COUNTRY COMPARATIVE GUIDES 2021

The Legal 500 Country Comparative Guides

Brazil

DATA PROTECTION & CYBER SECURITY

Contributing firm

Azevedo Sette Advogados

Ricardo Barretto Ferreira da Silva

Senior Partner | barretto@azevedosette.com.br

Lorena Pretti Serraglio

Senior Lawyer |

Camilla Lopes Chicaroni

Associate |

Nariman Ferdinian Gonzales

Associate |

Isabella da Penha Lopes Santana

Associate |

This country-specific Q&A provides an overview of data protection & cyber security laws and regulations applicable in Brazil.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

BRAZIL
DATA PROTECTION & CYBER SECURITY

The firm would also like to thank Mariana de Carvalho Rici and Lais Litran Motta for their contribution to this chapter.

1. Please provide an overview of the legal and regulatory framework governing privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws)?

The Brazilian Federal Constitution sets forth the core principles on the protection of privacy and personal information. According to the Constitution, privacy, private life, honor, and image of individuals are inviolable, and the right to be compensated for economic and moral damages resulting from violation thereof is ensured.

Brazil enacted, in August 2018, the General Data Protection Act (Law No 13,709/2018 – "LGPD"), which most of its provisions came into force in September 2020, following legislative and executive discussions on the issue. The articles that provide for the administrative sanctions applicable to non-compliance agents will come into force in August 2021, through Law No. 14,010/2020.

LGPD provides a wide regulation for personal data protection, including collection, storage, registration, monitoring, processing, and disclosure of users' personal data. The law requires that personal data processing activities comply with several principles, such as purpose, transparency, security, free access by the data subject, prevention of damages, and non-discrimination.

Besides, two bills are going through the House of Representatives, which intend to change the effective date of the administrative sanctions of the LGPD. The first of them, Bill No. 500/2021 was presented in February and intends to postpone the effectiveness of the financial sanctions of LGPD until January 1, 2022, for the reasons of the pandemic context and its impact on the society and economy. At the beginning of March 2021, it was presented Bill No. 578/2021 which intends to impose LGPD sanctions immediately, under the reasons of a data breach that occurred in Brazil, with leakage of millions of data subjects' information and the formation and performance of the ANPD, which would be ready to apply the applicable sanctions. Both Bills are awaiting further legislative action.

The National Data Protection Authority – "ANPD", the body responsible for interpreting and enforcing compliance with the LGPD has already been formed and is operating in the Brazilian jurisdiction. At the end of January 2021, the ANPD made public its initial regulatory agenda, through Decree No. 11, which placed as a priority an educational and regulatory agenda, with the provision of important issues in the privacy and data protection scenario such as small and medium-sized enterprises, rights of data subjects, administrative sanctions, communications on security incidents, among others.

At the end of March, 2021, the ANPD also updated its communiqué on data breaches, which includes provisions such as the concept of a data breach, actions that must be taken by the controller, recommendations for information in data breach notifications, recommended deadline for communication, a model form of notification to ANPD, among others. Currently, one of the most important sectoral laws is the Brazilian Civil Rights Framework for the Internet (Law No. 12.965/2014, the "Internet Law") which establishes principles, guarantees, rights, and obligations for the use of the Internet in Brazil. Besides, Decree No. 8,771 of May 11, 2016, which regulates the Internet Law, sets forth the rules related to the request of registration data by public administration authorities, as well as the security and confidentiality of records, personal data,

and private communications.

There are other sectorial laws and regulations concerning rights to privacy and data protection, including, but not limited to:

- Civil Code (Law No. 10,406/2002) grants general privacy rights to any individual and the right to claim against any attempt to breach such rights by any third party;
- Consumer Code (Law No. 8,078/1990) provides for the principles of transparency, information, and quality of data on its provisions;
- Positive Credit Registry Act (Law No. 12,414/2011) permits databases of 'positive' credit information (i.e., fulfillment of contracted obligations) but prohibits the registry of excessive information (i.e., personal data which is not necessary for analyzing the credit risk) and sensitive data;
- Complementary Law No. 166/2019 that amends the Positive Credit Registry Act, authorizing the inclusion of natural persons and legal entities in positive registration databases, without their prior request;
- Telecommunications Act (Law No. 9,472/1997) grants privacy rights to consumers about telecommunications services;
- Wiretap Act (Law No. 9,296/1996) establishes that interception of communications can only occur by court order upon request by police authorities and the Public Prosecutor's Office for purposes of criminal investigation or discovery in criminal proceedings;
- Bank Secrecy Act (Complementary Law No. 105/2001) requires that financial institutions (and similar entities) hold financial data of individuals and entities in secrecy, except under judicial order issued for purposes of investigation of any illegal acts or discovery in criminal proceedings;
- Resolution 3/2009 of the Internet Steering Committee in Brazil (CGI.br), establishes principles for ensuring privacy and data protection on the use of the internet in Brazil, mainly regarding activities developed by internet service providers;
- Resolution 124/2006 of the National Supplementary Health Agency imposes a fine on health insurance companies up to BRL 50,000 for the breach of personal information related to the health conditions of a patient;
- Law No. 13,989/2020. Provides for the use of telemedicine during the COVID-19 crisis. The law for the use of telemedicine after the pandemic context is already being studied by the Federal Council of Medicine that intends to elaborate an ethical, technical, and safe law to provide adequate practice of telemedicine in Brazil, considering the privacy and data protection for both parts (patients and doctors).
- Resolution of the Brazilian Central Bank No. 1 of 2020. Establishes the Pix payment arrangement and approves its Regulation that provides for the need to obtain the formal consent from users for the registration of keys and use of the instant payment method.
- Joint Resolution of the Brazilian Central Bank and the National Monetary Council No. 1 of 2020. Provides for the implementation of the Open Banking, which brings privacy and data security as one of the goals of Open Banking, and also imposes obtaining formal consent from users;
- National Monetary Council Resolution No. 4,865 and Brazilian Central Bank Resolution No. 29 of 2020. Establish the guidelines for the operation of the Controlled Test Environment for Financial and Payment Innovations (Regulatory Sandbox) and the conditions for the supply of products and services in the context of this environment within the National Financial System. Both resolutions bring privacy as one of the objectives and guidelines of the Regulatory Sandbox.
- Law No. 14,129/2021. Provides for principles, rules, and instruments for Digital Government and the increase of public efficiency, and foresees data protection and privacy as a governmental principle, mentioning the compliance with LGPD.
- National Monetary Council Resolution No. 4,883 of 2021. Provides for the cybersecurity policy and the requirements for contracting data processing and storage and cloud computing services to be observed by institutions authorized to operate by the Brazilian Central Bank.

There are also important laws under the Brazilian Congress' analysis, like the Proposal for Constitutional Amendment No. 17/2019, which complements item XII of article 5 and adds item XXX to article 22 of the Brazilian Federal Constitution to include protection of personal data within the citizens' fundamental rights and to set the Union's exclusive jurisdiction to legislate about this subject.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

Brazilian law does not require any prior licensing or registration for data processing activity. On the other hand, companies are required to get licenses/authorizations to be issued by the competent regulatory agencies as regards, for example, the provision of telecommunication, banking, health, and other regulated activities/services. Those are the so-called regulated service sectors.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

The LGPD defines:

- Personal data as information regarding an identified or identifiable natural person;
- Sensitive information such as personal data concerning racial or ethnic origin, religious beliefs, political opinions, philosophical membership of trade unions or religious, philosophical or political organizations, data concerning health or sex life, genetic or biometric data, when related to a natural person.

Other key definitions are:

- Data subject: a natural person to whom the personal data object of processing refers to;
- Data controller: natural person or legal entity, of public or private law, responsible for making decisions about the processing of personal data;
- Data processor: natural person or legal entity, of public or private law, that processes personal data in the name of the controller;
- Data protection officer: person appointed by the controller and the processor, who acts as a channel of communication between the controller and the data subjects and the supervisory authority;
- Processing agents: data controller and data processor;
- Processing: any operation carried out with personal data, including, but not limited to, those concerning collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, assessment or control of information, modification, communication, transfer, dissemination or extraction;
- ANPD: agency of the public administration responsible for supervising, implementing and monitoring compliance with this Law in the national territory.

4. What are the principles related to, the general processing of personal data or PII?

Every processing activity of personal data shall observe good faith and the following principles: i) purpose; ii) adequacy; iii) necessity; iv) free access; v) quality of the data; vi) transparency; vii) security; viii) prevention; ix) non-discrimination; and x) accountability.

Also, the LGPD establishes that processing of personal data shall only be carried out in the following cases:

- By means of the data subject's consent;
- For compliance with legal or regulatory obligation by the controller;
- By the public administration for the processing and shared use of data required for the implementation of public policies;
- For the conduction of studies by research entities, ensuring, whenever possible, the anonymization of personal data;
- When necessary for the performance of a contract or preliminary proceedings related to a contract to which the data subject is a party, at the request of the data subject;
- For the regular exercise of rights in judicial, administrative or arbitral procedures;
- For the protection of the life or physical safety of the data subject or a third party;
- For the protection of health, in procedures carried out by health professionals or sanitary entities;
- When necessary to serve the legitimate interests of the controller or of third parties, except in the event of prevalence of fundamental rights and liberties of the data subject, which requires protection of the personal data;
- When the fundamental rights and liberties of the data subject requires personal data protection;
- For credit protection including provisions of relevant legislation.

The personal data shall be eliminated after termination

of the processing thereof, within the scope and technical limits of the activities. The storage of personal data after the processing is authorized for the following purposes:

- Compliance with a legal or regulatory obligation by the controller;
- Study by a research entity, ensuring, whenever possible, the anonymization of the personal data;
- Transfer to third parties, provided that all legal requirements set forth in the Law are complied with;
- Exclusive use of the controller, with forbidden access to third parties, and provided the data has been anonymized.

In addition, sectoral legislation, such as the Consumer Code, National Tax Code, Labor Legislation, among others, provides different rules regarding data storage.

Specifically for internet application, the Internet Law establishes that application service providers must keep records of internet access (*i.e.*, the set of information regarding date and time of use of a particular internet application from a particular IP address) applications under secrecy, in a controlled and safe environment, for a minimum term of six months and in the provision of internet connections, the autonomous system administrator shall keep records of the connection logs under secrecy for at least one year.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII and, if so, are there are rules relating to the form, content and administration of such consent?

Consent is one of the legal bases provided in the LGPD to process personal data and has specific rules to its use. In this regard, for example, when we are processing personal data, consent must be a free, informed and unambiguous manifestation by the data subject for a specific purpose, given in writing or by another means that demonstrates his/her manifestation of will; on the other hand, the processing of sensitive personal data requires a specific and highlighted consent, for specific purposes.

If consent is provided in writing, the contractual clause must appear highlighted from the other contractual clauses. Additionally, to process child and adolescent data as well, at least one of the parents or legal representative shall give his/her specific and highlighted consent.

Also, one of the mechanisms that allow international transfers is the specific and highlighted consent given by the data subject, with prior information about the international nature of the operation, being clearly distinct from other purposes.

Finally, in cases where the processing of personal data is based on consent, LGPD establishes that the consent can be revoked at any time by the data subject, by means of an express, free and facilitated procedure.

The LGPD also determines that the data subject can require the erasure of personal data processed with the data subject consent, unless the processing occurs under the following conditions:

- compliance with legal or regulatory obligation by the data controller;
- studies by a research body, subject to anonymization of personal data, whenever possible;
- transfer to third parties, subject to compliance with data processing requirements; or
- for exclusive use by the data controller, with no access by third parties and provided such data is anonymized.

6. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

According to the LGPD, it is not prohibited to collect and process sensitive personal information. However, the processing of sensitive personal data may only occur if the data subject or his/her legal representative consents, in a specific and highlighted way, for such specific purposes. Without the data subjects' consent, the processing of sensitive personal data must follow one of the events listed below, whenever it is indispensable:

- For compliance with legal or regulatory obligation by the controller;
- By the public administration for the processing and shared use of data required for the execution of public policies;
- For the conduction of studies by research entities, ensuring, whenever possible, the anonymization of personal data;
- When necessary for the performance of a contract or the regular exercise of rights in judicial, administrative or arbitral procedures;
- For the protection of the life or physical safety of the data subject or a third party;
- For the protection of health, in procedures carried out by health professionals or by

health entities;
- For the guarantee of the prevention of fraud and safety of the data subjects, in processes of identification and authentication of registration in electronic systems, observing the data subject rights, and except in the event of prevalence of fundamental rights and liberties of data subjects that require protection of personal data.

7. How do the laws in your jurisdiction address children's personal data or PII?

According to the Child and Adolescent Statute (Law 8,069/1990 – "ECA"), children and adolescents have a peculiar condition of being in development. In this sense, the LGPD gives them stricter data protection rules and determines that processing of personal data belonging to children and adolescents shall be done in their best interest, pursuant to the rules below and applicable legislation.

Accordingly, the LGPD set forth the following rules to process children's and adolescents' personal data:

- The processing of children's and adolescents' personal data requires specific and highlighted consent of at least one of the parents or by the legal guardian;
- When processing data based on consent, controllers shall keep public the information on the types of data collected, the way it is used and the procedures for exercising the rights established in the LGPD;
- Children's and adolescents' personal data may be collected without consent when it is necessary to contact the parents or legal guardian, used only once and without storage, or for the children's protection. Under no circumstances shall the data be transferred to third parties without the proper consent;
- Data controllers shall not condition the participation of data subjects in games, internet applications or other activities to the provision of personal information beyond what is strictly necessary for the activity;
- The controller shall make all reasonable efforts to verify that the person responsible for the child or adolescent has given the consent, considering the available technologies;
- Information on the processing of children's and adolescents' data shall be provided in a simple, clear and accessible manner, taking into account the physical-motor, perceptual, sensory, intellectual and mental characteristics of the user, with the use of audiovisual resources when appropriate, in order to provide the necessary information to the parents or legal guardian and appropriate to the understanding of the child.

8. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

The LGPD does not apply to the processing of personal data:

- Carried out by a natural person for strictly personal and non-economic purposes;
- Carried out exclusively for journalistic, artistic or academic purposes;
- Carried out exclusively for purposes of public safety, national defense, state security, or activities of investigation and prosecution of criminal offenses;
- Originated from outside the national territory and which are not the object of communication, shared use of data with Brazilian processing agents or subject to international transfer of data with another country that is not the country of origin, provided that the country of origin has a level of personal data protection suitable for the provisions of LGPD.

9. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

The LGDP establishes that processing agents shall adopt security, technical and administrative measures able to protect the personal data from unauthorized access and accidental or unlawful situations from the design phase of the product or service until its implementation.

The concept of privacy by default is implicit in the LGPD as companies are subject to the following principles, among others:

- Purpose: processing for legitimate, specific and explicit purposes, previously informed to the data subject, with no possibility of subsequent processing incompatible with these purposes;

- Necessity: limitation of the processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportional and non-excessive in relation to the purposes of the data processing.
- Accountability: demonstration by the processing agent of the adoption of effective measures capable of proving compliance with the rules of personal data protection and its enforcement, including the effectiveness of such measures.

Business typically meet these requirements through an adequacy program, where they need to: i) keep records of personal data processing operations carried out by them; ii) prepare a Data Protection Impact Assessment (DPIA), with a description of the types of data collected, the methodology used for collection and for ensuring the security of information and the analysis by the controller regarding the adopted technical and administrative measures, safeguards and mechanisms of risk mitigation; and iii) adopt good practices of privacy and be transparent.

The ANPD may provide for minimum technical standards to render applicable the provisions of LGPD, taking into consideration the nature of the information processed, specific data processing characteristics and the available technology, in particular in case of sensitive personal data.

10. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

Both the controller and the operator must keep records of the personal data processing operations they carry out, especially when based on legitimate interest. Also, it is highly recommendable to the controllers and operators to have an updated data mapping, to present a Data Protection Impact Assessment (DPIA) whenever required, complying with the principle of accountability.

This topic may be complemented by the LGPD Good Practices Guideline that will be issued by ANPD or in the Guidelines for the Rights of data subjects, both part of the phase three of ANPD's regulatory agenda (to be conducted within 2 years), as established by the Ordinance No. 11 of January 27, 2021.

11. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

There is no legal provision requiring or recommending consultation with regulators to process personal data. However, according to LGPD, it is possible to consult with the data privacy regulators about questions and queries regarding personal data. It is also possible for the data subject to petition against the controller before the ANPD, regarding his/her personal data, after proving that the complaint was not solved within the legal term.

The ANPD is already in operation and has a communication channel available at the website *https://www.gov.br/anpd/pt-br/canais_atendimento*.

12. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

ANPD may require that the controller must prepare a data protection impact assessment (DPIA), including sensitive data, referring to its data processing operations, in accordance with regulations, with due regard for trade and industrial secrets. According to the LGPD, the DPIA shall contain the description of all personal data processes that could generate risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms to mitigate these risks.

Also, when processing is based on the legitimate interest, it must be carried out in accordance with the processing of data strictly necessary for legitimate purposes, considered from concrete situations, therefore, the National Authority may request for the controller a data protection impact assessment (DPIA).

Finally, the matter will also be the object of a resolution to be issued by the ANPD, according to its regulatory agenda, scheduled for the first half of 2021.

13. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

According to the LGPD, the controller shall nominate a data protection officer. The identity and contact

information of the DPO shall be publicly disclosed, in a clear and objective manner, preferably on the controller's website. Although LGPD does not impose the nomination as an obligation to the processors, they also may appoint a DPO, according to Article 5, VIII.

The activities of the data protection officer consist of:

- Accept complaints and communications from data subjects, provide clarifications and adopt measures;
- Receive communications from the National Authority and adopt measures;
- Guide employees and contractors regarding the practices to be taken in relation to the protection of personal data;
- Perform other duties determined by the controller or established in complementary rules.

In addition, the National Authority may establish complementary rules about the definition and attributions of the data protection officer. The Authority will determine cases of waiving the need of a data protection officer, according to the nature and size of the entity or the volume of data processing operations, as defined by its agenda for the first half of 2022.

14. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).

Yes. The data subject has the right to easy access of the information about the processing of his or her data, which should be provided in a clear, adequate and ostensible manner concerning it, including other aspects provided for in regulations for compliance with the principle of free access, such as:

- The specific purpose of processing;
- Form and duration of the processing, observing business and industrial secrets;
- Data controller identification;
- Information about the shared use of data by the controller and for which purpose;
- Responsibilities of the agents that will carry out the processing;
- Rights of the data subject, explicitly mentioning the rights provided in the LGPD.

If there is a change about specific purposes of the processing, type or duration of the processing, identification of the controller and information regarding the shared use of data, the controller shall inform the data subject, with a specific highlight of the content of the changes. In the cases in which the legal basis of the processing is consent, whenever there are changes in the purposes of the processing of personal data that are not compatible with the original consent, the controller shall previously inform the data subject of the changes of the purpose, and the data subject may revoke the consent whenever there may exist disagreements with the changes.

Also, if the processing of personal data is a condition for the supply of a product, the provision of a service or the exercise of a right, the data subject shall be informed of this fact and of the means by which the exercise of the rights set forth in the LGDP may be carried on.

ANPD is supposed to regulate on data subject's rights by the first half of 2022, which might add some rules to the notice requirements imposed on businesses in Brazil.

15. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (E.g. are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

LGPD defines controllers and processor as "processing agents" and distinguishes their concepts. A data controller is a natural person or legal entity of public or private law that has the competence to make decisions regarding the processing of personal data and the data processor is a natural person or legal entity of public or private law that processes personal data on behalf of the controller.

Furthermore, LGPD foresees that the processor shall carry out the processing according to the instructions provided by the controller, which shall verify compliance of its own instructions and the rules governing the matter.

The Brazilian Data Protection Act also set the responsibility of the controller or the processor who, as a result of carrying out activities of processing personal data, causes material, moral, individual or collective damage to others, in violation of the data protection legislation shall redress/repair it.

The data processor is jointly liable for any damages caused by the processing if it fails to comply with the

obligations of the data controller, or fails to follow the lawful instructions of the controller in which case the processor is deemed equivalent to the controller, except if they prove that:

- They did not carry out the processing of personal data that is attributed to them;
- Although they carried out the personal data processing attributed to them, there was no violation of the data protection law;
- The damage results from the exclusive fault of the data subject or any third party.

At last, the controller or the processor who neglects to adopt security information measures foreseen in the law shall be held liable for the damages caused by the violation of the data security, like data breaches.

16. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g. due diligence or privacy and security assessments)?

There is no legal provision requiring minimum contract terms or other restrictions related to hiring service providers. Companies shall negotiate contract limits and restrictions between themselves. Nonetheless, the LGPD provides general guidelines related to security issues for data processors and data controllers and establishes that this matter can be further regulated by the national authority.

According to LGPD, the service providers (Controllers and Processors) may formulate rules for good practice and governance that set forth conditions of organization, procedures, complaints, and petitions for data subjects, technical standards, and specific obligations for the involved parties, among others.

Also, when creating these rules, the controller and the processor should consider some items in the moment of the creation and implementation of good practice rules and data governance, regarding the data processing, as nature, scope, purpose, probability, and the risks and benefits that will result from the processing of data subject's data.

The ANPD has made public its strategic planning for the period of 2021-2023 and according to this planning, one of the priorities is educational. The Authority has undertaken to engage in dialogue with governmental and non-governmental bodies to produce guides and educational materials with best practice recommendations on personal data protection. These discussions may or may not result in recommendations on minimum contract terms with processors.

These discussions might also be reflected in the LGPD Good Practices Guideline, which shall be issued by the ANPD by the second half of 2022, according to the phase three of the Authority's regulatory agenda (to be conducted within 2 years).

17. Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

There is no definition or specific regulation for tracking technologies, such as 'cookies' in Brazil, However, if the information gathered by any tracking technology is able to identify a natural person, it falls within the scope of the LGPD.

In attention to the principle of transparency, provided for in Article 6, item VI of the LGPD, the controller must inform the data subject about the use of tracking technologies on its websites and/or applications, explaining what each of them are for. In the specific case of cookies, all types must be listed.

The data subject's consent to each of the applicable tracking technologies should be collected in a segmented manner and they should be duly informed of the consequences of withholding consent, according to Article 18, item VIII of the LGPD.

18. Please describe any laws in your jurisdiction addressing email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

Although there is no legal rule concerning *spam*, the Internet Steering Committee (CGI.br) provides a guideline of good practices to avoid *spam*, as follows:

- To send e-mails only to customers who have opted for registration in the mailing list;
- Do not use third-party disclosure lists, or buy them from mailing lists sellers;
- Do not reuse disclosure lists, i.e. do not send e-mails to customers registered on mailing lists from another service, even if they are from the same company;

- To respect customers' options given by registration forms, in writing or online;
- To respect a consumer's option to be unsubscribed from the mailing list;
- Do not start the first contact with customers by e-mail, i.e. sending the first e-mail without prior authorization characterizes the practice of *spam*.

Additionally, Brazil has a Self-Regulation Code for E-mail Marketing Practice – CAPEM signed by representative entities of marketing companies, internet service providers and consumers. The Code authorizes e-mail marketing when the recipient has so requested (opt-in) or upon evidence that the sender has a previous relationship with the recipient, whether commercial or social (soft opt-in) and regardless of the recipient's express consent. Up to this moment, we have not had any Court decision or ANPD's analysis on which practice should prevail, so the market has adopted a more conservative practice.

Some other rules of CAPEM Code are also worth highlighting, such as (i) the prohibition of using third-party domains for e-mail marketing; and (ii) the prohibition of sending a first e-mail so that the recipient opts-in the mailing list and, by doing so, authorizes the receipt of the following e-mails.

The Brazilian Council of Advertising Self-Regulation – CONAR, which also has influence on the sending of e-mail marketing, stablishes that the policies and good practices adopted to offline advertising are also applicable to online advertising.

Lastly, it bears mentioning that Law No. 13,226/2008, enacted by the State of São Paulo, creates a registration list for blocking telemarketing calls with the purpose of preventing companies making marketing calls not authorized by the consumer.

19. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

The Brazilian Data Protection Act foresees biometrics data as a sensitive category of personal data. The law considers as sensitive any data related to racial or ethnic origin, religious beliefs, political opinions, philosophical membership of trade unions or religious, philosophical or political organizations, data concerning health or sexual life, genetic or biometric data, when related to a natural person.

The processing of biometric data shall observe the specific list of legal basis and other provisions, because of the high risk that the processing of this category of personal data poses to data subjects' fundamental rights.

There is still no specific law about facial recognition in Brazil, but there are some Bills under discussion by the House of Representatives.

One of these, is Bill No. 2537 of 2019, which obliges all commercial establishments that use facial recognition software to alert consumers with signs or stickers fixed at the entrance of their facilities. If approved by the House of Representatives, this Bill will be submitted to the Federal Senate for analysis.

Another one is Bill No. 4612 of 2019, that intends to regulate the development, application, and use of facial and emotional recognition technologies, as well as other digital technologies aimed at the identification of individuals and behavior prediction or analysis. This project is still proceeding in the House of Representatives and, if approved, has the potential to complement the provisions of biometric data in the Brazilian legislation, in special, LGPD. The most recent bill pending in the National Congress on this subject is Bill No. 572/2021, presented on February 24, 2021 and suggests the creation of the National Database for Facial and Digital Recognition.

20. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does cross-border transfer of personal data or PII require notification to or authorization form a regulator?)

LGPD regulates transfer of data outside jurisdiction. According to Article 33 of the LGPD, the international transfer of personal data is only allowed in the following cases:

- To countries or international organizations that provide a level of protection of personal data that is adequate to the provisions of the LGPD;
- When the controller offers and proves guarantee of compliance with the principles, rights of the data subject and the regime of data protection established in the LGPD, in

the form of:

a. Specific contractual clauses for a given transfer;
b. Standard contractual clauses;
c. Global corporate rules;
d. Regularly issued stamps, certificates and codes of conduct;

- When the transfer is necessary for international legal cooperation between public intelligence and investigation bodies, in accordance with instruments of international law;
- When the transfer is necessary for the protection of the data subject's or a third party's life or physical safety;
- When the National authority authorizes the transfer;
- When the transfer is the result of a commitment assumed in an international cooperation agreement;
- When the transfer is necessary for the execution of a public policy or legal attribution of a public service;
- When the data subject has provided specific and highlighted consent for international data transfer, with prior information about the international nature of the operation, with this information being clearly distinct from other purposes;
- For compliance with legal or regulatory obligation by the controller, when necessary for the performance of a contract or preliminary proceedings related to a contract to which the data subject is a party, at the request of the data subject and for the regular exercise of rights in judicial, administrative or arbitral procedures.

Although the articles related to international data transfer of LGPD is in full force since September 2020, the efficacy of some of its provisions requires regulation by the ANDP. This is the case for some of the provisions on international data transfer, such as standard contractual clauses and global corporate rules.

Aware of these gaps in the LGPD, the ANPD has included international data transfers in its regulatory agenda's phase two (to be conducted within a year and a half). Among the main objectives of the Authority, we highlight, without prejudice to other regulations, (i) the definition of which countries or places will be considered with "an adequate level of data protection"; (ii) the creation of standard contractual clauses; and (iii) the verification of standard contractual clauses.

21. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

The LGPD establishes that processing agents shall adopt security, technical and administrative measures able to protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing.

Under LGPD, ANPD can establish minimum technical standards to make the provisions above applicable, taking into account the nature of the processed information, the specific characteristics of the processing and the current state of technology, especially in the case of sensitive personal data, as well as the data protection principles. From February 22 to March 24 2021, ANPD carried out a public consultation in order to receive relevant subsidies from civil society regarding notifications of security incidents. Although there is no regulation up to this moment, ANPD has released, on March 31, 2021, a public note with guidelines and a form to notify this body in case of an incident. The controllers and processors shall ensure the security of the information as provided for in the LGPD, even when the processing is over. Besides, the software or systems used for processing personal data shall be structured to be in compliance with the security requirements, standards of good practice and governance, general data protection principles and other sectorial regulatory rules.

Also, the Internet Act provides security requirements for internet service providers. Decree 8.771/2016 provides the security standards for handling personal data and private communications, as follow:

- Definition of responsibilities and authentication mechanisms so as to ensure individualization of the persons who will have access to and handle data, as well as detailed access logs;
- Creation of detailed inventory of access to connection records and access to applications containing time, duration, identity of the designated employee or individual responsible for the access in the company and the accessed file; and
- Management solutions of records through techniques that ensure the inviolability of data, such as the use of encryption or equivalent protection measures. The safeguard and availability of connection logs and access data, as well as PII and the

content of private communications, must meet the security requirements to preserve intimacy, privacy and image of the parties directly or indirectly involved.

Moreover, the Brazilian Central Bank issued Resolution 4.658/2018, which provides a cyber-security policy and the requirements for contracting services of data processing, data storage and cloud computing to be observed by financial institutions and other institutions licensed by the Brazilian Central Bank.

22. Do the laws in your jurisdiction address security breaches and, if so, how does the law define “security breach”?

Although the LGPD does not provide a definition of “security breach”, it addresses the issue.

Generally, any security incident that may result in any relevant risk or damage to the data subjects may be considered a “security breach” and the data controller must communicate to the National Authority and the data subject about it, within a reasonable period.

On March 31, the ANPD released a note in which the most recent definition of a security incident is: any adverse event, confirmed or suspected, related to the breach in the security of personal data, such as unauthorized, accidental or unlawful access that results in destruction, loss, alteration, leakage or in any way inadequate or unlawful data processing, which may cause risk to the rights and freedoms of the data subject.

23. Does your jurisdiction impose specific security requirements on certain sectors or industries (e.g. telecoms, infrastructure)?

There are several sectorial laws and regulations concerning security requirements for specific regulated sectors and industries, such as, but not limited to:

- The Brazilian Civil Rights Framework (Law 12.965/2014, the “Internet Law”), which provides security requirements for internet service providers, and the Decree 8.771/2016, that provides security standards for handling personal data and private communications for internet service providers;
- Cybersecurity Regulation Applied to the Telecommunications Sector of the National Agency for Telecommunications – ANATEL which aims to establish conducts and procedures for the promotion of security in telecommunications networks and services, including cybersecurity and the protection of critical telecommunications infrastructures. The regulation was approved on December 17, 2020 and is in force since January 4, 2021, with a 180-day deadline for adequacy and implementation of service provider companies.
- Decree 9.637/2018, which institutes the National Information Security Policy and provides for the governance of information security, and the Normative Ruling 4/2020 of the Institutional Security Office, which provides on the minimum requirements cyber security requirements to be adopted when establishing 5G networks;
- Decree 9.573/2018, which approves the National Critical Infrastructure Security Policy, and the Decree 10.222/2020, which approves the National Strategy of Cyber Security;
- Complementary Law 105/01, which provides for the secrecy of operations in financial institutions, the Resolution 3.380/06 of the Brazilian Central Bank, which provides on the implementation of an operational risk management structure for financial institutions, and the Resolution 4.658/2018 of BACEN , which provides on the cyber security policy and the requirements for hiring data processing and storage services and cloud computing to be observed by financial institutions and other institutions authorized to operate by BACEN;
- Ordinance 271/2017, which provides the Information Security and Communications Policy of the Ministry of Health (POSIC/MS), and Ordinance 1.966/18, which defines information and communication security standards within the Ministry of Health;
- Provisional Measure No. 2.200-2/01, which establishes the Brazilian Public Key Infrastructure – ICP-Brazil, to ensure the authenticity, integrity and legal validity of documents in electronic form, support applications and qualified applications that use digital certificates, as well as secure electronic transactions;
- Circular 249/04 and 285/05 of the Superintendence of Private Insurance – SUSEP, which determine internal controls of activities and information systems insurance companies, capitalization companies and public pension entities and establish information security policy requirements, as well as Circular 599/2020 of SUSEP, which establishes that the request for accreditation

by an entity registering insurance operations, open supplementary pension, capitalization and reinsurance must present an executive summary of data secrecy and cyber security policies and a declaration that these policies comply with the legislation and regulations in force;
- Resolution 656/15 of the National Telecommunications Agency (Anatel), which establishes standards on Risk Management of Telecommunications Networks and Use of Telecommunications Services in Disasters, Emergency Situations and Public Disaster;
- NBR ISO/IEC 27001 and 27002 approved in 2013 by the Brazilian Association of Technical Standards (ABNT), which provide on security techniques, information security management systems and Code of practice for information security management.
- Resolution 124/2006 of the National Supplementary Health Agency imposes a fine on health insurance companies up to BRL 50,000.00 for the breach of personal information related to the health conditions of a patient, as mentioned above.

24. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

As mentioned above, ANPD has released, on March 31, 2021, a public note with guidelines and a form to notify this body in case of an incident. The guidelines point out that in case of an incident (including a data breach):

i. the incident should be assessed internally, regarding the nature, category and quantity of data and data subjects affected, also concrete and probable consequences;
ii. the Data Protection Officer should be notified;
iii. the PII owner/controller should be informed, in case of being a processor;
iv. the ANPD and the data subject should be notified in case of potential or relevant damage; and
v. an internal report should be carried out, assessing the incident, the measures taken and a risk analysis, in order to comply with the principle of accountability.

According to the guidelines and article 48 of LGPD, the PII owner/controller is responsible for notifying ANPD and the data subject. This document also recommends that controllers adopt a cautious position, so that the communication is render even in cases in which there is doubt about the relevance of the risks and damages involved. Although the responsibility and obligation for communication to the ANPD rests with the controller, if information is exceptionally presented by the processor, it will be duly examined by ANPD.

In order to evaluate the relevance of the potential risk of damage to data subjects, the document presents two questions that should be answered by the controller when analyzing the incident:

1) Has there been a security incident related to personal data? If not, it is not necessary to notify ANPD. If yes, the next question should be answered.

2) Is there a relevant risk or damage to the individual rights and freedoms of the affected data subjects as a result of the security incident? If yes, ANPD and data subject should be notified. If not, the notification will not be necessary if the controller can demonstrate, in an irrefutable way, that the incident does not constitute a relevant risk to the rights and freedoms of the data subjects.

The notification must contain clear and concise information. It is recommended, in these guidelines, that the document comprehends at least the identification and contact details of: the entity or person responsible for the processing activity; the Data Protection Officer or other contact person; the indication of whether the notification is complete or partial – and, in this last case, if it is a preliminary communication or a complementary communication. It should also contain information about the incident, such as the circumstances in which it occurred, a description of the personal data and information affected, potential consequences, the pre-existent and also implemented measures, among others.

Finally, the public note addresses that, while the regulation is pending, it is recommended to notify ANPD within a period of 2 working days, counted from the date of awareness of the incident. Additionally, the Special Unit for Data Protection and Artificial Intelligence (ESPEC), linked to the Federal Public Prosecutors Office, suggests companies to notify data breaches. For this purpose, the Commission provides a webpage where companies can communicate security incidents and breaches of personal data.

Also, the Brazilian Computer Emergency Response Team (CERT.br) presents some recommendations for the notification of security incidents, giving guidance about what to notify, who to notify, formats for the notification,

among other instructions.

25. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

Brazil does not have a unique legislation about how to deal with cybercrimes, presenting sectorial laws on various subjects.

In this regard, Law 12,737/12 amended the Brazilian Criminal Code (Decree-Law 2,848/1940) and provided for the criminal classification of computer-related crimes, such as the intrusion of a computing device, for example.

In the same way, Law 12,735/12 determined the installation of police stations and specialized teams to combat digital crimes. In conjunction with the police stations specialized in cybercrime, there are non-governmental institutions that work in partnership with the Government and the Public Prosecutor's Office to combat cybercrime, such as SaferNet Brazil, which offers a service for receiving anonymous reports of crimes and violations against Human Rights on the Internet.

Other normative instruments can be nominated, such as Law 11,829/08, which institutes the crime of child pornography on the Internet, and Law 13,.185/15, which establishes a mandatory program to fight the cyberbullying.

Also, the Bill 154/2019, which amends the Brazilian Criminal Code to establish a generic aggravating factor for cybercrimes, due to the extended range of the practice, is being discussed in the House of Representatives.

The payment of ransoms in ransomware attacks and other cybercrimes related to money laundering, financial pyramids, crimes related to cryptocurrencies, among others can be addressed by the Judiciary on the infractions provided for in the Brazilian Criminal Code or in specific regulation. These legislations do not expressly address a response to cybercrimes but can be used to deal with these violations.

26. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

Brazil does not have a separate cybersecurity regulator.

In this regard, cybersecurity challenges might be dealt with by public authorities, such as the Public Prosecutor's Office, or by the Judiciary, when the demand is brought to its attention, with the help of independent agencies or entities, such as Computer Security Incident Response Teams (CSIRTs). In cases of incidents of cybersecurity involving the Brazilian Public Administration, for example, the Computer Network Security Incident Treatment Center of the Federal Public Administration (CTIR) should be contacted.

27. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

The LGDP sets forth that all-natural people are ensured the ownership of their personal data and the guarantee of the fundamental rights to freedom, intimacy, and privacy. It also establishes that data subjects have the right to obtain from the controller, at any time and upon request:

- Confirmation of the existence of the processing;
- Access to the data;
- Correction of incomplete, inaccurate, or outdated data;
- Anonymization, blocking, or erasure of unnecessary or excessive data or data processed in non-compliance with the provisions of the LGPD;
- Portability of data to another service or product provider, upon express request, by the regulations of the ANPD, observing commercial and industrial secrets;
- Deletion of the personal data processed with the consent of the data subjects, except in cases of:
    a. Compliance with a legal or regulatory obligation by the controller;
    b. Conduction of studies by a research entity, ensuring, whenever possible, the anonymization of the personal data;
    c. Transfer to third parties, provided that all legal requirements outlined in this Law are complied with;
    d. Exclusive use of the controller, with forbidden access to third parties,

and provided the data has been anonymized;
- Information about public and private entities with which the controller has shared data;
- Information about the possibility of denying consent and the consequences of the denial;
- Revocation of consent;
- Opposition to processing carried out based on one of the situations of waiver of consent if there is noncompliance with the provisions of LGPD;
- Review of decisions taken by the controller solely based on automated processing of personal data that affects the data subject's interests, including decisions intended to define his/her personal, professional, consumer, or credit profile or aspects of his/her personality.

All the rights aforementioned shall be exercised through the express request by the data subject or his/her legal representative, to the controller. This request shall be fulfilled without costs to the data subject, and, in case it is not possible to promptly take the actions, the data controller shall send to the data subject a reply in which it may: (I) inform that it is not the data processing agent, indicating, if possible, the agent; or (II) point out legal and factual grounds preventing prompt action.

LGPD provides for that the ANPD may provide different deadlines and terms for specific industries other than those mentioned above, within periods and under the terms provided for in future regulation, which should occur within two years from now, according to ANPD's regulatory agenda.

Data subjects have the right to petition about their data against the controller before the National Authority. The defense of the interests and rights of data subjects may be carried out in court, individually or collectively.

The rights of confirmation of existence and access to data will be provided immediately, in a simplified format; or within fifteen (15) days as from the date of the data subject's request, through a clear and complete declaration that indicates the origin of the data, the nonexistence of record, the criteria used and the purpose of the processing, subject to commercial and industrial secrecy. Information and data may be provided by electronic means or in printed form. Also, when the processing is based on consent or in a contract, the data subject may request a complete electronic copy of its personal data, observing commercial and industrial secrecy, in a format that allows its subsequent utilization, including for other processing operations.

Besides, the Consumer Code sets forth that individuals have the right to access all data stored about themselves in consumer-related databases, and request changes, corrections, and even removal from the database. This right to access might also be exercised before consumer-defense entities.

Finally, according to the Internet Law, users have the right to request at the end of their contract with internet application providers the definitive exclusion of personal data, respecting the mandatory log retention rule.

28. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

Both. The Federal Constitution establishes that the law shall not exclude from the Judiciary's assessment injury or threat to rights; therefore, the defense of the interests and rights of data subjects may be exercised in court, individually or collectively, by the provisions of the relevant legislation, regarding the instruments of individual and collective protection.

In addition to this guarantee, LGPD stipulates that data subjects have the right to petition concerning their data against the controller before ANPD. The right to access might also be exercised before consumer-defense entities.

29. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

Yes. According to the Federal Constitution, any individual can file a judicial action pursuing compensation for economic and moral damages for violation of privacy or intimacy. Furthermore, the Brazilian Code of Civil Procedure determines that the exercise of the right of action depends on the interest and legitimacy of the claimant.

The Federal Constitution assures Brazilians and foreign nationals the right to rectify their data, and the Consumer Code provides that individuals have the right to access all data stored about themselves, and request changes.

The internet law provides for the user´s right to request the definitive exclusion of personal data, by the end of the relation with the internet application provider. Also, LGPD provides that the data subject may exercise their rights and interests through a court, individually.

30. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

According to LGPD, the controller or processor which, as a result of carrying out their activity of processing personal data, causes material, moral, individual or collective damage to others, in violation of personal data protection legislation, is obliged to redress it. Also, the controller or the processor who neglects to adopt measures to avoid security incidents shall be held liable for the damages caused by the violation of the data security that caused the damage.

Individuals affected by breaches of the law are entitled to compensation or monetary damages. Usually, actual damage is required and injury of feelings must be proved to justify compensation.

31. How are the laws governing privacy and data protection enforced?

According to the article 55 – I of LGPD, the Brazilian General Data Protection Authority (known as ANDP) is competent to ensure protection of personal data, supervise and impose sanctions in case of data processed in violation of the laws, through an administrative process ensuring defense and right to appeal. In addition, according to the ANPD's regulatory agenda, it is expected that it will issue a resolution in the first half of 2021 regarding the definition of the methodologies that will guide the calculation of the value of sanctions. The regulation will also establish the circumstances and conditions for the adoption of a fine.

In addition to the ANPD, other bodies already acted in the enforcement of privacy in Brazil, and will continue to act, such as the Public Prosecutor's Office, the Special Unit for Data Protection and Artificial Intelligence (ESPEC), the National Consumer Bureau (SENACON) and consumer protection authorities. These bodies opened several cases and investigations against companies that suffered security incidents and data breaches in Brazil or processed personal data and sensitive personal data in potentially or effectively harmful ways to the data subjects.

32. What is the range of fines and penalties for violation of these laws?

The LGPD provides that the ANPD will impose administrative sanctions on processing agents for breaches of the rules, namely:

- Warning, with an indication of the time period for the adoption of corrective measures;
- A simple fine of up to 2% (two percent) of a private legal entity, group or conglomerate's revenues in Brazil, for the prior financial year, excluding taxes, up to a total maximum of BRL 50,000,000.00 (fifty million reais) per infraction;
- A daily fine, observing the total limit referred above;
- Publication of the infraction after duly ascertained and confirmed its occurrence;
- Blocking of the personal data to which the infraction refers to until its regularization;
- Deletion of the personal data to which the infraction refers to;
- Partial suspension of the operation of the database to which the violation refers to for a maximum period of 6 (six) months, extendable for the same period, until the controller's regularization of the processing activity;
- Suspension of the exercise of the processing activity of the personal data to which the infraction refers to for a maximum period of 6 (six) months, extendable for the same period;
- Partial or total prohibition of the exercise of activities related to data processing.

Also, the Internet Law states that, without prejudice to any other civil, criminal or administrative sanction, the non-compliance with data protection rules can result in the following sanctions that may be applied on an individual or cumulative basis:

- A warning, with a deadline for the adoption of corrective measures;
- A fine up to 10% of the gross income of the economic group in Brazil in the last fiscal year, taxes excluded;
- Temporary suspension of the activities that entails the events set forth in any operation related to treatment of data;

Prohibition to execute activities that entail processing of data.

The Consumer Code determines a penalty of six months to one-year imprisonment or fine, or both, to those who block or hinder access by the consumer to respective information contained in files, databases or records, or those who are expected of knowing that information relating to the consumer as contained in any file, database, record or registration is incorrect and, nevertheless, fail to immediately rectify it. The same

statute sets forth administrative penalties imposed by the authorities in charge of protecting consumer rights, and such penalties include fines, intervention and counter-advertising.

The Bank Secrecy Law (Complementary Law 105/2001) establishes a penalty of one to four years' imprisonment and a fine for financial institutions (and similar entities) that breach the secrecy of the financial operations of, and the financial services provided to its users.

The Brazilian Criminal Code (Decree-Law 2.848/1940), as amended by Law 12.737/2012, sets forth the penalty of three months to one-year imprisonment and fine to those who invade another computer device connected or not to the internet through improper breach of security mechanism and for the purpose of obtaining, tampering or destroying data or information without the explicit or tacit authorization of the device owner or installing vulnerabilities to gain any illicit advantage.

33. Can personal data or PII owners/controller appeal to the courts against orders of the regulators?

There is no express provision about this possibility in the LGPD or any other legislation that refers to data protection in Brazil. However, taking into consideration that the Federal Constitution establishes that the law may not exclude from the Judiciary's assessment injury or threat to rights, data subjects could appeal to the courts against orders of the ANPD, provided that the data subject proves his/her right of action (interest and legitimacy).

Contributors

Ricardo Barretto Ferreira da Silva
Senior Partner
barretto@azevedosette.com.br

Lorena Pretti Serraglio
Senior Lawyer

Camilla Lopes Chicaroni
Associate

Nariman Ferdinian Gonzales
Associate

Isabella da Penha Lopes Santana
Associate

