Chambers
Global Practice
Guides

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

TMT
2022

Brazil: Law & Practice

Ricardo Barretto Ferreira da Silva, Danielle Chipranski Cavalcante, Juliana Gebara Sene Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto
Azevedo Sette Advogados

practiceguides.chambers.com

BRAZIL

Law and Practice

Contributed by:
Ricardo Barretto Ferreira da Silva, Danielle Chipranski Cavalcante, Juliana Gebara Sene Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto
Azevedo Sette Advogados see p.23

CONTENTS

1. Cloud Computing p.3
1.1 Laws and Regulations p.3

2. Blockchain p.4
2.1 Legal Considerations p.4

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence p.5
3.1 Challenges and Solutions p.5

4. Legal Considerations for Internet of Things Projects p.7
4.1 Restrictions on a Project's Scope p.7

5. Challenges with IT Service Agreements p.9
5.1 Legal Framework Features p.9

6. Key Data Protection Principles p.9
6.1 Core Rules for Individual/Company Data p.9

7. Monitoring and Limiting of Employee Use of Computer Resources p.15
7.1 Key Restrictions p.15

8. Scope of Telecommunications Regime p.17
8.1 Scope of Telecommunications Rules and Approval Requirements p.17

9. Audio-Visual Services and Video Channels p.18
9.1 Audio-Visual Service Requirements and Applicability p.18

10. Encryption Requirements p.19
10.1 Legal Requirements and Exemptions p.19

11. COVID-19 p.20
11.1 Pandemic Responses Relevant to the TMT Sector p.20

Contributed by: *Ricardo Barretto Ferreira da Silva, Danielle Chipranski Cavalcante, Juliana Gebara Sene Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto,* ***Azevedo Sette Advogados***

1. CLOUD COMPUTING

1.1 Laws and Regulations

Although there are no specific laws about cloud services in Brazil, many local laws refer to this matter, as follows.

The Internet Act (Law No 12,956/2014, MCI), further regulated by Decree No 8,771/2016, provides principles, rights and obligations about the use of internet in Brazil, and sets forth obligations for internet connection and application providers that are relevant for cloud computing solutions in general. The MCI main obligations regarding cloud are related to data retention by internet application providers.

The Brazilian General Data Protection Act (Law No 13,709/2018, LGPD), which came into force in 2020, provides for the processing of personal data irrespectively of industry or business – as controllers or processors of personal data, cloud service providers shall comply with the referred law. The LGPD impacts cloud computing and its providers, in particular with regard to the requirements for the processing of personal data and for data transfers.

On the matter of personal data processing, it is important to enhance the relevance of data protection in a cloud computing environment, highlighting specific issues in this context, as follows.

- In cloud environments, the hosting location of personal data remains relevant with respect to the applicability of national law, which will give guidance on the matter.
- In cloud computing, different players usually co-operate along the end-to-end value chain in order to deliver the service to the customer and this leads to difficult questions considering personal data processing requirements such as security of the data, which may be intensified when new providers are added to the service.
- Cloud computing leads to considerable transfers of personal data, involving many different parties and crossing borders between countries, including outside Brazil. It means that the data controllers and data processors must ensure the compliance of these transfers with data protection rules.

Law No 8,078/1990 (the Consumer Protection Code, CDC) governs all consumer relationships, including cloud computing products or services.

Brazilian Central Bank's Resolution No 4,893 of 2021 provides for the cyber data policy and establishes requirements for contracting cloud processing services to be observed by companies regulated by the Brazilian Central Bank.

Complementary Norm/No 14/IN01/DSIC/GSIPR, established in 2012 and edited in 2018, has the objective of setting guidelines regarding the use of technologies in government agencies. More specifically, it addresses cloud computing and the aspects related to security and data protection. The Norm requires that information classified as secret or top secret cannot be processed on the cloud, for any reason. Also, data and metadata produced by and/or under the responsibility of the agency must be stored in data centres within national territory. In addition, it is important to note that, in 2016, the Information Security Cabinet of the President's Office and the Ministry of Planning, Budget and Management – which is now part of the Ministry of Economy – issued a general guideline with best practices, orientations and restrictions to be followed by federal entities when contracting cloud computing services. The document outlines some contractual requirements that should be ensured by the agencies contracting cloud services, and the following are particularly worth mentioning.

- The data and information of the contracting agency must reside exclusively in the national territory, including replication and back-ups. This requirement is justified by the need to provide the contracting agency with all the guarantees of Brazilian law, as the service taker is responsible for safeguarding the information stored in the cloud.
- The Brazilian jurisdiction must be adopted to settle any legal issues related to contracts signed between the contracting agency and the cloud service provider.
- The contracting agency must ensure the portability of data and applications, as well as the availability of information for location transfer, in an adequate period of time and at no additional cost, in order to ensure business continuity and enable the contractual transition.
- The contractual provisions must ensure that the information in the provider's custody will be processed with confidentiality and cannot be used or provided to third parties without authorisation under any circumstances.

2. BLOCKCHAIN

2.1 Legal Considerations

Risk and Liability

Blockchain technology regulation is still in its initial phase in Brazil. The first guidelines in this regard were introduced by the Securities and Exchange Commission (*Comissão de Valores Mobiliários,* CVM) in 2020 through the Normative Ruling (No 626/2020) that encompasses new business models and technologies available in capital markets, such as blockchains. The Central Bank has announced that it will authorise the issuance of blockchain tokens in the national financial system, part of the regulatory sandbox. Also, since 2020, notary offices are able to certify and time-stamp official documents via blockchain technology.

Notwithstanding the foregoing, as this technology is being accepted to the fulfilment of many purposes, including as evidence to be used in court, it is necessary to observe the legality of the procedure and observe the principles of due process, not to mention the assurance with respect of ethics and constitutional values. Risks and liabilities involving personal data are mentioned in the topic below.

Intellectual Property

The Brazilian Copyright Association allows the registration of intellectual property in blockchain and recognises its validity in the same way as the procedures undertaken by the Brazilian National Library. The greatest difference between those two procedures is the time of processing, which via the National Library can take up to 180 days and does not include a digital registry, while when using blockchain technology it should not take longer than five minutes to register and includes digital registry.

Additionally, non-fungible tokens (NFTs) are being used as a means to register intellectual property and, since it is based on blockchain technology, it is given a digital certificate of copyright. IBM, for example, has announced that it will use NFTs to register patents and, even though the certificates of ownership are not equivalent to the register made in the National Institute of Industrial Property, they are able to identify the owner of a piece of art, a meme or a registry. Blockchain technology seems to be a promising way to facilitate access to such registries, since it is faster and costs less, which will enable small businesses and individual artists to certify the ownership of their work in a more efficient way.

Data Privacy

Blockchain is not incompatible with the Brazilian Data Protection Act (Law No 13,709/2018), even though its immutability may rise questions

regarding the right to be forgotten and the processing of personal data. One of the main issues debated in this context is the right to be forgotten, since personal data (or any information) contained in a blockchain would never be forgotten. The right to be forgotten, in turn, was recently declared by the Brazilian Supreme Court to be incompatible with the Federal Constitution in a very specific case, which did not analyse issues related to technology, the internet or blockchain. So, it is possible that the matter will generate new discussions in the future, especially when blockchain has its own regulation.

Service Levels

As the regulation of blockchain technology is still in its initial phase in Brazil, there are still no general rules regarding service levels.

For instance, MRV, a Brazilian constructor, recently carried out the first real estate development on the market using blockchain technology to optimise notary services in a virtual environment. The procedure refers to incorporation of a project to be launched by the construction company in the municipality of Duque de Caxias, in the State of Rio de Janeiro. Unlike the traditional process, MRV concluded the blockchain real estate development act in a few minutes. Through the physical means, such registration of the purchase and sale deed takes, on average, 30 days to be carried out by the notary's office. Other acts, such as the registration of the memorial of incorporation and convention of condominium, can take up to 45 days.

Jurisdictional Issues

The technology is accepted in courts to prevent and preserve evidence, mostly regarding digital media, such as registration of social media posts and app conversations. This is the understanding of the Court of Justice of the State of São Paulo, in the judgment of the cases 1000786-26.2019.8.26.0660 and 2237253-77.2018.8.26.0000, which recognised that blockchain registration is a valid proof for the existence of an online content.

As blockchain cannot be altered, it is very helpful to preserve digital events that could possibly be altered by a user (eg, social media posts), proving the authenticity of the evidence.

The technology is available and can be used by anyone, contrasting with older types of evidence registration such as depending solely on the notary's office to authenticate a document.

Recently, the Brazilian government officialised the use of blockchain through a Normative Ruling (ITI No 19/2021) issued by the National Institute of Information Technology, and this system will be used to certify the existence of a certain document at a specific date and time (ie, time stamp).

3. LEGAL CONSIDERATIONS FOR BIG DATA, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

3.1 Challenges and Solutions

Our society has been passing through two big waves of transformation in the area of technology – namely, big data and the usage of artificial intelligence (AI) in companies, projects and businesses in order to offer better and more effective solutions in their applications. The influence of big data and the use of AI through machine learning has been impacting several sectors of the world economy and this impact is only likely to increase in future.

In the Brazilian jurisdiction, there are several legal challenges when starting a project where big data and artificial intelligence are applied.

The biggest issue regarding those technologies is that Brazil has not yet provided regulation for the use of AI, machine learning or big data. Therefore, the main practical challenge is the lack of by-laws dealing with these matters. When managing a business programme involving such technologies, the legal, ethical and constitutional principles must be observed, as well as national and international frameworks and guidelines that have already been established, giving special attention to what is being discussed by Brazil's government, national authorities, and by courts related to the matter.

Big Data

When it comes to the use of large amounts of data, one of the main issues companies must be aware of is personal data protection.

In Brazil, the LGPD sets legal parameters for the use of personal data. The law is applicable to the activities of collecting and processing personal information with big data, which are mainly used by companies for purposes such as data mining and profiling. If not processed properly and in accordance with the law, those data processing techniques can cause severe damages to the rights of data subjects. Therefore, companies must structure their compliance and data governance programmes by adapting to data processing rules. These measures are important for organisations to have a safer and more reliable environment for the protection of society's fundamental rights of privacy and data protection.

Artificial Intelligence and Machine Learning

Many of the main challenges for implementation of AI and solutions where machine learning is applied in Brazilian companies are related to the needful observance to data protection principles and ethical usage of such technologies, and the absence of regulation regarding the matter. AI regulation is a highly discussed topic in Brazil, and there have recently been a number of proposed legislations, both by the Chamber of Deputies and the Federal Senate, some of which have caused controversy.

It should be mentioned that, according to the LGPD, data subjects have the right to request the review of decisions based exclusively on the automated processing of personal data that affects their interests, including decisions that define their personal, professional, consumer and credit status or their personality. However, the LGPD does not grant data subjects the right not to be subject to a decision based solely on automated processing that has a legal impact on them or affects them in any way. In addition, the LGPD does not have the obligation to provide information on automated decision-making, algorithmic logic and the consequences of such processing because, under the LGPD, in theory, if the information is claimed to infringe the industrial or trade secrets, the data controller may refuse to provide clear and sufficient information about the standards and procedures used for automated decision-making.

Even so, the LGPD has indirectly addressed the ethical issues raised by AI because it first stipulated in its legal text that data subjects may need to request to review decisions made only by automated machines. The clause would provide mechanisms to minimise the risks caused by the increasing use of algorithms to evaluate and classify people's lives and behaviours. However, this provision was banned and revised by the President of Brazil. Therefore, the review of the automated decision no longer needs to be done by a natural person. This change has not been welcomed by the legal community, who believe it is harmful to the rights of data subjects and to the moral use of artificial intelligence systems.

For that reason, in March 2020, the Brazilian Ministry of Science, Technology and Innova-

tions (MCTIC) wrapped up a Public Consultation on the Brazilian Artificial Intelligence Strategy (EBIA), in order to collect subventions to enhance the benefits of AI to the country and help mitigate negative impacts. The public consultations aimed to provide solutions related to legislation, regulation and ethical use of AI and machine learning in order to promote proper development and adoption of these technologies.

When it comes to the proposition of legislations, Draft Bill No 5051/20, proposed by Senator Styvenson Valentim, stands out for its proposal regarding the liability of damages caused by automated decisions of AI devices, stating that the responsibility should always lie with the human supervisor of the system. Also proposed by the same Senator, Draft Bill No 5691/2019 institutes a National Policy for Artificial Intelligence, addressing requirements for AI and machine Learning solutions to be understandable and accessible, with mechanisms for human intervention, if necessary, without discriminatory bias.

Another important proposed legislation was drafted by Deputy Eduardo Bismarck (Draft Bill No 21/20), establishing that the use of AI must be based on respect for human rights and democratic values, equality, non-discrimination, plurality, free initiative and data privacy. In addition, AI must have, as a principle, the guarantee of transparency in its use and operation, also imposing several duties on the development and operating agents, where these agents must provide clear and adequate information about the procedures used by AI systems, to which such duty is formerly imposed on the processing agents in the LGPD. Also, AI and machine learning operating agents should respond as stipulated by the law to decisions made by an AI system and provide continuous protection of AI systems against cybersecurity threats.

4. LEGAL CONSIDERATIONS FOR INTERNET OF THINGS PROJECTS

4.1 Restrictions on a Project's Scope

When contemplating a project with connected devices, Decree 9,854/2019, which instituted the National Internet of Things Plan to improve the quality of life, foster competition, increase productivity and Brazil's integration to the international landscape, among other objectives, should be considered. According thereto:

- Internet of Things (IoT) is the infrastructure integrating the provision of value-added services (VAS) with physical or virtual connection capabilities of things with devices based on information and communication technologies or evolutions thereof, with interoperability;
- machine-to-machine (M2M) communications systems are telecommunications networks, including access devices, for the transmission of data to remote applications aimed to monitor, measure and control the device itself, the environment around it, or data systems connected thereto by means of such networks.

Implementation and development of IoT is based on free competition and circulation of data, but compliance with information security and personal data protection guidelines is required. Health, cities, industries and rural environments are priorities for IoT solutions.

VAS/Telecommunications Services

According to Law 9472/1997 (General Telecommunications Law, LGT), VAS are not:

- telecommunications services (but rather, an activity adding new utilities related to the access, storage, presentation, movement or recovery of information to a telecommunica-

tions service supporting it), with which it is not confused;
- regulated by telecommunications authorities; or
- subject to the control of the National Telecommunications Agency (ANATEL).

Contrarily, telecommunications services (activities enabling the offer of transmission, emission or reception of symbols, characters, signs, writings, images, sounds or information, whether by wire, radio-electricity, optical means or any other kind of electromagnetic process), as per LGT, are regulated in Brazil and provision thereof depends on ANATEL's authorisation.

However, transmission of data between IoT devices is required for their operation and, thus, there should be connectivity. Consequently, two issues arise:

- should the IoT project contract connectivity from a third-party telecommunications provider holding the applicable ANATEL authorisation (eg, personal mobile service, multimedia communication service, global mobile satellite service), the IoT provider will be deemed user of the telecommunications service supporting the IoT application and will not be subject to telecommunications regulatory rules and ANATEL's control; and
- if the same project provides both the VAS (related to the IoT application) and the telecommunications service (connectivity for IoT devices), the IoT provider will be subject to telecommunications regulatory rules applicable and should hold an authorisation from ANATEL.

Device Authorisation/Licensing

Connected devices are deemed communications products using radioelectric spectrum for information's propagation, being subject to compliance with technical requirements, certification and authorisation by ANATEL.

Operation of radiocommunications transmitting stations also requires prior licensing with ANATEL, but Law 14108/2020 exempted stations integrating M2M communications systems from prior licensing.

Taxation

Being deemed VAS, IoT is not subject to the tax on circulation of goods and services (ICMS), levied on telecommunications services; tax on services (ISS) is due, but at rates lower than those of ICMS.

Law 14108/2020 also exempted M2M communications systems' stations from the payment of certain fees until December 2025.

Information Security/Personal Data Protection

Reliable and stable networks are fundamental for IoT. Regulations to avoid cyber-attacks and unauthorised access to data and disclosure thereof should be complied with. Several laws and regulations provide on the matter and should be considered, such as:

- Federal Constitution – privacy, private life, honour and image of people, as well as the confidentiality of data, are inviolable (except in cases of court orders related to criminal investigations or discoveries);
- Law 9,296/1996 – interception of information technology, telematics, telephone communications and others is a crime;
- LGT – stipulates privacy rights of telecommunications services' consumers;
- Law 12,737/2012 – provides information on cybercrimes and classifies disclosure of proprietary information as a crime;
- Law 12,965/2014 (Internet Bill of Rights) – sets principles and rules for ensuring privacy

and data protection in internet use, and establishes that applications providers should retain records of accesses to applications and connections;
- Decree 8,771/2016 – sets security standards for the custody, storage and processing of personal data and private communications by connections/applications providers;
- Law 13,709/2018 (General Data Protection Act) – regulates personal data protection and processing aspects, among other provisions;
- ANATEL's Resolution 740/2020 (Regulation of Cybersecurity Applied to the Telecommunications Sector) – establishes conducts and procedures to promote security in telecommunications networks and services, and protect critical structures; and
- ANATEL's Act 77/2021 – provides cybersecurity requirements for telecommunications equipment.

Fifth-generation (5G) technology is expected to be implemented in Brazil in 2022 and boost the IoT market, fostering innovation and impacting local economy and society. Minimum cybersecurity requirements for 5G networks were set by the Office of Institutional Security of the Republic Presidency's Normative Instruction 4/2020.

5. CHALLENGES WITH IT SERVICE AGREEMENTS

5.1 Legal Framework Features

As the law and case law in Brazil have not yet addressed the matter of IT service agreements in general, they must be regulated in specific details.

The main challenges of IT service agreements in Brazil are probably related to intellectual property rights (IPRs), service levels, liability and data privacy.

First, in the IT industry, the continuous development of technologies is essential and contracts shall clearly regulate the ownership of existing intellectual property and future intellectual property developed during the commercial relationship between the parties involved.

Furthermore, as software are often provided as a service in Brazil, service level agreements (SLAs) are heavily discussed. In this regard, although there is not specific regulation about SLAs (so this is mostly a commercial matter), general laws and customs provide minimum requirements in terms of uptime, back-ups, disaster recovery and business continuity.

Liability is always a significant issue. The Software Law (Law No 9,609/98) expressly says that clauses that "*exempt any of the contracting parties from any third-party actions arising from misuse, flaws, or violation or copyrights*" are null and void (Article 10). However, limitation of liability is allowed and case law varies considerably about the possible caps to indemnifications regarding IT contracts.

Finally, data privacy matters are also deeply discussed. Personal data (including sensitive data) is usually stored by IT systems, regulated by these IT agreements. Controllers and processors of data (as defined in the LGPD) shall comply with local regulation, subject to legal penalties.

6. KEY DATA PROTECTION PRINCIPLES

6.1 Core Rules for Individual/Company Data

Rules regarding Data Protection

Principles

The Brazilian Data Protection Act (LGPD), approved in Brazil in August 2018, effective since 2020, provides for the processing of per-

sonal data by natural persons or legal entities of public or private law.

The legislation states that the processing of personal data must be based on good faith and the following principles:

- adequacy – compatibility of the processing with the purposes informed to the data subject;
- purpose – processing of the data for legitimate, specific, explicit purposes that have been informed to the data subject;
- free access – guaranteeing that the data subjects may have access to consultations about the form and duration of the processing, and may exercise the rights regulated by the LGPD;
- non-discrimination – prohibition to process personal data for discriminatory or illicit purposes;
- data quality – guarantee assured to the data subjects of data clarity, accuracy and updating, always compatible with the need and fulfilment of the purpose of its processing;
- necessity – carrying out the minimum processing for the realisation of its purposes, covering only pertinent data and not excessive in relation to the purpose;
- transparency – assurance to the data subjects of clear, precise and accessible information about their data;
- prevention – use of measures that avoid damages resulting from the processing of personal data;
- accountability – demonstration that the agent adopts effective measures capable of proving compliance with the LGPD; and
- security – use of adequate measures to protect personal data.

Scope

Regarding the territorial scope, LGPD establishes that the law is applicable:

- to any processing activity performed by a controller or a processor in the Brazilian territory;
- to any processing activity whose purpose is to offer goods or services to individuals located in Brazilian territory;
- to any processing of personal data of individuals located in Brazilian territory; and
- when the personal data processed in the activity has been collected in Brazilian territory.

Definitions

The law defines personal data as any "*information related to any identified or identifiable individual*", while sensitive personal data is the personal data regarding racial or ethnic origin, religious belief, political opinion, affiliation to any trade union or to a religious, philosophical or political organisation, data relative to health or sex life, genetic or biometric data, when associated to an individual.

Legal basis for data processing

The processing of personal data shall only occur under the following legal basis:

- upon the data subject's consent;
- for compliance with a legal or regulatory obligation by the data controller;
- by the public administration, to process and share data required for the execution of public policies or based on contracts or similar instruments under the terms of the law;
- for the performance of studies by a research body, with guarantee of anonymisation of personal data wherever possible;
- when necessary for the execution of a contract or preliminary proceedings related to a contract to which the data subject is a party;
- for regular exercise of rights in court, administrative or arbitration proceedings;
- for the protection of a third party's or data subject's life or physical integrity;

- exclusively for the protection of health under procedures performed by healthcare professionals, health services or health authority;
- when necessary to meet legitimate interests of a third party or data controller, except where fundamental rights and freedoms of the data subject requiring protection of personal data prevails; and
- for the protection of credit.

Special rules may apply when concerning the legal basis for processing sensitive personal data.

Data protection impact assessments

When the processing is based on the legitimate interest of a controller or third parties, the Brazilian National Authority (ANPD) may require the data controller to submit a data protection impact assessment (DPIA). This report must contain, at least:

- a description of the types of data collected;
- the methodology used for collection and to ensure security of information; and
- the analysis of the controller regarding measures, safeguards and mechanisms adopted to mitigate risks.

Data subjects rights

Processing agents must provide means for the exercise of rights of data subjects, which are:

- confirmation that their data is being processed;
- access to their data;
- correction of incomplete, inaccurate or outdate data;
- anonymisations, blocking or erasure of unnecessary, excessive data or data processed in violation of the LGPD;
- portability of their data to another service or product provider, upon express request;
- erasure of personal data processed with the data subject's consent, except in the events provided for in the law;
- information about public and private entities with which the controller shared use of data;
- information on the possibility of refusal of consent and on the consequences of such refusal;
- revocation of consent under the terms of the law; and
- right to request a review of decision solely taken based on an automated processing of personal data that affects their interests, including decisions intended to define their personal, consumer and credit profiles or aspects of their personality.

Obligations of processing agents

The LGPD determines that data controllers are required to record:

- the name and contact details of the controller;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data will be disclosed;
- international transfers of personal data, with the identification of third countries or international organisations, and the documentation of suitable safeguards adopted;
- the estimated time limits for erasure of the categories of data; and
- a general description of the technical and organisational security measures adopted.

When the processing agent is a small business or start-up, the record of processing activities may be simplified, and the template will be provided by the regulatory authority.

According to the LGPD, data controllers must appoint a DPO and disclose their identification and contact information to the public in a clear

and objective form, preferably on the data controller's webpage. The duties of the data protection officer are the following:

- accept data subjects' communications and complaints, provide clarifications and adopt measures;
- receive communications from the national authority and take measures;
- instruct the entity's employees and vendors on practices to be adopted regarding personal data protection; and
- perform other duties established by the controller or by additional rules.

According to Resolution No 2, small businesses and start-ups that process personal data are not required to appoint a DPO, provided that they do not (i) perform high-risk personal data processing or (ii) earn, individually or within the sum with their economic group, gross revenue above BRL4.8 million per year (or BRL16 million per year in the case of start-ups). The obligation to establish a communication channel with the data subject remains maintained.

The LGPD also determines that the controller must notify the national authority and the data subjects immediately, whenever a security incident that may pose a significant risk or cause damage to data subjects occurs. A security incident with personal data is defined as any confirmed adverse event related to a breach in the security of personal data, such as unauthorised, accidental or unlawful access that results in the destruction, loss, alteration, leakage or any form of data processing inadequate or unlawful, which may pose a risk to the rights and freedoms of the holder of the personal data. The incident notice must contain, at least:

- a description of the nature of the affected personal data;
- information about the affected data subjects;
- an indication of the security and technical measures adopted to protect data, subject to trade secrets;
- risks associated to the incident;
- in case the notice was not submitted promptly, the reasons for the delay;
- measures adopted or to be adopted to reverse or mitigate loss effects.

Besides those elements listed above, the ANPD recommends that the notice contains:

- identification and contact details for –
  (a) entity or person responsible for the processing,
  (b) data officer or other contact person,
  (c) indication of whether the notification is complete or partial, or, in case of partial communication, indication that it is a preliminary communication or a complementary communication;
- information about the security incident with personal data, namely –
  (a) date and time of detection,
  (b) date and time of the incident and its duration,
  (c) circumstances in which the security breach of personal data occurred, (eg, loss, theft, copying, leakage),
  (d) description of personal data and affected information, such as nature and content of personal data, category and amount of data and affected data subjects,
  (e) summary of the security incident with personal data, indicating the physical location and storage means,
  (f) possible consequences and negative effects on affected data subjects,
  (g) preventive security, technical and administrative measures taken by the controller in accordance with the LGPD,
  (h) summary of measures implemented so far to control possible damage,
  (i) possible problems of a cross-border

nature,
(j) other useful information for affected people to protect their data or prevent possible damage.

If it is not possible to provide all the information at the time of the preliminary communication, additional information may be provided later. Whilst the regulation is pending, it is recommended that after becoming aware of the adverse event and having a relevant risk, the ANPD shall be contacted as soon as possible, this being considered as an indicative period of two business days, counting from the date of knowledge of the incident.

In relation to small sized processing agents, according to Resolution No 2 from ANPD, they will have double the period established in the LGPD to undertake some acts, such as responding to a data subject's requests and communicating to the ANPD and the data subject about the occurrence of security incidents.

International data transfers

LGPD establishes the permitted hypothesis of transfers. It allows international data transfers, including:

- to countries or international bodies that provide a degree of personal data protection in line with the provisions of this law;
- data controller offers and substantiates guarantees of compliance with principles, data subject's rights and data protection system established by the LGPD, in the form of –
  (a) specific contractual clauses for a given transfer,
  (b) standard contractual clauses,
  (c) global corporate rules, or
  (d) seals, certificates and codes of conduct regularly issued;
- when the transfer is necessary for international legal co-operation among public intelligence, prosecution and enforcement bodies, according to instruments of international law;
- when transfer is necessary for protection of a data subject's or third-party's life or physical integrity;
- upon authorisation from the national authority;
- when the transfer results from a commitment undertaken pursuant to an international co-operation agreement;
- when transfer is necessary for purposes of enforcement of a public policy or a legal duty of public service, being made public pursuant to the law;
- upon express consent from a data subject for the transfer, with prior knowledge about the nature of the transaction, clearly differentiating it from other purposes;
- to meet the requirements of the following items of Article 7 of the LGPD –
  (a) compliance with a legal or regulatory obligation by the controller,
  (b) when necessary for the performance of a contract or preliminary proceedings related to a contract to which the data subject is a party, upon the request of the data subject, and
  (c) for the regular exercise of rights in court, administrative or arbitration proceedings.

The LGPD determines that the level of data protection in foreign countries/international bodies will be assessed by the national authority, along with the definitions of content of specific contractual clauses, SCCs, global corporate rules or seals, certificates and codes of conduct.

Up to this point, the national authority has not yet issued opinions on the subject and has also not undertaken data protection adequacy level analysis of other countries. It is estimated that the topic will be considered in the first half of 2022, when it will be the subject of a resolution by the ANPD, according to its regulatory agenda.

Enforcement and administrative penalties

The LGPD establishes that any data controller or processor who, through personal data processing, gives rise to pecuniary or moral damage, individually or collectively, in violation of applicable personal data protection laws, shall have to compensate it.

The Brazilian law also establishes that the data processor shall be jointly liable for damages caused by the processing of data in violation of applicable data protection laws or due to failure to follow any lawful instruction from the controller, in which case the processor shall be deemed equivalent to the controller, except if an exclusion of liability is applicable.

In Brazil, it is still important to mention that the consumer defence bodies have had an effective performance, following all the movements related to the subject of privacy and protection of personal data, besides filing countless lawsuits.

In regard to the penalties foreseen by the law, the LGPD defines the administrative penalties in case of violation of privacy laws. Processing agents will be subject to the following sanctions by the national authority:

- warning, indicating a deadline to take corrective measures;
- simple fine of up to 2% of the turnover of the legal entity subject to private law, group or conglomerate in Brazil in the last year, excluding taxes, limited to the aggregate amount of BRL50 million per infringement;
- daily fine, subject to the aggregate limit referred to in the previous item;
- disclosure of the infringement to the public once it has been duly investigated and confirmed;
- blocking of personal data to which the infringement relates, until its regularisation;
- erasure of personal data related to the infringement;
- partial suspension of operation of database to which the infringement refers for a maximum period of six months, renewable for the same period, until regularisation of the processing activity by the controller;
- suspension of processing activity relative to personal data to which the infringement refers for a maximum period of six months, renewable for the same period;
- partial or total prohibition of data processing activities.

The LGPD does not limit the sanctions to those imposed by the supervisory authority. Data subjects and their representatives go to court for compensation, in which case the limitation of the monetary amount imposed by the LGPD will not be applicable.

Regulatory authority

In respect of the National Data Protection Authority (ANPD), the LGPD defines it as a public administration body responsible for ensuring, implementing and overseeing compliance with this law within the whole national territory.

The ANPD is responsible for defining the minimum level of security, rules of data portability, enforcement of sanctions and other factors, in the LGPD. According to the LGPD, the ANPD shall be competent to:

- ensure protection of personal data, pursuant to the terms of applicable laws;
- ensure compliance with trade secrets, subject to protection of personal data and the confidentiality of information protected by law or in case breach of confidentiality violates the grounds of Article 2 (grounds of personal data protection);
- prepare guidelines for the National Policy for Protection of Personal Data and Privacy;

- supervise and impose sanctions in case of data processed in violation of the laws, through an administrative process ensuring adversary proceeding, fair hearing and right to appeal;
- assess petitions from the data subject against the controller after substantiation by the data subjects to file a complaint against the controller, not solved within the period established by regulation;
- promote, within the population, knowledge of public rules and policies on protection of personal data and of the security measures;
- promote co-operation measures with personal data protection from other countries, of an international or transnational nature.

Besides the actions mentioned above, the national authority may establish additional rules, authorise international transfers of personal data, and assess the level of data protection of foreign countries or international bodies, considering the parameters set out by the LGPD. The ANPD is also responsible for defining the content of standard contractual clauses, verifying specific contractual clauses for a given transfer, global corporate rules or seals, certificates and codes of conduct. The national authority will be in charge of enforcing the administrative sanctions mentioned in the topic above, and may order the data controller to prepare an impact assessment report on the protection of personal data relative to its data processing operations, pursuant to regulation, subject to trade secrets.

Distinction between Companies/Individuals

The LGPD rules apply to processing activities involving personal data (information relating to an identified or identifiable natural person). Brazilian law, therefore, adopted the expansionist criterion. Therefore, personal data can be anything from a name, a telephone number, a home address, the IP number of a computer, or any other information that can identify an individual. On the other hand, data relating to legal entities are not considered personal data – for example, company name, National Register of Legal Entities and business address.

General Processing of Data

Every day companies have access to a huge volume of data, whether internal to the business, external or coming from third-party databases. These companies can process data, which is nothing more than the collection, compilation, organisation and disposition of information.

There is no provision for applying the LGPD to the processing of information that is not considered personal or sensitive data. However, their good practices can still be observed.

Processing of Personal Data

Brazilian law considers a large number of activities as processing personal data. They include the collection, classification, reproduction, receipt, archiving, dissemination, extraction, access, transmission, distribution, processing, communication, transfer, or any operation performed with some kind of handling of personal data.

7. MONITORING AND LIMITING OF EMPLOYEE USE OF COMPUTER RESOURCES

7.1 Key Restrictions

Monitoring and limiting the use by employees of computers resources are common practices used by companies in Brazil. However, in order to implement this practice in accordance with the Brazilian Consolidation of Labour Laws (Law No 5,452/43, CLT), the Brazilian General Data Protection Act (Law No 13,709/18, LGPD) and case law, there are specific rules that must be observed.

There are no restrictions on prohibiting or limiting the use of private email, social media, and/or specific websites or content during working hours. Nevertheless, if the company allows their employees the use of working devices for non-working-related activities or to access personal content, the monitoring of the device, if implemented incorrectly, may result in a violation of the employee's rights regarding their privacy and personal data.

In accordance with the case law of the Superior Court of Justice (Brazil, Superior Court of Justice. Lawsuit AIRR – 305840-29.2005.5.09.0013) communications sent using business tools defined by the company (eg, business email address) can be monitored provided that the company informs the employee in advance of this practice in a transparent and clear way. The communication to the employee about the monitoring activities can occur through the employment contract, the company's privacy policy and the company's security information policy, among others. In any case, it is important to provide evidence that the employee is aware of such monitoring procedure.

Furthermore, with the entry into force of the LGPD, new obligations regarding the processing of employee's personal data, and therefore the monitoring of their activities, has emerged. The LGPD requires that, in addition to the obligation of processing personal data only under one of the legal bases listed on Article 7 and/or Article 11, the processing can only occur under the following conditions.

- In accordance with the principle of purpose, provided for in Article 6, item I, of the LGPD, the processing must be performed for legitimate, specific and explicit purposes, duly informed to the data subject. Whereas the monitoring of employee's computers or working devices generally has the specific purpose of ensuring the fulfilment of the employment contract and protecting the company's information (including personal data of its employees, clients, partners, suppliers, among others), the monitoring activities have legitimate and specific purposes, which does not exclude the obligation of communicating to the employee about the monitoring. Notwithstanding, the employer and/or the company shall ensure that the monitoring of employee's computer activities does not occur for other purposes than the one duly informed to the data subject.
- Regarding the principle of necessity, provided for in Article 6, item III, of the LGPD, the processing must be limited to the minimum required to achieve its purposes.
- In attention to the principle of transparency, provided for in Article 6, item VI of the LGPD and the case law regarding this matter, the company/employer must provide the employee with clear, accurate and easily accessible information, prior to the processing of personal data by monitoring their working devices.
- When the monitoring is based on legitimate interest, it must be carried out in accordance with the processing of data strictly necessary for legitimate purposes, considered from concrete situations, in which case the national authority may request from the controller a data protection impact assessment (DPIA).

The employment of technical measures to protect personal data from unlawful situations of destruction, loss, change, communication or dissemination (eg, data loss prevention tools (DLP), web traffic monitoring) is required by the LGPD, provided for in Article 6, item VII. However, the obligations and requirements listed above must be considered prior to the implementation of security information tools/mechanisms, in order to ensure that the employee's fundamental rights and personal data are not infringed.

Contributed by: *Ricardo Barretto Ferreira da Silva, Danielle Chipranski Cavalcante, Juliana Gebara Sene Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto,* ***Azevedo Sette Advogados***

8. SCOPE OF TELECOMMUNICATIONS REGIME

8.1 Scope of Telecommunications Rules and Approval Requirements

According to LGT and complementary rules (eg, issued by ANATEL, the agency in charge of administering radio frequencies' spectrum and orbits' use), telecommunications services might be:

- provided under the public regime (subject to stricter legal/administrative conditions), or private regime (less regulated); and
- of community interest (provided to any party interested in its enjoyment, under non-discriminatory conditions) or restricted interest (intended for the own executor's use or provided to groups of users selected by provider, prohibits interconnection to other networks).

The following telecommunications technologies are the main currently regulated.

- Fixed-switched telephone service (FSTS): transmits voice and other signals, being intended for communication between fixed determinate points using telephony processes. This is the only service rendered under the public regime (based on concessions, subject to greater state control), but it can also be provided under the private regime (based on authorisations).
- Personal mobile service: enables communication between mobile stations, and mobile and other stations.
- Multimedia communication service: enables the supply of transmission, emission and receipt capacity of multimedia information (ie, audio, video, data, voice and other sound signals, images, texts, other information of any nature), and allows the provision of internet connection using any media to subscribers thereof. Importantly, transmission, emission or receipt of information which might constitute broadcasting or conditioned-access services is not allowed.
- Conditioned access service: distributes audio-visual content by means of any technology, process, electronic media and communication protocols, with access thereto based on a paid subscription.
- Private limited service: restricted-interest service, encompasses multiple applications, such as communication of data, video/audio signals, voice and text, and capture/transmission of scientific data (eg, meteorology).

Brazilian and foreign satellites might be used by community-interest services providers to transport telecommunications signals, but this is not intrinsically a telecommunications service.

Provision of FSTS under the public system depends on a concession granted in a bid and the execution of the concession agreement. Law 13879/2019 stipulates that concessionaires might request ANATEL to adjust the concession into an authorisation, if certain requirements are met by the interested party.

Exploitation of telecommunications services in the private regime depends on ANATEL's prior authorisation. The following applies:

- authorisation is not required for telecommunications activities restricted to the limits of the same construction or movable/immovable property (except if involving the use of radio frequencies by means of radiocommunication equipment not categorised as restricted radiation equipment);
- authorisation for the exploitation of services is waived if the support telecommunications networks use exclusively confined means and/or restricted-radiation radiocommunication equipment, provided no numbering

resources are employed, and, in the case of community-interest services, there is less than 5,000 users – however, the provider should inform ANATEL prior to the activities' onset.

For an authorisation to be granted, the provider should:

- be organised in accordance with Brazilian laws, with its principal place of business and administration in Brazil;
- be able to contract with public authorities;
- have the technical qualification required to provide the service, good economic/financial standing and tax regularity;
- be in good standing with the Social Security; and
- should not be responsible for providing the same kind of service in the same location.

The interested party requires the applicable authorisation through ANATEL's information system, providing certain information and documents according to such agency's Resolution 720/2020. Prior notification to ANATEL regarding which services will be provided is mandatory. The authorisation's amount due is BRL400 for community-interest services and BRL20 for restricted-interest services. Nevertheless, when the provision of community-interest services can be impacted by many competitors, a bid might be required for the issue of authorisations.

Additionally, the provider should comply with all specific conditions established by regulations applicable to the relevant telecommunications service, which requires a deep analysis.

Services and solutions adding utilities – and not to be confused with the telecommunications services supporting them (eg, instant messaging, RFID tags, communication between computers connected to the internet with no connection to telephony networks) – are deemed VAS and are not subject to telecommunications rules.

However, if they also encompass the provision of telecommunications services, ANATEL's authorisation is required and telecommunications regulations will apply. Computers' communication using voice-over IP (VoIP) to connect with fixed/mobile phones, and VoIP services simultaneously originating and terminating the communication with public telephony networks are examples of this.

Moreover, communications products using the radioelectric spectrum for the propagation of information should comply with the applicable technical requirements, in addition to being certified and authorised by ANATEL.

9. AUDIO-VISUAL SERVICES AND VIDEO CHANNELS

9.1 Audio-Visual Service Requirements and Applicability

Audio-visual and media services (broadcasting services) are subject to the Federal Union in terms of regulation, maintenance and exploitation, although the Brazilian Telecom Code (BTC) allows private individuals to execute such services under proper concessions, authorisations or permissions to be granted for renewable and successive deadlines of ten (radio broadcasting) or 15 years (television broadcasting). Concessions and authorisations are not exclusive and the Federal Union may directly execute the same services.

After publication of a notice, interested parties may present their proposals, which will be subjected to the President of the Republic after the competent body analyses the proposals and issues its opinion. The broadcasting

station is subject to a previous licence, which must be required after the concession contract is registered by the audit officer. If the station is approved, the licence shall be issued within 60 days.

The authorisation or permission is subject to the following requirements:

- 70% or more of the total and voting capital must belong, directly or indirectly, to native Brazilians or those naturalised for more than ten years (to be proved by documents annually submitted to the competent bodies), who will mandatorily exercise the management of activities and establish the content of the programming;
- contractual amendments must be subject to the executive authority within 60 days;
- the transfer of the concession, authorisation or permission to third parties depends on prior approval of the competent body;
- the information, entertainment, advertising and publicity services of the broadcasting companies are subordinated to the educational and cultural purposes inherent to broadcasting, aiming at the best interests of the country;
- the radio broadcasting stations are obliged to daily retransmit the official information programme of the Brazilian Republic, *A Voz do Brasil* (except on weekends, holidays and other specific occasions), as per specificities provided by the law;
- the same person may not participate in the administration or management of more than one concessionaire, licensee or authorised of the same type of broadcasting service, in the same location;
- broadcasters, including television, must fulfil their informative purpose, allocating a minimum of 5% of their time to broadcast news service;
- executives or partners cannot have suffered any condemnations related to ineligibility criteria;
- in the 90 days prior to elections, the broadcasting stations shall reserve two hours daily for free party political broadcasts.

The fees payable for the use of the telecommunications services provided by the entity will be fixed in order to always remunerate the total costs of the services, the amortisation of the invested capital and the formation of funds necessary for the conservation, replacement and modernisation of the equipment, and extensions of services.

These requirements do not apply to application providers, such as platforms on which users may post their content, such as videos. These platforms are foreseen by specific law, which regulates the use of the internet in Brazil, which includes the application providers.

10. ENCRYPTION REQUIREMENTS

10.1 Legal Requirements and Exemptions

Legal Requirements Governing the Use of Encryption

Although Brazil's General Data Protection Regulation (LGPD) does not explicitly address the matter, encryption is one of the fundamental principles of information security, ensuring confidentiality of processed data. Hence, the LGPD does not require the use of encryption as an obligation to companies. However, the law mentions the adoption of technical and organisational measures to protect data from unauthorised access and from accidental or unlawful situations of destruction, loss, alteration, communication, or any form of inappropriate or unlawful processing. Up until now, Brazil's Data Protec-

tion Authority (ANPD) has not issued such regulation providing for minimum technical standards to make these security measures, such as encryption, applicable.

It is important to highlight that Article 5 of the Brazilian Federal Constitution guarantees the secrecy of correspondence and telegraphic, data and telephonic communications as inviolable, except, in the latter case, by court order, in the situations and manner established by law for purposes of criminal investigation or the fact-finding phase of a criminal prosecution. Also, Article 7(III) of the Civil Rights Framework for the Internet (Law No 12,965) guarantees the inviolability and secrecy of online user communications, with exceptions only permitted by court order.

Digital signature and encryption

Companies and individuals can request a digital signature (known as ICP-Brasil), issued through a certificate by the National Institute of Information Technology, according to Provisional Measure 2,200/2001, establishing the Brazilian Public Key Infrastructure – ICP-Brasil, which ensures the authenticity, integrity and legal validity of documents in electronic format. The rules established by the management committee of ICP-Brasil determine that the signature associates an entity or a person with a pair of cryptographic keys, through asymmetric cryptography. Thus, when a document is encrypted with the public key, it can only be decrypted with the corresponding private key.

11. COVID-19

11.1 Pandemic Responses Relevant to the TMT Sector

In Brazil, several legislations were created to address relevant issues involving the impact caused by the COVID-19 pandemic. Specific to the TMT sector, telecommunications and internet services were included in the list of essential activities, defined as ones that are essential to meet the urgent needs of the community – ie, those that, if not attended, endanger the survival, health or safety of the population:

- Law No 13,989/2020 provides for the use of telemedicine (long-distance patient and clinician contact) during the COVID-19 crisis, and establishes that the Federal Council of Medicine may regulate telemedicine after the pandemic;
- Law No 14,063/2020 provides for the use of electronic signatures in interactions with public entities, acts of legal entities and in health issues, and on software licences developed by public entities, reducing the bureaucracy of electronic signatures in documents to expand access to digital public services;
- Law No 14,075/2020 extends the use of digital social savings account to receive social benefits from the federal government;
- the Department of Education of the State of São Paulo published Resolution No 30/2021, authorising the use of mobile data by providing a SIM card to students in the state public network, in order to try to guarantee access to the contents made by SEDUC-SP, through the São Paulo Education Media Centre (CMSP) and educational platforms – these measures were also adopted by other states, such as Rio de Janeiro and Maranhão.

Contributed by: *Ricardo Barretto Ferreira da Silva, Danielle Chipranski Cavalcante, Juliana Gebara Sene Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto,* ***Azevedo Sette Advogados***

Azevedo Sette Advogados was founded in 1967 and has established, in its five decades of existence, a history of strength, credibility and excellence in legal services. Ethics, quality and respect are the major values in the daily practice of the firm. The firm has a compliance programme establishing rules and regulations regarding the conduct and acts of its partners, lawyers and employees in order to ensure the practices of good business and corporate governance, particularly related to anti-corruption practices. Azevedo Sette Advogados is internationally recognised for providing solutions in different areas of law (full service), covering competently each of these practices, working in consulting and legal and tax advice, preparation of contracts, in the preparation of opinions and preventive legal analysis, as well as in the sphere of judicial and administrative litigation. The firm currently has six offices located in the cities of Belo Horizonte, Brasília, Goiânia, Rio de Janeiro, São Paulo and Recife; it is supported by an extensive network of corresponding firms in South America, North America, Europe and Asia.

The authors of this article are grateful for the contributions of Stefania Mariotti Masetti, Juliana Petrella Hansen, Isabella Lopes Santana, Laís Litran Motta, Carolina Simioni Perdomo, Julyanne Nascimento and Anna Beatriz Medeiros.

AUTHORS

Ricardo Barretto Ferreira da Silva was co-founder and managing partner of two renowned law firms, CFF and BKBG (1975–2004 and 2004–16, respectively), before becoming a senior partner and head of TMT legal practice at Azevedo Sette Advogados. He graduated from São Paulo University (USP) Law School in 1973 and undertook graduate research work in taxation and corporate law at the University of North Dakota, USA (1974). Ricardo is an attorney with experience in corporate, tax, M&A, intellectual property, technology, media, telecommunications, privacy and data protection. His professional credits include: co-founder, vice-president (1989–94) and president (1995–98) of the Brazilian Information Technology and Telecommunications Association; chair of the Membership Latin America Committee (1993–95); and board member (1995–2001 and 2003–05), secretary, treasurer and vice-president (2001–03) of the International Technology Law Association. Ricardo has had various articles published in Brazil and abroad on IP, IT, media, telecom, privacy, data protection, outsourcing and copyright.

Contributed by: *Ricardo Barretto Ferreira da Silva, Danielle Chipranski Cavalcante, Juliana Gebara Sene Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto,* ***Azevedo Sette Advogados***

Danielle Chipranski Cavalcante is a partner at Azevedo Sette Advogados, practising in the areas of litigation, TMT and data privacy. With solid theoretical and practical knowledge in civil law and civil procedure, acquired in 17 years of exclusive practice in the area, she is responsible for the strategic management of administrative, judicial and alternative dispute resolution claims, dealing with clients from various branches of activity, performing direct contact with clients to define strategies, preparation and review of high-complexity procedural pieces, guidance of the team in the preparation of procedural documents, reports and procedures. She also prepares responses to consultations, involving several areas. Her education includes a Bachelor's degree from Pontifical Catholic University of São Paulo (PUC-SP), 2008, and a specialisation degree in civil procedure at Pontifical Catholic University of São Paulo (PUC-SP), 2014. She has co-authored several articles in her areas of expertise.

Juliana Gebara Sene Ikeda is a partner at Azevedo Sette Advogados. She acts in the areas of technology, media and telecommunications, focusing on contractual, regulatory, intellectual property, copyright, and life sciences matters. Her education includes a Bachelor's degree, from the Pontifical Catholic University of São Paulo (PUC-SP), 2006; a specialisation degree in contracts, at Getúlio Vargas Foundation (FGV), 2010; and an LLM in Intellectual Property, provided by the University of Turin and the World Intellectual Property Organization, 2013. Juliana co-ordinates projects in order to structure technology companies in Brazil and assists clients with the preparation of legal opinions, contracts and memos, especially addressing intellectual property and regulatory matters. She is co-author of a number of articles in the areas of digital law and technology.

Contributed by: *Ricardo Barretto Ferreira da Silva, Danielle Chipranski Cavalcante, Juliana Gebara Sene Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto,* ***Azevedo Sette Advogados***

Lorena Pretti Serraglio is a senior associate at Azevedo Sette Advogados and co-ordinator of its privacy and data protection area. She acts in the areas of technology, media and telecommunications. She is a consultant of the Special Data Protection Commission of the Federal Council of the Brazilian Bar Association. Lorena has an MBA in electronic law from Escola Paulista de Direito. She attended the School of Internet Governance run by the Brazilian Internet Steering Committee, and graduated from a course on protection of personal data and privacy provided by Data Privacy Brasil. Lorena is a co-author of various articles and books, one of which was elected by the Superior Court of Justice as an appropriate work for understanding privacy and data protection in Brazil. She is also a speaker on digital law, cybersecurity and data protection. Lorena co-ordinates projects to assist clients with compliance with the Brazilian General Data Protection Act and the preparation of legal opinions, contracts and memos in the areas of digital law, privacy and data protection.

Sylvia Werdmüller von Elgg Roberto is an associate at Azevedo Sette Advogados. She acts in the areas of technology, media and telecommunications, focusing on telecommunications matters. Her education includes a Bachelor degree from Mackenzie University Law School, Brazil (1993) and a postgraduate degree in Digital Law from EPD – Escola Paulista de Direito, Brazil (ongoing, 2021–22), and courses in Compliance and Business Integrity from IDP – Instituto de Direito Público; Contract Law, Data Protection and Legal Aspects of Innovation from ESA – Escola Superior de Advocacia; and Political Science from IBPEX – Instituto Brasileiro de Pós-Graduação e Extensão. She has co-authored articles in the area of telecommunications and associated subjects.

Azevedo Sette Advogados

Av. Pres. Juscelino Kubitschek 1327
11º andar
04543-011
São Paulo
SP
Brazil

Tel: +55 11 9 9292 3172
Fax: +55 11 4083 7601
Email: barretto@azevedosette.com.br
Web: www.azevedosette.com.br

Azevedo Sette
ADVOGADOS