Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top-ranked lawyers

Data Protection & Privacy

Brazil: Law & Practice

Claudio Barbosa, Aline Zinni, Anderson Ribeiro and Larissa Martins
Kasznar Leonardos Intellectual Property

practiceguides.chambers.com

2021

BRAZIL

Law and Practice

Contributed by:
Claudio Barbosa, Aline Zinni, Anderson Ribeiro and Larissa Martins
Kasznar Leonardos Intellectual Property see p.15

Contents

Contributed by: Claudio Barbosa, Aline Zinni, Anderson Ribeiro and Larissa Martins
Kasznar Leonardos Intellectual Property

1. Basic National Regime

1.1 Laws

Enacted in 1888, the Brazilian Federal Constitution protects the fundamental rights of privacy, honour and image in Article 5, and addresses the inviolability of private life and intimacy in item X and the right to secrecy of correspondence and of telegraphic, data and telephone communications in item XII. Crimes related to wiretapping are addressed by Law No 9296/96, while Law No 12737/2012 criminalises the act of hacking electronic devices with the aim of obtaining, modifying, destroying or disclosing data or information without the owner's authorisation.

The Brazilian Civil Rights Framework for the Internet (Law No 12965/2014 – Internet Act) also addresses the right to privacy, data protection and secrecy of private communication, according to its Article 3, section II, and Articles 8 and 11. The Internet Act also sets forth the obligation to comply with standards related to the security of data and network functionality.

The Brazilian General Personal Data Protection Act (Law No 13,709/2018 – LGPD) was enacted on 14 August 2018, and came into force on 18 September 2020, but its sanctions will only be enforceable as of 15 August 2021. Provisional Measure No 869/2018 was turned into Law No 13853/2019 and created the Data Protection National Authority (ANPD), which will be entitled to regulate, enforce and apply penalties based on the LGPD. The ANPD's directive body was recently appointed and is structured as follows:

- President: Waldemar Ortunho (an engineer with a military career and more than 40 years of experience in information technology);
- Arthur Sabat (a member of the National Chamber of Security since 2018);
- Joacil Rael (an expert in computer science and Data Protection Officer (DPO) of Telebras – Telecomunicações Brasileiras. S.A.);
- Nairane Rabelo (a lawyer specialising in Tax Law, Privacy and Data Protection); and
- Miriam Wimmer (a lawyer specialising in Public Law, a former agent of the National Telecommunications Agency (ANATEL), a former agent of the Management Committee for the Internet in Brazil and current director of the Ministry of Communications).

In general terms, the LGPD applies to all personal data (defined as "information related to an identified or identifiable natural person") undergoing processing operations, whether performed by an individual or company, online or offline, in the following locations:

- 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 was collected in Brazil.

The exceptions are listed in Article 4, which sets forth that the LGPD will not apply if the data processing is carried out exclusively for private and non-economic purposes (if performed by an individual), or for artistic, journalistic, academic, public security, state security, national defence and/or criminal repression purposes.

Since the LGPD was inspired by the General Data Protection Regulation in force in Europe, it also provides for basic proceedings in case of a data breach. The controller must send a notification (which must contain all details about the incident) to the ANPD and to the data subject if the incident is significant enough to pose any risk of damage to the data subjects.

The administrative penalties set forth by the LGPD for the infringement of a data subject's rights range from warnings to fines, depending on the degree and recidivism of the controller or processor. Administrative penalties do not prevent infringing entities being held civilly liable.

Other Brazilian legislation that also addresses the protection of the right to privacy, intimacy and freedom of expression includes:

- the Brazilian Civil Code, addressing personality rights and liability;
- the Child and Adolescent Statute, addressing specific issues and enhanced protection applicable to minors' image and privacy; and
- laws and regulations on telecommunication, consumer and financial aspects, addressing the secrecy of communications, as well as credit, financial and tax information.

1.2 Regulators

The ANPD has been created but is not yet in full operation. On 27 January 2021, the ANPD issued Decree No 11, which made public its regulatory agenda for 2021-2022. The activities are divided into three phases, as follows.

- Phase 1:
  (a) draft of the ANPD's Internal Regulation;
  (b) the ANPD's strategic management;
  (c) regulation about data protection for start-ups, small and medium companies;
  (d) regulation for better understanding about the applicable

sanctions (from article 52 on);
(e) communication of security incidents and deadline for notification; and
(f) Data Protection Impact Assessment.
- Phase 2:
  (a) DPO; and
  (b) international transfer.
- Phase 3:
  (a) compliance with data subjects' rights; and
  (b) legal basis.

The issuance of regulation on such topics will be highly significant for the correct enforcement of the LGPD and effective data protection in Brazil.

Considering the significant amount of data collected and processed in commerce, the National Consumer Protection Secretariat (SENACON) and the Protection and Consumer Protection Foundation (PROCON) must also be considered as regulators when there is personal data involved. ANATEL oversees data protection issues related to telecommunications services. Public prosecutors may also initiate proceedings to investigate potential infringements in the civil and criminal spheres, in addition to individual claims. In such cases, an inquiry is initiated upon the prosecutor's request, and the investigation may be followed by a judicial proceeding.

It is important to highlight that the ANPD cannot audit controllers or processors, but is able to request information through administrative proceedings.

1.3 Administration and Enforcement Process

Although the LGPD is already in force, the administrative sanctions will only be enforceable as of 15 August 2021. Additionally, the ANPD already has plans to address the enforceability of such sanctions in the first semester of 2021 (Decree No 11/2021).

Regardless of this, the administrative consumer protection entities and public prosecutors are bound to act in accordance with general procedures. In short, such procedures may be initiated by a complaint from the offended parties or ex officio, and the investigated entity is entitled to access all documents and to present its defence. Once a decision is rendered by the authority, the parties may file an appeal, which will be analysed and ruled on by or on behalf of the president or governing body of such authority. Considering that most of the authorities entitled to pursue data protection claims are part of the federal public administration, decisions rendered thereby are subject to revision by a Federal Court; if rendered, for example, by the Federal District Public Prosecutor's Office, which is part of the State administration, then it shall be reviewed by the State courts.

Once in force, the ANPD will be bound by the rules on general administrative procedures, but some specific provisions set forth by the LGPD will apply. Oversight, enforcement and sanctioning will be conducted through an administrative proceeding, making sure that the investigated party has the right to an adversary system and full defence.

According to Article 52, 1st Paragraph, the penalties for infringement of the law shall be enforced according to the following criteria:

- the severity and nature of the infractions and the personal rights affected;
- the good faith of the infringer;
- the advantage realised or intended by the infringer;
- the economic condition of the infringer;
- recidivism;
- the level of damage;
- the co-operation of the infringer;
- the 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;
- the adoption of a good practice and governance policy;
- the prompt adoption of corrective measures; and
- the proportionality between the severity of the breach and the intensity of the sanction.

1.4 Multilateral and Subnational Issues

As it has only recently enacted specific legislation concerning data protection, Brazil is still not considered by any foreign data protection body to provide an adequate level of data protection. However, once the law is in force and the national authority starts enforcing it, it is likely that Brazil will strengthen its relationship with data protection entities around the world and be considered as providing an adequate level of protection, especially due to the LGPD's roots in the GDPR.

As a Federative State, Brazil may have national, State and Municipal laws. However, State and Municipal laws are only allowed to address local aspects of national laws – ie, a federal law must have already been created to legitimise the existence of State and Municipal laws ruling the same matter. Some attempts to implement regional laws on data protection have already been ruled unconstitutional based on such disposition. However, several States have bills pending that aim to govern data processing operations in their respective territories, as State-level general data protection laws. Brazilian cities have also enacted data protection rules or are attempting to pass bills of law addressing the subject.

1.5 Major NGOs and Self-Regulatory Organisations

A significant number of Brazilian companies and foreign companies doing business in Brazil are members of the Brazilian Direct Marketing Association (ABEMD), which is a non-profit entity focused on encouraging, expanding and setting up basic rules related to direct marketing in Brazil. ABEMD issued the Email Marketing Self-Regulatory Code (CAPEM), developed in 1997, and sets forth that companies need to provide an opt-out option in their marketing e-mails. CAPEM is being largely adopted not only by ABEMD members but also by non-members, even though its provisions and resolutions are not binding or mandatory.

Two Brazilian NGOs deserve to be mentioned, as they have been very active in monitoring and promoting discussions in many sectors about data protection, including participating in the 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) is an independent, non-profit research institute studying the impacts of and trends in technology in Brazil and the world. Its team has more than ten years of expertise, analysing matters in several areas and providing independent opinions in partnership with universities, civil society, the private sector and government agencies. Recently, in partnership with the Center of Law, Internet and Society of the Brazilian Institute of Public Law, ITS joined an expert team in privacy and data protection to teach a short-term course about data protection and privacy.
- InternetLab is a centre of interdisciplinary research, promoting academic debate and knowledge production on legal and technology areas. Constituted as a non-profit research institute, InternetLab 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 like Google, the Ford Foundation and the Open Society Institute.

1.6 System Characteristics

The current Brazilian legal framework on data protection is similar to the US model, in the sense that it is fragmented into rules applicable to specific situations (consumer protection matters, internet users' rights, etc). Upon the entrance into force of the LGPD, the data protection regulation will be converted into a centralised model, more like the European model. The LGPD was generally inspired by the GDPR and, although it is clearly less detailed and sophisticated than the GDPR, it can be deemed as being very similar thereto.

The similarities between the Brazilian and EU systems are as follows:

- the 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 liability are cumulative;
- processing agents have an obligation to appoint a DPO; and
- international data transfers are allowed for countries that ensure adequate levels of data protection, among other possibilities.

Although the regulations are functionally similar, the following differences are noteworthy:

- the GDPR provides the definition of identifiable natural person, while the LGPD only mentions it;
- while the LGPD does not detail all data considered to be sensitive, the GDPR provides the definitions for health, biometric and genetic data;
- the GDPR sets forth that the consent for processing children's data can be given after a subject reaches 16 years of age, while the LGPD follows the Civil Code and the Child and Adolescent Statute, which determine that the legal age is 18 years old;
- unlike the GDPR, the LGPD waives data processing agents' liability when damage is exclusively caused through the fault of the data subjects or third parties;
- the GDPR provides that the relationship between controller and processor needs to be formalised by an agreement or other legal act, while the LGPD has no such specification;
- the data protection impact assessment report is more detailed in the GDPR than in the LGPD; and
- the term for a data breach notification under the GDPR is 72 hours, while the LGPD determines that breaches must be notified within a reasonable period.

1.7 Key Developments

The entering into force of the LGPD in 2020 is certainly the most important legal development on the matter since the Internet Act (2014).

The creation of the ANPD, the appointment of the board of directors and the disclosure of the agenda for 2021-2022 are also important developments so far. The ANPD is still managing to address important topics, but no specific regulations have been enacted so far.

After the LGPD entered into force, litigation cases started to arise in the Judiciary. The most commented-upon decision was

rendered by the 13th Civil Panel of the State Court of São Paulo, due to the sharing of personal data with third parties not related to the agreement. The panel ruled for the payment of BRL10,000 as moral damages.

There are also other lawsuits, including lawsuits filed by the Federal and State Public Prosecutor's offices, that are willing to enforce the LGPD through public civil actions. Among the matters discussed, the offices question the selling of data and the processing of biometrical data.

1.8 Significant Pending Changes, Hot Topics and Issues

After the entering into force of the LGPD, the appointment of the ANPD's board of directors and the disclosure of the authority's main activities for the next two years, the pending developments concern the following:

- clarification about the liability of and necessity for a DPO in small companies;
- more details about security standards, including in the drafting of data protection impact assessment reports;
- regulation for international transfers and a list of countries considered adequate; and
- a definition of standards for the enforceability of sanctions.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Appointment of Privacy or Data Protection Officers

All personal data controllers must appoint a Data Protection Officer (DPO). This requirement will be further detailed in the first semester of 2022, when the ANPD is planning to issue a specific regulation on the matter.

Criteria to Authorise Collection, Use or Other Processing

The Internet Act predicts the possibility of processing internet users' data only if the data subject provides consent (online environment). The exception for the consent requirement rests in a preceding Court Order.

Upon the LGPD's entrance into force, data processing operations are legitimate if they comply with the following legal basis:

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

"Privacy by Design" or "by Default"

Although there is no explicit definition of these terms, the LGPD provides that security measures must be adopted from the conception phase of the product or service until and during its operation.

Privacy Impact Analyses

There is currently no legal obligation to conduct a privacy impact analysis. Upon the LGPD's entrance into force, the ANPD will be entitled to order a data protection impact assessment report referring to the controller's data processing operations. The report must contain the description of the types of data collected, the methodology used for the collection and the analysis of the controllers regarding adopted measures, safeguards and mechanisms of risk mitigation.

Internal or External Privacy Policies

In order to comply with the obligation set forth by the Internet Act and the LGPD to obtain a data subject's clear, free and informed consent, it is recommended to adopt external privacy policies. There is no such obligation to adopt internal privacy policies, although doing so is also recommended, especially due to Article 50 of the LGPD, which refers to having internal policies in place as a "good practice".

Data Subject Access Rights

Although it is applicable to the use of personal data in the digital environment, the only legislation currently in force that more extensively provides for data subjects' access rights is the Internet Act, which sets forth that the data subject has the right to request the definitive elimination of the personal data provided to a certain internet application at the end of the relationship between the parties, except in cases of mandatory log retention.

Sector-driven legislation also provides for specific rules, such as the Consumer Protection Code, the Access to Information Act (applicable to the public sector), the Tax Code, the Bank Secrecy Act and the Compliant Debtors List Act.

Once the LGPD is in force, data subjects' access rights will be more extensive, since the LGPD explicitly provides for the right to the following:

- confirmation of the existence of the processing activity;
- the access to personal data;

- correction of incomplete or out-of-date information;
- the anonymisation, blocking or deletion of unnecessary or excessive data or data processed contrary to the LGPD;
- the deletion of personal data processed with the consent of the data subject (unless the law provides otherwise); and
- access to information about public and private entities with which the controller has shared data.

Use of Data Pursuant to Anonymisation, De-identification and Pseudonymisation

Brazilian legislation does not provide a definition of de-identification and pseudonymisation, but anonymisation is defined by the LGPD as the "use of reasonable technical means available at the time of processing, by means of which the data loses the possibility of direct or indirect association to an individual." According to the LGPD, anonymised data can be freely processed – ie, the processing does not need to be endorsed on a legal basis, provided that the anonymisation process cannot be reversed with reasonable efforts.

It is also up to the ANPD to regulate standards and techniques to be used in anonymisation processes, and to make verifications about the security thereof.

Restrictions or Allowances

The data subjects have the right to request the review of decisions made based only on the automated processing of personal data that affects their interests, including decisions made in the sense of defining their personal, consumption and credit profile or aspects of their personality. The ANPD will be entitled to audit the automated processing if it suspects the processing is discriminatory.

The Concept of "Injury" or "Harm"

The LGPD does not provide any definition or idea of "harm", apart from the one already stated in the Brazilian Civil Code, according to which one who causes harm to another, by action or omission, commits an illicit act, and is liable therefor. In this sense, indemnification is due from any harm arising from a violation of data privacy rights.

The LGPD reiterates such provision in its Article 42: controllers or processors are liable for any harm caused to data subjects in violation of their rights and their indemnification obligation. The processor will be jointly liable if it violates data protection legislation or acts contrary to the controller's instructions. All controllers directly involved in the violation of data protection rights will also be jointly liable therefor. Additionally, Article 45 provides that the consumerist legislation is applicable when data protection is violated in the consumerist context.

The LGPD sets forth the following liability exception when a controller and/or processor can prove that they did not participate in any of the processing activities, that their participation in the processing activity does not violate any data protection legislation, and that the harm arises exclusively through the data subject's fault.

2.2 Sectoral and Special Issues

The LGPD determines that "sensitive personal data" is "personal data concerning racial or ethnic origin, religious belief, public opinion, association to any trade union or religious organisation, philosophical or political organisation association, data concerning health or sex life, genetic or biometric data, whenever related to a natural person."

According to the LGPD, the processing of sensitive personal data is legitimate only in the following cases.

- When specific and express consent is obtained from the data subject or her/his legal representative, for specific processing purposes.
- If there is no consent from the data subject, when the processing is indispensable for:
  - (a) compliance with a statutory or regulatory obligation by the controller;
  - (b) the joint processing of data when necessary by the public administration for the execution of public policies provided for in laws or regulations;
  - (c) studies by research bodies, ensuring, whenever possible, the anonymisation of the sensitive personal data;
  - (d) the regular exercise of rights, including in contracts, lawsuits and administrative or arbitration proceedings;
  - (e) protecting the life or physical safety of the data subjects or third parties;
  - (f) the protection of health, exclusively in a procedure carried out by health professionals, health services or a health authority; or
  - (g) ensuring the prevention of fraud and the safety of the data subject, in the processes of identification and certification of records in electronic systems, except in the event of the prevalence of fundamental rights and liberties of the data subjects that require protection of the personal data.

Financial Data

Although financial data is not specifically addressed by the LGPD, confidentiality obligations regarding this type of data are provided for in the Brazilian Federal Constitution and the Bank Secrecy Act.

Health Data

The health sector in Brazil is highly regulated, so health data is addressed by different laws and regulations.

Rule No 124/2006 issued by the Brazilian National Supplementary Health Agency (ANVISA) determines that private healthcare services providers must not share data subjects' personal data with third parties without obtaining previous consent, under the penalty of BRL50,000 (approximately USD12,000).

The Code of Medical Ethics, drafted by the Brazilian Federal Medicine Council, sets forth that healthcare professionals must protect patients' data.

Law No 13,787/2018, enacted in December 2018, addresses the digitalisation, retention, storage and handling of patients' records. The law establishes that the records of all patients must be digitalised, and the physical files discarded, unless they have historical value. The digitalised records may be deleted 20 years after the last update.

Furthermore, within clinical trials, ANVISA's Board of Directors Resolution RDC 09/2015 and Resolution No 466/2012 of the National Council of Health provide that the data and privacy of clinical trial participants shall be protected.

With the LGPD in force, health data is being treated as sensitive personal data and the processing thereof is subject to stricter rules, as noted above.

In this sense, the group of pharmaceutical companies (Sindusfarma) created a guideline about data protection, in order to provide companies with general information and sectorial advice on pharmacovigilance.

Communications Data

The Brazilian Federal Constitution provides that the privacy of communications is a fundamental right and, therefore, is granted a special level of protection. The Internet Act also grants the inviolability of the user's communications through the internet, except when supported by 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 their communication and privacy, unless otherwise determined.

The LGPD does not list communications as sensitive data, but they could be considered as such if they contain any of the specific matters considered as sensitive.

Voice Telephony and Text Messaging

Voice communications and text messages are protected under the fundamental right of privacy granted by the Federal Constitution and applicable to communications. In this sense, Law No 9,296/1996 allows for a breach in communication only in cases where such information is needed to help a criminal investigation and is supported by a court order.

Content of Electronic Communications

The same protection granted to private communications is applicable to electronic communications. Additionally, Law No 12737/2012 criminalises the act of hacking electronic devices with the aim of obtaining, modifying, destroying or disclosing data or information without the owner's authorisation.

Children's or Students' Data

The Civil Code and the Child and Adolescent Statute establish 18 years as the legal age, so any act practised by anyone under this age will be null if not preceded by 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.

The LGPD introduced further provisions on the processing of data involving children and adolescents, establishing that such data must be processed in the best interests of the children and must be preceded by obtaining separate consent from one of his or her parents or legal representatives.

There are no provisions involving educational or school data specifically. When related to under-age individuals, the same rules apply as above.

Employment Data

There is no specific law regarding the protection of employees' data. The LGPD only determines that data about participation in trade unions is considered sensitive.

The obligation to respect the privacy of communication – according to the Federal Constitution and Internet Act – is applicable. However, the employer has the right to use technologies to identify content accessed by its employees using workplace devices (eg, corporate e-mail, company's internal systems, etc). In this case, it is recommended that employees are previously informed that the devices used during the employment relationship will be monitored.

Internet, Streaming and Video Issues

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 process-

ing must be preceded by the user's consent and, to do that in a practical way, companies generally use technologies such as cookies (with a warning on the initial screen of their website), beacons, etc. Because much information obtained from users' access to the internet is able to identify them, it should be considered as personal data and, therefore, incurs the same need for consent or other legal basis for processing personal data as under the LGPD.

Additionally, the Internet Act provides an obligation for internet connection and application providers to refrain from disclosing connection, access, personal data and private communications without a supporting court order. Connection records must be kept for one year, while access records must be kept for six months – both periods of time may be increased upon the request of the police authority or the Public Prosecutor's office.

Hate speech, disinformation, abusive material or political manipulation is more relevant to personality rights than data protection rights under Brazilian legislation. There are penalties in the civil and criminal spheres for those who disseminate 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, upon notification by a party (with no need for a court decision).

Data Subject Rights

The Internet Act sets forth that data subjects have the right to request the definitive elimination of the personal data provided to a certain internet application at the end of the relationship between them, except in cases of mandatory log retention.

Sector-driven legislation also provides for specific rules, such as the Consumer Protection Code, the Access to Information Act (applicable to the public sector), the Tax Code, the Bank Secrecy Act and the Compliant Debtors List Act. All these rules are basically founded on the data subject's right to information.

The data subjects' rights are more extensive, since the LGPD explicitly provides for the right to the following:

- confirmation of the existence of the processing activity;
- access to the personal data;
- correction of incomplete or out-of-date information;
- the anonymisation, blocking or deletion of unnecessary or excessive data or data processed contrary to the LGPD;
- the portability of the data to other service providers or suppliers of product, at the express request, in accordance with the regulation of the controlling body, observing the commercial and industrial secrecy;
- the deletion of personal data processed with the consent of the data subject (unless the law provides otherwise);
- access to information about public and private entities with which the controller has shared data;
- access to information on the possibility of denying consent and on the consequences of the denial; and
- revocation of the consent.

Data subjects also have the right to be informed in a clear and ostensive way about:

- the specific purpose of the processing;
- the type and duration of the processing, with commercial and industrial secrecy being observed;
- the identification of the controller;
- the controller's contact information;
- information regarding the shared use of data by the controller and the purpose; and
- the responsibilities of the agents who carry out the processing.

Right to be Forgotten

Currently, there is no specific legislation in Brazil providing for the "right to be forgotten". According to the LGPD, erasure will be one of the statutory rights of data subjects. After the controllers/processors have processed the data, they will need to erase the personal data, 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.

The Brazilian Supreme Court of Justice is deciding about the concept and the boundaries for the application of the right to be forgotten. This decision will provide more legal certainty in cases regarding such matter.

Data Access and Portability

Data subjects have the explicit right to obtain confirmation of the existence of the processing activity, to access the personal data, and to transfer the data to other service providers or suppliers of product, at the express request, in accordance with the regulation of the controlling body, observing commercial and industrial secrecy.

Right of Rectification or Correction

Data subjects have the explicit right to correct incomplete or out-of-date information, and to revoke consent.

2.3 Online Marketing

There is no specific law in Brazil governing online marketing. However, certain legislation may apply, as follows.

Companies must comply with the Brazilian Consumer Defence Code (Law No 8,078/1990 – CDC), which is the general set of rules governing consumerist relations in Brazil. The CDC provides that marketing activities must not be abusive or deceiving and, for this reason, companies should refrain from sending unauthorised marketing communications to customers. There are many official entities responsible for enforcing the rules set forth by the CDC in different levels of the public administration (public prosecutors, local and state PROCONs, public attorneys, police stations and civil organisations for consumer defence), and they are all part of SENACON.

As marketing activities are based on the use of personal information (e-mails and telephone numbers – even if related to a business), the LGPD is also applicable in the sense that the use of e-mails or telephone numbers must also comply with the rules set forth by the LGPD (data subjects' rights, legal basis for processing).

The Internet Act is also applicable to e-mail marketing since it governs the relationships among internet users. It provides for the need of previous and unequivocal consent from data subjects previous to sending e-mail marketing.

Although Brazil does not have a specific e-marketing law, a significant number of Brazilian companies as well as foreign companies doing business in Brazil are members of ABEMD, which is a non-profit entity focused on encouraging, expanding and setting up basic rules related to direct marketing in Brazil. ABEMD issued CAPEM, which is being largely adopted not only by ABEMD members but also by non-members, even though its provisions and resolutions are not binding or mandatory.

Many companies are also members of the National Council of Self-Regulation in Advertising (CONAR), which is a non-governmental entity aimed at promoting freedom of speech and defending constitutional rights applicable to advertising. CONAR has also published a set of rules applicable to advertising activities, the so-called Brazilian Code of Self-Regulation in Advertising (CSRA). Although it has no legal effects since it has not been enacted by a governmental entity, the CSRA is considered a cornerstone in the marketing business by members and non-members, who generally comply with such rules.

SMS/MMS marketing by telecommunications service providers is governed by telecommunication rules, more specifically by Ordinance No 632/2014 issued by ANATEL. Among other provisions, the Ordinance sets forth that the telecommunication services user has the right not to receive marketing messages unless they are preceded by previous, free and unequivocal consent (Article 3, XVIII). Complementary to the Ordinance, through Circular Letter No 39/2012/PVCPR/PVCP, ANATEL sets forth general rules for sending advertising messages using personal mobile telephone services, which require that all companies that send SMS/MMS marketing messages make an opt-out function available to the customer.

2.4 Workplace Privacy

There is no specific law regarding the protection of employees' data. The obligation to respect the privacy of communication applies, according to the Federal Constitution and the Internet Act. However, according to case law on this matter, the employer has the right to use technologies to identify content accessed by its employees using workplace devices (eg, corporate e-mail, company's internal systems, etc). In this case, it is recommended that employees are previously informed that the devices used during the employment relationship will be monitored.

The Role of Labour Organisations or Works Councils

Labour organisations and work councils are not yet sufficiently engaged in privacy protection matters, so there are still no relevant actions from these entities providing for the protection of employees' data. However, as soon as such entities realise the importance of this matter, it is possible that they will include privacy protection clauses in their collective labour agreements or collective labour conventions.

Whistle-Blower Hotlines and Anonymous Reporting

Currently, there is no law in Brazil specifically addressing whistle-blower hotlines or anonymous reporting; there is also no specific reference 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.

E-discovery Issues

There are certain legal procedures that could give rise to an injunction or a court order determining the disclosure of specific data located in servers, if connected to a given criminal investigation or civil lawsuit. Such data is requested by a court or a competent authority, and is disclosed voluntarily by the data controller. Penalties may arise for non-compliance with the court order or the injunction, including daily fines, interruption of services and the imprisonment of corporate officials in Brazil.

Other Issues

There are no specific provisions about digital loss prevention technologies or scanning/blocking websites. The only rule related to digital loss prevention is the obligation to implement minimum standards of security in order to avoid data loss, as set forth by the Internet Act and the LGPD. Except for websites disclosing personal sexual material, the request for blocking websites must be preceded by a court order.

2.5 Enforcement and Litigation

Currently, claims regarding violations of privacy and data protection rights basically arise from the lack of consent to data processing. When it comes to privacy specifically, the standards will also depend on the specifications of the case, according to the Internet Act.

Now that the LGPD is in force, the ANPD must establish standards to claim violations by controllers and/or processors, on the basis of the violation of data subjects' rights according to the law.

Potential Enforcement Penalties

Current administrative penalties established by the Internet Act are as follows:

- warnings, with an 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 acts listed above.

In the case of penalties enforced against a foreign company, any subsidiary, branch office or establishment in Brazil will be jointly liable for the payment of the fines. Such penalties are currently being enforced by the rules of civil liability (Articles 186 and 927 of the Civil Code). Depending on the specifics of each case, additional criminal and civil liabilities may also apply.

The penalties applicable for infringing the LGPD are as follows:

- warnings, with an indication of the time period for adopting corrective measures;
- a simple fine of up to 2% of the revenues in Brazil of a private legal entity, group or conglomerate, for the prior financial year, excluding taxes, up to a total maximum of BRL50 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.

The value of daily fines applied to violations 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. In its agenda for the next two years, the ANPD has already stated it will establish the calculation methodology for administrative fines and the circumstances and conditions to enforce such sanction.

Leading Enforcement Cases

The Public Prosecution has – more than once – opened investigations against the credit bureau SPC Boa Vista, mainly in 2018 and 2019.

In the action, the Public Prosecutor's Office of the Federal District (MPDFT) highlights that Boa Vista SCPC is considered a manager by the Positive Registry Law and, as such, has objective and joint liability for the material and moral damages it causes to those registered on its platforms.

MPDFT is also investigating the data leakage of health data from approximately 16 million patients infected with COVID-19. The information was publicly available for one month after passwords were discovered and enabled the access to such sensitive data. MPDFT is still investigating the case with the Brazilian Ministry of Health and the hospital involved.

Private Litigation

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

Although Brazilian law does not allow class actions as they are known in the United States, if there is a massive data breach the public prosecutor or another specific organisation can initiate an investigation and civil actions against the controller/proces-

sor of data, according to the Public Civil Action Law (Law No 7,347/1993).

Due to the entering into force of the LGPD, private litigation cases are on the rise. The main request is the compensation of moral damages after illegal data processing operations by controllers and processors.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

As a general rule, access to any data requires court authorisation. However, in the case of criminal investigations, Law No 12,850/2013 allows for the public prosecutor or the chief police officer to have access only to the data containing personal qualifications, affiliations and addresses maintained by the electoral justice, telecommunication 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.

Since privacy is safeguarded by the Federal Constitution and the Brazilian Civil Code, every time that law enforcement runs against individuals' privacy rights, it gives rise to a lot of discussion in courts. The Brazilian Supreme Court has ruled that internet service providers of messaging services are not bound to reveal the content of those messages to public authorities. 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

Please see **3.1 Laws and Standards for Access to Data for Serious Crimes**.

3.3 Invoking Foreign Government Obligations

There are currently no obstacles to an organisation invoking a foreign government access request as a legitimate basis to collect and transfer personal data. Under the LGPD, from August 2020, the collection and transfer of personal data upon the request of a foreign authority will only be considered licit if such 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. Since the public is still unaware of its data protection rights (both existing and upcoming), government actions to process additional data from citizens are rarely contested. The upcoming LGPD is likely to change that. In this regard, some caution-inspiring legislation has recently been 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.

Data processing operations carried out by the government must be interpreted under Articles 23 to 32 of the LGPD. The government has to process data based strictly on 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

According to the LGPD, international data transfers are allowed in the following situations:

- 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 interna-

tional 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.

The ANPD's agenda suggests that such topic will be correctly regulated in the first semester of 2022.

4.2 Mechanisms That Apply to International Data Transfers

Please see **4.1 Restrictions on International Data Issues**.

A current best practice adopted by companies is to ensure data is encrypted on an end-to-end basis when it is transferred abroad, to reduce the probability of hacking or leaks.

4.3 Government Notifications and Approvals

According to the LGPD, international data transfers will be allowed under certain circumstances, one of which is the granting of an authorisation by the ANPD.

4.4 Data Localisation Requirements

The Internet Act does not require data to be maintained in the country, so the data can be stored in cloud storage in another country, for example. However, storing the data abroad does not stop the Brazilian law from being applicable. The LGPD does not have any requirements to maintain the data in-country, but the requirements for international transfer (see **4.1 Restrictions on International Data Issues**) will need to be complied with in order 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

International data transfers are allowed 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 co-operation;
- 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 legislation does not provide for blocking statutes specifically related to privacy or data protection.

Generally, as provided for by the Federal Constitution, international treaties, conventions and international acts must be executed by the President and approved by the Congress in order to be valid in Brazil.

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. Such obligation is more explicit with the application of the LGPD, especially due to the principle of necessity.

Automated decision-making entails a right of the data subject to request a review of decisions taken solely on the basis of the automated processing of personal data, including decisions related to the personal, professional, consumer or credit profile and personality.

Data used for profiling can be considered personal data under the LGPD and, therefore, the purpose of processing such data will only be legitimate if it is carried out under one of the legal bases.

Currently, artificial intelligence and the Internet of Things are not addressed by law. Under the LGPD, the ANPD may issue regulations on such matters.

Facial recognition is not currently addressed by law. Under the LGPD, it is highly likely that the face will be considered sensitive personal data, and will therefore be subject to special protection.

Biometric data is considered a type of sensitive personal data and, therefore, will be subject to special protection.

Geolocation is able to identify or make a natural person identifiable, so the requirements of the LGPD are applicable to that processing of data.

The operation of drones is regulated by the 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 and ANATEL. The LGPD does not have any provisions regarding drones.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Although many organisations are starting to implement protocols for digital governance, or fair data practice review boards or committees to address the risks of emerging or disruptive digital technologies, such practice is not legally mandatory. However, with the LGPD in force, data processing agents are obliged to adopt security measures to protect databases, and to 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.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

In January 2021, the database of Serasa Experian (a well-known credit bureau in Brazil) was leaked, and data about 223 million Brazilian citizens was made available. PROCON and SENACON have already notified the bureau for clarification on the matter, but the incident is the most significant security breach in Brazil to date.

5.4 Due Diligence

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

5.5 Public Disclosure

There are no non-privacy/data protection-specific laws that mandate the disclosure of an organisation's cybersecurity risk profile or experience.

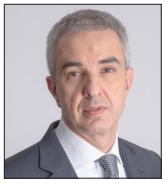
5.6 Other Significant Issues

There are no further significant issues.

Contributed by: Claudio Barbosa, Aline Zinni, Anderson Ribeiro and Larissa Martins
Kasznar Leonardos Intellectual Property

Kasznar Leonardos Intellectual Property provides tailored solutions to the most complex IP issues, both nationally and internationally, with a deep understanding of different cultures and business industries. The team has 22 partners and more than 240 employees, with correspondents in every state of Brazil and a broad international network, and specialises in the management of intellectual assets. The firm acts as legal adviser on contractual matters, as industrial property agent with the Brazilian Patent and Trade Mark Office, and as lawyer, arbitrator and mediator in litigation and extrajudicial dispute resolution. The firm's main areas of practice are patent and trade mark prosecution, industrial designs, regulatory law, life sciences, digital law, marketing and entertainment law, sports law, biodiversity, copyright, unfair competition, plant varieties, technology transfer, geographical indication, trade secrets, franchising and licensing, fashion law, licence compliance and anti-piracy.

Authors



Claudio Barbosa is the senior partner, and head of the firm's Digital Law practice. He is active in IP law and digital and data protection law. Claudio lectures on the Brazilian General Personal Data Protection Law (LGPD) for companies and associations. He advises clients on their Data Protection Law compliance programmes, and advises companies in Brazil on implementing e-commerce, privacy policies and internal policies concerning data protection (including the leading construction material retailer chain and the leading agribusiness information company).

Anderson Ribeiro is a partner at the firm, and co-head of the Life Sciences group. He is active in relation to life sciences, patents, compliance, healthcare and regulatory matters. Anderson is a member of Sindusfarma – Data Protection Task Group, where he lectures about the enactment of the Brazilian Data Protection Law (LGPD) and its implications for the pharmaceutical industry.

Aline Zinni is a senior associate in the Digital Law practice. She advises clients on their Data Protection Law compliance programmes, and advises companies in Brazil and abroad on implementing e-commerce, privacy policies and internal policies concerning data protection, including major players in the social media sector. Aline also lectures on the Brazilian General Personal Data Protection Law (LGPD) for companies and associations.

Larissa Martins is an associate at the firm, who specialises in intellectual property, digital law and data protection. In addition to her law degree, Larissa completed an intensive course on Data Protection at Fundação Getúlio Vargas Law (FGV Law), from September to December 2018 and a postgraduate course on Intellectual Property and New Businesses, from 2019 to 2020.

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