially by means of terms and conditions of use and privacy and data protection policies.

Social Media, Search Engines, Large Online Platforms
Consent is the key to platforms such as social media and search engines, based on the Internet Act. On social media, platforms are interactive and the data subject has access to its activities, shared data and information. In general, agreements (such as terms and conditions of use, privacy policies and warnings about the use of cookies) are very important to maintain transparency between the company and the user.

Regulatory Obligations
Regulatory Obligations are discussed in **2.2 Sectoral Issues**.

Right to Be Forgotten (or of Erasure)
Currently, the Internet Act does not mention the right to be forgotten/erasure, but only determines periods from six months to one year to store access, connection and application logs. Before these specific timeframes, the controller cannot erase this data, not even upon the request of the data subject.

With the application of the LGPD from August 2020, erasure will be a right of data subjects. After the controllers/processors have processed the data, they must erase the information, unless:

- it is necessary to comply with legal or regulatory obligations;
- it is needed for study by a research entity, ensuring, whenever possible, the anonymisation of the personal data;
- it is to be transferred to third parties, provided that the requirements for data processing are obeyed; and/or
- it is for the exclusive use of the controller, with access by third parties prohibited, and provided the data has been anonymised.

Addressing Hate Speech, Disinformation, Abusive Material, Political Manipulation, etc
Hate speech, disinformation, abusive material, political manipulation is more relevant to personality rights than data protection rights in Brazilian legislation. There are penalties in civil and criminal spheres for those who addresses hate speech, spread disinformation or attempt political manipulation over the internet. Specifically, when the abusive material contains sexual content (eg, revenge porn), the Internet Act establishes that the internet-provider must remove the content immediately, considering only the notice by a party, with no need for a court decision (Article 21).

Data portability
There are no current provisions on data portability, but the measure is listed as a data subjects' right under Article 17 of the LGPD.

Children's Privacy
Discuss age and consent issues, parental disclosure and consent.

The Civil Code and the Child and Adolescent Statute establish 18 years as the legal age, so anyone under this age needs the authorisation of a responsible person. The Internet Act establishes parental disclosure, since the user (responsible person for the minor) will have the opportunity to choose the content they find appropriate (or not) for the child or adolescent (Article 29).

The application of the LGPD will introduce further provisions on the processing of data involving children and adolescents. According to the law, the data will be processed in the best interests of the children and by the separate consent of one of his or her parents or legal representatives. (Article 14).

Educational or school data
There are no provisions involving educational or school data specifically. When related to children, the same rules above apply.

2.3 Online Marketing

Considering the need to gain consent to process data on the internet, as established by the Internet Act, commercial and marketing communications emails need to have an opt-in and opt-out option. If the user decides to opt-out, the controller needs to remove him or her from its mailing list. With the enactment of the LGPD and its application from August 2020, the opt-in and opt-out system remains, and the data subject will need to give their consent by accepting the terms and conditions of use, for example.

Both current (Internet Act) and upcoming (LGPD) legislation have the same main obstacle to behavioural advertising – the lack of data subject consent to process data. Once consent is obtained by whichever valid means, there are no additional constraints to the practice.

Both current (Internet Act) and upcoming (LGPD) legislation have the same main obstacle to location-based advertising – lack of data subject consent to process data. Once consent is obtained by whichever valid means, there are no additional constraints to the practice.

2.4 Workplace Privacy

There is no special law regarding monitoring the workplace and privacy. The need to respect the privacy of communication – according to the Federal Constitution and Internet Act – remains. The employer has the right to use technologies to identify content accessed by its employees.

In order to harmonise privacy protection, communications secrecy and protection of trade secrets, there is extensive case law on the lawfulness of monitoring employees' use of the internet in the workplace, provided that the monitoring is not targeted to a specific individual. For their own safety, companies must adopt terms and conditions of use and privacy policies online, as well as detailed internal rules for the security of information, with the consent of their employees to validate the processing of their personal data according to the current and future applicable legislation.

Hypothetically, labour organisations and work councils can include data-protection provisions in their collective labour agreements or collective labour conventions. However, con-

sidering the low level of awareness of the subject in Brazil, there are no current CLAs or CLCs dealing with the protection of employees' data. The growing importance of the subject in Brazil indicates that data protection may be discussed by such entities soon.

Currently, there is no Brazilian law that specifically addresses whistle-blower hotlines or anonymous reporting. There is also no specific mention in the LGPD. However, companies can include whistle-blowing provisions in their internal security policy, to identify, among other things, data breaches, hate-speech, abusive material or content involving sexual acts or nudity.

Brazilian law does not establish specific prohibitions or boundaries to the use of digital loss-prevention technologies.

2.5 Enforcement and Litigation

Regarding privacy and data protection, regulators must currently establish that the violation arises from the lack of consent to data processing. When it comes specifically to privacy, the standards will also depend on the specifications of the case, according to the Internet Act.

Under the LGPD, the ANPD must establish standards to allege violations by the controller and/or processor, proving which data subjects' right is being violated. From then on, the standards will vary according to the violation.

Current administrative penalties established by the Internet Act are:

- warnings, with indication of the deadline for a corrective action to be taken;
- fines of up to 10% of the revenues of the economic group in Brazil in its last financial year, excluding taxes, considering the economic condition of the offender and the principle of proportionality between the seriousness of the misconduct and the intensity of the penalty;
- temporary suspension of activities involving any operation of gathering, storage, custody and treatment of records, personal data or communications by connection and internet application-providers; and
- prohibition from carrying out activities involving the same acts above.

In the case of penalties for a foreign company, its subsidiary, branch office or establishment in Brazil will be jointly liable to pay the fines. These penalties are not applied due to a lack of a centralised agency and the low actuation of fragmented entities. It is applied only by the regulation of civil liability (Articles 186 and 927 of the Civil Code). Additional criminal and civil liabilities may apply.

From August 2020, administrative penalties for irregular data processing will include (Article 52):

- warnings, with an indication of the time-period for adopting corrective measures;
- a simple fine of up to 2% of a private legal entity's, group's or conglomerate's revenues in Brazil, for the prior financial year, excluding taxes, up to a total maximum of BRL 50 million per infraction;
- a daily fine, subject to the total maximum referred to above;
- publicising of the infraction once it has been duly ascertained and its occurrence has been confirmed;
- blocking the personal data to which the infraction refers until its regularisation; and
- deletion of the personal data to which the infraction refers.

These penalties do not exclude the judicial compensation of moral and material damages to the data subject, in a value that will be determined by a judge and can be – or not – based on the administrative fines (paragraph 3).

The value of daily fines applied to infractions of the LGPD shall be subject to the severity of the infraction, the extent of damage or losses caused and grounded reasoning by the national authority.

As Brazil's legal system is transitioning from a US to an EU model, there are currently few cases brought to justice. A major case recently brought in refers to facial analysis in connection with advertising.

The concessionaire of São Paulo's subway installed advertising panels with facial-analysis technology in three subway stations. These panels detected the reaction to the advertisement (impressed, happy, sad, indifferent, etc). The Brazilian Institute of Consumer Protection (IDEC) filed a Public Civil Action against the concessionaire, claiming the sensor of the doors forced the passengers to look at the panels, thus allowing an intrusive collection of their personal data. There is no relevant decision yet. While data protection was a side claim, the case is an example of the possible implications of the use of the described technology.

More cases are expected to be filed after the entry into force of the LGPD in August 2020.

Legal standards are set by the Civil Procedure Code. The plaintiff must be the legitimate party to file the lawsuit, and have the interest to act and demonstrate on the legal possibility of its request. In addition, the plaintiff must demonstrate the defendant's illicit conduct, the damage borne by the plaintiff and the cause–consequence relation between them.

Brazilian law does not allow class actions. However, in the case of massive leaks of data, the public prosecutor or other specific organisations can initiate an investigation and civil actions against the controller/processor of data, according to the Public Civil Action Law (Law No 7,347/1993).

There are no relevant public civil actions involving privacy and data protection matters, but only open investigations regarding the leak of personal data (question **6.9 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation** below).

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

As a rule, access to any data requires court authorisation. However, in the case of criminal investigations, under Article 15 of Law No 12,850/2013, the public prosecutor or the chief police officer can have access only to the data that inform personal qualification, affiliation and address maintained by the electoral justice, phone companies, financial institutions, internet-providers and credit card administrators. In addition, according to Brazilian case law, the Brazilian Federal Revenue Office may request data from banks when necessary to investigate financial crimes against the public administration, under Complementary Law no 105/2001. The entry into force of the LGPD is not expected to change the application of such prior laws, as the law will not apply to processing operations carried out for law-enforcement purposes.

Privacy is safeguarded by the Federal Constitution and the Brazilian Civil Code. In practice, there is a lot of discussion on how law enforcement deals with the privacy of people under investigation. The Brazilian Supreme Court has ruled that internet service-providers allowing exchanges of messages are not bound to reveal the content of those messages to public authorities, following a series of decisions determining the blocking of WhatsApp services in Brazil in view of the company's "lack of collaboration." In addition, there is an ongoing discussion regarding the legality of police authorities analysing the contents of cell phones of people under investigation.

3.2 Laws and Standards for Access to Data for National Security Purposes

As a rule, access to any data requires court authorisation. However, in cases of national security, under Article 15 of Law No 12,850/2013, the public prosecutor or the chief police officer can have access only to the data that inform personal qualification, affiliation and address maintained by the electoral justice, phone companies, financial institutions, internet providers and credit card administrators. In addition, according to Brazilian case law, the Brazilian Federal Revenue Office may request data from banks when necessary to investigate financial crimes against the public administration, under Complementary Law No 105/2001. The entry into force of the LGPD is not expected to change the application of such prior laws, as the law will not apply to processing operations carried out for national security purposes.

Privacy is safeguarded by the Federal Constitution and the Brazilian Civil Code. In practice, there is a lot of discussion on how law enforcement deals with the privacy of people under investigation. The Brazilian Supreme Court has ruled that internet service-providers allowing exchanges of messages are not bound to reveal the content of those messages to public authorities, following a series of decisions determining the blocking of WhatsApp services in Brazil in view of the company's "lack of collaboration." In addition, there is an ongoing discussing regarding the legality of police authorities analysing the contents of cell phones of people under investigation.

3.3 Invoking a Foreign Government

Currently, there are no obstacles to such invocation. Under the LGPD, from August 2020, the collection and transfer of personal data upon request of a foreign authority will only be considered licit if that request constitutes a legal or regulatory obligation.

3.4 Key Privacy Issues, Conflicts and Public Debates

There are few public debates on government access to personal data. As the general public is still generally unaware of its data protection rights (both existing and upcoming), government actions to process additional data from citizens are seldom contested. In this regard, some caution-inspiring legislation recently passed in Brazil, including a national decree issued in 2016 (Decree No 8789/16), which authorises all government bodies to share their databases with other government bodies, to simplify the offering of public services.

On the other hand, citizens are entitled to request full access to their personal data held by government bodies, under Law No 12,527/2011.

Once the LGPD is in force, data processing operations carried out by the government will also be regulated, under Articles 23 to 32. The government will have to process data pursuing the public interest, if it communicates the situations in which, in the exercise of its competences, it carries out the processing of personal data, supplying clear and up-to-date information about the legal basis, purpose, procedures and practices used to carry out these activities in easily accessible media, preferably on its websites.

4. International Considerations

4.1 Restrictions on International Data Issues

Currently, Brazilian law does not provide any restrictions specific to international data transfers. Once the LGPD starts to be applied from August 2020, international data transfers will only be possible (Article 33):

- to countries or international organisations that provide adequate levels of data protection;
- when the controller offers and proves compliance with the principles and rights of the data subject and the regime of data protection, upon specific contractual clauses, standard contractual clauses, global corporate rules or regularly issued stamps;
- when the transfer is necessary for international legal co-operation between public intelligence, investigative and prosecutorial agencies;
- when the transfer is necessary to protect the life or physical safety of the data subject or of a third party;
- when the ANPD authorises the transfer;
- when the transfer results in a commitment undertaken through international co-operation;
- when the transfer is necessary for the execution of a public policy or legal attribution of public service;
- when the data subject has given his or her specific consent for the transfer, with prior information about the international nature of the operation, with this being clearly distinct from other purposes; and
- when it is necessary to satisfy compliance with regulatory obligations by the controller, execution of a contract or preliminary procedures related to it and the regular exercise of rights in judicial, administrative or arbitration procedures.

4.2 Mechanisms That Apply to International Data Transfers

Currently there is a lack of regulation regarding international data issues. The LGPD, as explained above, established that international data transfers must be formalised by contractual provisions or corporate rules when there is no level of protection of the country that is receiving the data. The consent will have to be granted by the data subject when there are no other requirements for data processing.

One practice of companies is to ensure the data is end-to-end encrypted when it is transferred, to reduce the probability of hacking or leaks.

4.3 Government Notifications and Approvals

Brazilian law does not currently regulate international data transfers. According to the LGPD, when applicable, international data transfers will be allowed under a list of circumstances, one of which is the obtainment of an authorisation by the ANPD (Article 33, item V).

4.4 Data Localisation Requirements

The Internet Act does not require that data is maintained in the country, so the data can be stored in cloud storage in another country, for example. After the LGPD comes into force, there will be no requirement to maintain the data in-country, but the requirements of Article 33 will need to be followed to validate the data transfer.

4.5 Sharing Technical Details

There is no current or upcoming regulation that determines the sharing of algorithms or technical details with the government.

4.6 Limitations and Considerations

Brazilian law does not currently regulate international data transfers. With the application of the LGPD after August 2020, international data transfers (Article 33) may be considered for foreign data requests, litigation proceedings or internal investigations if:

- the transfer is necessary for international legal co-operation between public intelligence, investigative and prosecutorial agencies, in accordance with the instruments of international law;
- the transfer results in a commitment undertaken through international cooperation;
- the transfer is made to ensure compliance with a legal or regulatory obligation by the controller; and
- the transfer is necessary for the regular exercise of rights in judicial, administrative or arbitration procedures.

4.7 "Blocking" Statutes

Brazilian law has no blocking statutes related to privacy or data protection.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

There is no legislation addressing the term 'Big Data.' The Internet Act prohibits the storing of excessive personal data in relation to the purpose for which the data subject gave their consent, so it is important to observe the correct processing of this data. With the future application of the LGPD, this need to regularise the processing of data will increase.

Currently, the following issues are not addressed by law:

- *automated decision-making*: once the LGPD is applied, it will be a right of the data subject to request a review of decisions taken solely on the basis of automated processing of personal data, including decisions related to the personal, professional, consumer or credit profile and personality (Article 20).

- *profiling*: Once the LGPD is applied, data used for profiling can be considered personal data (Article 12, paragraph 2) and will only be susceptible to processing under one of the legal grounds set forth in Article 7.
- *artificial intelligence (including machine learning)*: under the LGPD, the ANPD may issue regulations on the matter.
- *Internet of Things (IoT)*: under the LGPD, the ANPD may issue regulations on the matter.
- *autonomous decision-making (including autonomous vehicles)*: under the LGPD, the ANPD may issue regulations on the matter.
- *facial recognition*: under LGPD, it is highly likely that the face will be considered a sensitive personal data, and will therefore enjoy a special protection.
- *biometric data*: after August 2020, LGPD will consider biometric information as sensitive personal data (Article 5, Section II).
- *geolocation*: once the LGPD is applied, if the geolocation can identify or make identifiable a natural person, the LGPD will apply to that processing of data.
- *drones*: the operation of drones is regulated by Brazilian Civil Aviation Special Regulation no 94/2017, enacted by the National Agency of Civil Aviation (ANAC). Unmanned aircraft operations (for recreational, corporate, commercial or experimental use) must follow ANAC rules, which are complementary to the regulations of other public agencies such as the Air Space Control Department (DECEA) and the National Telecommunications Agency (ANATEL). The LGPD does not have any provisions regarding drones.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators

It is worth mentioning that the Internet Act deals with cybersecurity and data breaches. To store and maintain the availability of connection and access logs, internet-providers need to establish their security and secrecy measures for providing services in a clear way and meet the standards set by regulation, respecting the right to confidentiality regarding trade secrets.

The Central Bank Resolution no 4,658/2018, regarding cybersecurity policy and requirements for processing and storage data and cloud computing, is observed by financial institutions and other institutions authorised to operate by the Central Bank of Brazil.

The Penal Code lists some actions as crimes, such as hacking/invasion of computer device (Article 154-A) and credit/debit card falsification (Article 298, sole paragraph).

Once the LGPD is applied, data processing agents shall adopt security, technical and administrative measures able to protect personal data from unauthorised accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing. The ANPD sets out minimum technical standards of security for data processing agents (Article 46).

The Central Bank may have an extensive role in regulating and enforcing its regulations on cybersecurity for financial organisations. For the repression of cyber-attacks listed as crimes, valuable work has been conducted by specialist police units (mainly in São Paulo) and public prosecutors.

Brazil does not have any cybersecurity agencies equivalent or similar to ENISA.

The ANPD sets minimum standards of security and serves as a centre of information in the case of data breaches, since the LGPD establishes that data processing agents must communicate with the ANPD in the case of risk for data subjects.

The Central Bank may have an important accessory role to ANPD's in connection with data protection in the financial sector, as it will enforce Resolution No 4,658/2018.

The impact of the LGPD and of the activities of the ANPD on other regulators such as ANATEL, CADE and SENACON is yet to be known. Public prosecutors may enhance their data protection and cybersecurity related activities by collaborating with the ANPD.

6.2 Key Frameworks

Currently, ISO 27001 is considered the deployed guidance for information security.

6.3 Legal Requirements

When LGPD becomes applicable, data processing agents should adopt security measures to protect databases and implement a governance programme for privacy that establishes adequate policies and safeguards based on a process of systematic evaluation of the impacts and risks to privacy (Article 50, Section I, item d).

According to the LGPD, an incident response plan is encouraged as good practice (Article 50, Section I, item g).

There are no legal requirements referring to the appointment of a chief information security officer. The measure may be important, or even essential, for some entities, depending on the nature of their activities, but may prove excessively burdensome to others.

There are no legal requirements referring to the involvement of the board of directors in information security issues. Such involvement, however, is highly recommended as a good practice on which the success of any internal policies on the matter will rest.

There are no legal requirements referring to conducting preventive measures such as internal risk-assessments, vulnerability scanning, or penetration tests. These measures can be considered as good practice by the LGPD and, in the future, potentially decrease the eventual value of the fine applied to the controller/processor (Articles 50 and 52, paragraph 1, Section VIII).

There are no legal requirements referring to the adoption of insider-threat programmes.

There are no legal requirements referring to due diligence, oversight and monitoring of vendors or service-providers. However, data processing agents must be reasonably diligent to avoid claims of gross negligence in the case of security breaches caused by or with the contribution of a related third party.

The training of employees is considered good practice by the LGPD and, in the future, could potentially decrease the eventual value of the fine applied to the controller/processor (Articles 50 and 52, paragraph 1, Section VIII).

6.4 Key Multinational Relationships

There are no current multinational relationships involving Brazil regarding data protection.

6.5 Key Affirmative Security Requirements

Currently, there are no key affirmative security requirements addressed by law for the following:

- personal data;
- material business data, networks or systems;
- critical infrastructure;
- prevention of denial of service attacks, or similar attacks on system or data availability or integrity; or
- other data or systems.

Under the LGPD, the ANPD may issue regulations on these matters.

Kasznar Leonardos Intellectual Property

Teófilo Otoni St
63/ 5º-7º floor
ZIP code: 20090-070

Tel: +55 21 2113 1919
Email: mail@kasznarleonardos.com
Web: www.kasznarleonardos.com

Kasznar Leonardos 1919
INTELLECTUAL PROPERTY BRAZIL

6.6 Data Breach Reporting and Notification

Currently, there is no specification for how a potentially reportable data security incident or breach is defined. Once the LGPD comes into force, the controller must communicate the occurrence of a security incident that may create risk or relevant damage to the data subjects. The guidance of the ANPD will be essential for detailing this obligation.

All data elements are considered as personal data and sensitive data.

Currently, no systems are addressed by law. Under the LGPD, the ANPD may issue regulations on the matter.

No security measures apply to medical devices currently. Under the LGPD, the ANPD may issue regulations on the matter.

There are no security requirements which currently apply to Industrial Control Systems (and SCADA). The ANPD may issue regulations on the matter, under the LGPD.

Currently, no security requirements apply to the IoT. Under the LGPD, the ANPD may issue regulations on the matter.

Currently, data processing agents are not under a legal obligation to report to government authorities, individuals or other companies or organisations. After August 2020, the LGPD provides that an incident response plan will be necessary (Article 48). The LGPD determines that communication with the data subject and the ANPD must be carried out within a reasonable period, when there a is possibility of risk or relevant damage to the data subject. The sections of Article 48 specify the requirements of this report.

If there is a risk of harm, the controller must send a report informing the security incident or data breach to the ANPD, containing:

- a description of the nature of the affected personal data;
- information on the data subjects involved;
- an indication of the technical and security measures used to protect the data, subject to commercial and industrial secrecy;
- the risks related to the incident;
- the reasons for delay, in cases in which communication was not immediate; and
- the measures that were or will be adopted to reverse or mitigate the effects of the damage.

6.7 Ability to Monitor Networks for Cybersecurity

There is no permission or prohibition to monitor networks for cybersecurity specifically in the current legislation or even in the LGPD. However, the use of monitoring tools is widespread by companies.

6.8 Cyberthreat Information Sharing Arrangements

Cybersecurity information sharing has received little attention in Brazil to date but is expected to see significant developments in the next few years.

Voluntary information-sharing opportunities have received little attention in Brazil to date but is expected that significant developments will be seen during the next few years.

6.9 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

Currently, Brazilian law does not provide for audits for cybersecurity violations or data security incidents. The public prosecutors of the federal district are very proactive in investigating data-breach incidents and are currently working on several parallel cases, such as the breaches recently suffered by companies such as Tivit, Sky, FIESP, Stone and Netshoes.

There are no relevant known private cases of litigation involving such allegations. As Brazilian law does not allow class actions, most lawsuits filed under those claims are very small (ranging from one to 50 plaintiffs) and must not be considered a substantial sample for analysis of court interpretation of data protection dispositions.