
CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2023

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

Brazil: Law & Practice

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

Law and Practice

Contributed by:

Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto Azevedo Sette Advogados see p.15



Contents

1. Metaverse	p.3
1.1 <u>Laws and Regulations</u>	p.3
2. Digital Economy	p.4
2.1 <u>Key Challenges</u>	p.4
3. Cloud and Edge Computing	p.6
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.6
4. Artificial Intelligence and Big Data	p.7
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.7
5. Internet of Things	p.8
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.8
6. Audio-Visual Media Services	p.10
6.1 <u>Requirements and Authorisation Procedures</u>	p.10
7. Telecommunications	p.11
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.11
8. Challenges with Technology Agreements	p.13
8.1 <u>Legal Framework Challenges</u>	p.13
9. Trust Services and Digital Entities	p.13
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.13

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

1. Metaverse

1.1 Laws and Regulations

The metaverse is the virtual environment in which people, through various technologies (such as augmented or virtual reality, NFTs, crypto-active, blockchain and avatars), seek to reproduce and interact with the real world. Although the metaverse is at a stage of technological development around the world, when it comes to a regulatory framework, there is still a long way to go.

In Brazil, so far, there are no specific laws or regulations for the metaverse, and no legal cases or court decisions have considered the matter thus far. It is possible that in the coming years there will be discussion about the regulation of the relations performed in the metaverse, besides the application of the already existing laws, such as the following.

- Consumer Protection Code (Law No 8,078/1990), which establishes principles and standards of consumer protection and defence and its Decree No 7,962/2013, which regulated electronic commerce providing for the consumer's right to information about the products and services offered, as well as the registration data of suppliers and the service channels they offer, to facilitate customer service and provide for the right to regret. Thus, in the case of a purchase and sale, or provision of services to a consumer in the metaverse, it is possible that the application of this legislation will be questioned.
- Industrial Property Law (Law No 9,279/1996), which preserves the rights of creators and their inventions, ensuring the registration of patents, industrial and model designs, trade marks, etc. With the increasing popularity and the consequent development of more advanced tools to access the metaverse, new applications for software and device patents, and the creation of other trade marks may arise.
- Copyright Act (Law No 9,610/1998) providing for protection of the creation, reproduction, publication, distribution, etc., of literary, artistic, or scientific works. With the large-scale distribution of these works within the digital space, the misuse, misappropriation or exploitation of moral and patrimonial rights of digital products may arise.
- Brazilian Internet Act (Law No 12,965/2014), which establishes principles, guarantees, rights and obligations for the use of the internet in the country and its Decree No 8,771/2016 which regulates the law by establishing procedures related to the retention and protection of data by connection providers and applications, and points out transparency and inspection measures regarding personal data and private communications.
- Labour Reform (Law No 13,476/2017), which introduced a new chapter to the Consolidation of Labour Laws (a Brazilian labour regulation) providing for work outside the employer's premises, with the use of information and communication technologies (teleworking) and the recently enacted Law No 14,442/2022 which regulates the details of teleworking in the country. People working in the metaverse can give rise to labour issues.
- Brazilian Data Protection Act (Law No 13,709/2018), which aims to regulate the processing of personal data in the Brazilian territory, including in digital media, by individuals or legal entities, of public or private law, in order to ensure the free development of the personality and dignity of the natural person, protecting their fundamental rights of freedom and privacy. It is very possible that the processing of personal data will have its limits

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

questioned in the metaverse, mainly about where controllers and processors would be located and which laws could be applied.

- Decree No 9,854/2019, which establishes the National Plan for the IoT aiming to implement and develop the IoT in Brazil, based on free competition and free movement of data, subject to information security and data privacy guidelines. The integration of IoT in the metaverse can contribute to an accurate representation of an object or an individual with very specific details collected from the real world.

The metaverse experience will require a series of solutions that aim to deal with some challenges that are already present (and others that will arise), such as:

- interoperability between cryptocurrencies, for the purchase of goods and/or services;
- verification systems and tools for proving personal identities (and their respective representations);
- security, privacy, and data protection, in view of the innovative ways of processing such data;
- issues about intellectual property with regard to territoriality, licensing, unauthorised use, copyright, royalties, patents, etc;
- issues about civil and criminal liability;
- debates about the competent jurisdiction to prosecute a claim related to an obligation contracted in the metaverse;
- social issues about misinformation, racism, misogyny, inappropriate behaviour, harassment, etc; and
- physical and mental health issues caused by prolonged immersion.

2. Digital Economy

2.1 Key Challenges

The digital economy in Brazil results in billions of daily online connections among people, companies, devices, data, and processes. Technological evolution has changed the way society interacts and consumes products and services. The speed at which technology reaches business models and industries means that governments and society need to be brought up to date much faster. There is a need for the legislature to move as fast as the digital economy, as companies often need opinions and solutions that are not regulated in Brazil at a given moment.

Brazil has been moving towards adequate regulation of several digital economy services, as illustrated by the examples below.

- Artificial Intelligence – Bill No 21/2020 proposes regulating the development and use of AI in Brazil. This bill is being analysed by the Brazilian Congress and is eagerly awaited by the digital environment. It is worth noting that AI is one of the subjects in stage 3 (one year – six months) of the Regulatory Agenda of the National Data Protection Authority (ANPD), which is expected to issue guidelines on AI that will also serve as a basis for the development of other rules that may be necessary to discipline the AI system.
- Telemedicine – With the COVID-19 pandemic, teleconsultations were regulated on an emergency basis in Brazil. In view of the modality's efficiency, in May 2022, CFM Resolution No 2,314/2022 was published to regulate telemedicine.
- Start-ups – Complementary Law No 182/2021, also known as the Legal Framework for Start-ups, is aimed at improving innovative entrepreneurship in Brazil and

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

leveraging the modernisation of the business environment.

- **Transportation apps** – Law No 13,640/2018 regulates the operation of paid private individual passenger transportation in Brazil.
- **Data Protection** – The General Data Protection Act (LGPD - Law No 13,709/2018) establishes that the processed data of individuals must be used in compliance with the law.
- **Financial Technology** – Fintechs became regulated in 2018 through Brazilian Central Bank Resolution No 4,656/2018.
- **Internet** – The Brazilian Internet Act (Law No 12,965/2014) disciplines the use of the internet in Brazil by providing principles, guarantees, rights and duties for those who use the network, as well as determining guidelines for state action.
- **E-commerce** – Law No 7,962/2013, known as the E-commerce Law, regulates the Consumer Protection Code in relation to e-commerce; this law contains specific provisions about transactions conducted between an online store and its consumer.
- **Electronic signatures** – Provisional Measure No 2,200-2/2001 regulates the use of electronic signatures in Brazil, establishing the Brazilian Public Key Infrastructure (ICP-Brazil), and Law No 14,603/2020 classifies signatures into simple electronic signature, advanced electronic signature and, finally, qualified electronic signature. The three types of signature characterise the level of trust in the identity and the expression of will of its titleholder, and the qualified electronic signature has the highest level of reliability based on its norms, standards and specific procedures.
- **Software** – Law No 9,609/1998 regulates software protection, its commercialisation, and stipulates rights and duties regarding its use.

Although the Brazilian legislature has approved various laws that touch upon digital economy, technology is always evolving and is innovative by nature. In this context, the absence of regulations for specific sectors may be the biggest challenge in relation to digital economy. This absence signifies legal uncertainty for companies and society, difficulty in applying the law, insecurity for investors, and limitation on guidance for clients and internet users, who are not always aware of the legal changes.

Nonetheless, the Brazilian government has taken steps towards promoting digital transformation in the country, through the implementation of the Brazilian Strategy for Digital Transformation (SinDigital). The purpose is to harmonise the federal executive initiatives linked to the digital environment, to harness the potential of digital technologies towards sustainable social and economic development, innovation, increased competitiveness and productivity, among other objectives.

This initiative is composed of the Brazilian Strategy for Digital Transformation (E-Digital), its thematic pillars (split between enabling and digital transformation pillars) and a governance structure. These are set forth by Federal Decree No 9,319/2018, which implements SinDigital and the Brazilian Strategy. SinDigital is co-ordinated by the office of the President's Chief of Staff.

The digital transformation pillars comprise digital transformation of the economy and of the government. On the other hand, some of the enabling pillars are:

- technology infrastructure and access to information and communication technologies, including increased access for the population to the internet and digital technologies;

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

- trust in the digital environment, relevant for ensuring a safe, trustworthy digital environment for services and consumption, respecting the citizens' rights;
- education and professional capacitation, for educating society in the use of advanced technology and preparation for the future of labour; and
- international dimension, for strengthening Brazil's presence and promoting regional integration in digital economy.

The 2018-22 initial E-Digital agenda ended up getting expedited with the COVID-19 pandemic, and the government issued a 2022-26 update after an evaluation process that included public consultations, meetings with experts and other initiatives.

In the above context, it will be important to follow up on the digital transformation expected to take place in Brazil, based on the governmental initiatives, on the legislation updates, and on the private sector inputs and demands.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Although there are not specific laws about cloud services in Brazil, many local laws refer to this matter, including the following.

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

set out by the MCI 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, irrespective 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 this 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:

- 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 surrounding personal data processing requirements such as security of the data, which may be intensified when new providers are added to the service; and
- cloud computing leads to considerable transfers of personal data, involving many different parties and crossing borders between countries, including outside Brazil, which 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.

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

Brazilian Central Bank's Resolution No 4,658, replaced in 2021 by Resolution No 4893, establishes requirements for cloud services to financial institutions. This ruling has established important obligations on companies regulated by the Brazilian Central Bank, such as specific rules for internal policies relating to cybersecurity and the cloud environment in general.

The Brazilian Superintendence of Private Insurance (SUSEP) has also published standard cybersecurity rules to be followed by insurance companies and their service providers, which are also applicable to cloud services in general (Circular No 638/2021).

Complementary Norm No 14/IN01/DSIC/GSIPR, established in 2012 and amended in 2018, has the objective of setting guidelines regarding the use of technologies in government agencies. More specifically, it addresses cloud computing and the aspect 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 is worth mentioning.

The data and information of the contracting agency must reside exclusively in the national

territory, including replication and backups. This requirement is justified by the need to provide the contracting agency with all the guarantees of Brazilian law, as the client 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; and
- the contractual provisions must ensure that the information in the provider's custody will be processed with confidentiality and cannot be used by or provided to third parties without authorisation under any circumstances.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

The use of AI is currently being discussed in Brazil through Bill No 5,691/2019, which establishes the "National Policy for Artificial Intelligence", with the goal of stimulating the formation of a favourable environment for the development of technologies in AI. This bill is the result of a union of other previous bills that discussed the topic:

- Bill No 5,501/2019 – intended to establish the principles for the use of AI and regulate its use;

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

- Bill No 872/2019 – intended to provide for the ethical frameworks and guidelines that underlie the development and use of AI; and
- Bill No 21/2020 – intended to create the legal framework for the development and use of artificial intelligence by public authorities, companies, and individuals, and the text established principles, rights, duties, and governance instruments for AI.

The National AI Policy establishes as its core principles:

- inclusive and sustainable development;
- respect for ethics, human rights, democratic values and diversity;
- protection of privacy and personal data; and
- transparency, security, and reliability.

The bill also states that AI should:

- respect people's autonomy;
- preserve people's intimacy and privacy;
- preserve the bonds of solidarity between people and different generations;
- be intelligible, justifiable, and accessible;
- be open to democratic scrutiny and allow for debate and control by the population;
- be compatible with maintaining social and cultural diversity and not restrict personal lifestyle choices;
- contain safety and security tools that allow human intervention where necessary;
- provide traceable decisions without discriminatory or prejudiced bias; and
- follow governance standards that ensure ongoing management and mitigation of potential technological risks.

Pending the regulation of AI in Brazil, since there are no specific laws about the matter, other legislation may impact the way AI is used and

may dictate rules and obligations for the parties involved, such as data privacy rules, internet use, and the Consumer Protection Code, for example.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Decree No 9,854/2019 instituted the National Internet of Things (IoT) Plan, aimed at improving the quality of life, fostering competition, increasing productivity, and integrating Brazil into the international landscape, in addition to other objectives. Health, cities, industries, and rural environments are priorities for IoT solutions.

According to this plan, 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, in turn, 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.

The provision of IoT/M2M solutions is not regulated in Brazil. However, the connectivity required for the transmission of data between the solution's devices might have an impact on the activity, since telecommunications services are regulated activities, being subject to the provisions of Law No 4,972/1997 (General Telecommunications Law, LGT) and the regulations issued by the National Telecommunica-

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

tions Agency (ANATEL), requiring a licence from ANATEL for their provision.

As per the LGT, VAS refers to activities that involve adding new utilities related to the access, storage, presentation, movement, or recovery of information to a telecommunications service supporting it, with which it is not confused. The LGT also stipulates that telecommunications services are activities enabling the offer of transmission, emission or reception of symbols, characters, signs, writings, images, sounds or information by wire, radio-electricity, optical means or any other kind of electromagnetic process.

Therefore, two situations should be considered.

- If the solution contracts the necessary connectivity from a third-party telecommunications provider holding the applicable license, the IoT/M2M provider is deemed user of the telecommunications service supporting the application, as such not being subject to telecommunications regulatory rules or to ANATEL's control. In this case, the tax on services (ISS) is due, the rates of which vary according to the applicable municipality.
- In case the solution encompasses both the VAS (related to the IoT/M2M application) and the telecommunications service (related to devices' connectivity), the solution provider is subject to telecommunications regulatory rules and ANATEL's control, and it should hold the relevant authorisation. Moreover, in this case, the state tax on circulation of goods and services (ICMS) is due, which has rates higher than ISS rates.

Furthermore, connected devices are deemed communications products using a radio-electric spectrum for information propagation. As such, they should comply with technical requirements

issued by ANATEL, and be certified and homologated by the same agency.

Prior licensing with ANATEL is also required for radiocommunication transmission stations to operate; however, Law No 14,108/2020 exempted stations integrating M2M communications systems from such prior licensing, and exempted said systems from the payment of certain fees until December 2025.

Importantly, although the implementation and development of IoT in Brazil is based on free competition and circulation of data, there must be compliance with information security and personal data protection guidelines. In this regard, several laws and regulations may apply, including:

- Federal Constitution provisions on 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 No 9,296/1996 provides that the interception of information technology, telematics, telephone communications, etc, is a crime;
- Law No 12,737/2012 provides for cyber-crimes and classifies disclosure of proprietary information as a crime;
- Law No 12,965/2014 (Brazilian Internet Act) sets principles and rules for ensuring privacy and data protection in internet use;
- Decree No 8,771/2016 sets security standards for the custody, storage, and processing of personal data and private communications by connections/applications providers;
- Law No 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 Telecommunica-

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

tions Sector) establishes conduct and procedures to promote security in telecommunications networks and services and protect critical structures; and

- ANATEL's Act 77/2021 provides for cybersecurity requirements for telecommunications equipment.

In addition, reliable and stable networks are fundamental for the IoT. In this regard, 5G technology began being implemented in Brazil in 2022, and is expected to boost the IoT market, fostering innovation and impacting local economy and society. Minimum security requirements for 5G networks were set by the Office of Institutional Security of the Republic Presidency's Normative Instruction 4/2020.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Audio-visual and media (broadcasting) services are regulated, maintained and exploited by the Federal Union. However, the Brazilian Telecom Code (BTC) allows individuals to execute broadcasting services through the due concessions, authorisations or permissions to be granted for renewable and successive terms of ten (radio broadcasting) or 15 years (television broadcasting).

The process begins with the publication of a notice; the interested parties present proposals that will be sent to the President of the Republic after the analysis by the competent body and issuing of an opinion. A prior licence is required for broadcasting stations, which must be required after registration of the concession contract by the Public Finance Court. If the sta-

tion is approved, the private licence is to be issued within 60 days.

The authorisation/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 individuals naturalised as Brazilian for more than ten years (this must be proved by documents submitted to the competent bodies on a yearly basis), who will obligatorily carry out the administration activities and establish the content of the programming;
- contractual amendments must be submitted to the executive branch within 60 days;
- the transfer of the concession, authorisation or permission to third parties depends on prior approval by the competent body;
- the broadcasters' information, entertainment, advertising and publicity services are subordinated to the educational and cultural purposes inherent to broadcasting, aiming at the best interests of the country;
- radio stations are obliged to rebroadcast the official information programme of the Brazilian Republic called "A Voz do Brasil" on a daily basis (except on weekends, holidays and other specific occasions);
- the same person cannot participate in the administration or management of more than one concessionaire, licensee or be authorised of the same type of broadcasting service in the same location;
- broadcasting organisations, including television, must allocate at least 5% of their time to the broadcasting of news services; and
- executives or partners cannot have suffered condemnations related to the ineligibility criteria provided for in specific law.

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

The fees to be paid are fixed, taking into account the total costs of the services, the amortisation of the invested capital and the formation of necessary funds for the conservation, replacement and modernisation of the equipment, and extensions of the services.

Application providers, such as platforms on which user-generated content such as videos and photos is posted are regulated by specific law regulating the use of the internet in Brazil, so the above-mentioned requirements do not apply to application providers.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

According to the LGT and complementary rules (eg, those issued by ANATEL), 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 executor's own use or provided to groups of users selected by the provider, and interconnection to other networks is prohibited).

The following are the main communications technologies 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 between 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 or conditioned access services are not allowed.
- Conditioned access service distributes audiovisual content by means of any technology, process, electronic media and communication protocol, with access based on a paid subscription.
- Private limited service is restricted-interest service which 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 No 13879/2019 stipulates that concessionaires might request ANATEL to adjust the concession into an authorisation, if certain requirements are met by the interested party.

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

Exploitation of telecommunications services in the private regime depends on ANATEL's prior authorisation. However, the following exceptions exist.

- 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 case of community-interest services, there is less than 5,000 users; however, the provider should inform ANATEL prior to the start of the activities.

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
- 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 ANATEL Resolution

720/2020. Prior notification to ANATEL regarding the services that 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 to and not confused with the telecommunications services supporting them (eg, instant messaging – 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 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 radio-electric spectrum for the propagation of information should comply with the applicable technical requirements, in addition to being certified and homologated by ANATEL.

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

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

As the law and case law in Brazil have not yet addressed the matter in depth, technology agreements must be regulated in detail. The main challenges of these agreements in Brazil are probably related to IP rights, service levels, liability, and data privacy. The continuous development of technologies is essential and agreements shall clearly regulate the ownership of existing intellectual property and future intellectual property developed during the commercial relationship between the parties involved.

Regarding software licence agreements, as software is 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, backups, disaster recovery, and business continuity.

Liability is always also a significant issue. Although 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 of copyrights” are null and void (Article 10), limitation of liability is allowed and case law varies a lot with regard to the possible caps to indemnifications regarding technology contracts.

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

such agreements constantly involve the international transfer of personal data, a subject that is pending regulation by the Regulatory Authority, mainly regarding the approval of binding corporate rules and the issuance of standard contractual clauses, among other mechanisms provided for in the LGPD.

Finally, note that, as a rule, technology transfer agreements, which include IP licences, know-how licences, and software licences (if the software source code is transferred) shall be registered with the Brazilian National Institute of Industrial Property (INPI) for the following purposes:

- to produce effects in relation to third parties;
- to allow tax deductibility for the licensee of amounts paid as royalties and technical service fees; and
- to legitimise remittances of royalties abroad (if licensor is foreign).

Nonetheless, Law No 14,286/2021, which entered into force on 31 December 2022 and regulates the Brazilian exchange market, actually amends Law No 8,383/91 and, as a result, these so-called “technology transfer agreements” will not need to be registered in order to allow royalty payments abroad.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Brazil has had an advanced digital signature structure since the year of 2001, when it established the Provisional Measure No 2,200-2 (MP 2,200-2), regulating the use of electronic signatures in Brazil and creating the Brazilian Public

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

Keys Infrastructure (ICP-Brasil). The ICP-Brasil is composed of a managing authority and a chain of certifying bodies, which are entities accredited to issue digital certificates.

Through this methodology, each digital certificate belongs to a person and has a pair of encrypted keys, which must be in their exclusive control, use, and knowledge. The rules established by the ICP-Brasil management authority determine that when a document is encrypted with the public key; it can only be decrypted with the corresponding private key, which means that the digital signature associates an entity/person with a pair of encrypted keys, through asymmetric encryption.

According to MP 2,200-2, electronic documents are considered public or private for all legal purposes, and the content of documents electronically produced with the certification of ICP-Brasil are considered authentic regarding the signatories thereof. In addition, it is important to highlight the difference between digital and electronic signatures. Digital signatures use ICP-Brasil infrastructure through a digital certificate issued by the ICP-Brasil. On the other hand, the electronic signature does not use a digital certificate issued by ICP-Brasil. Although the legal presumption of authenticity and integrity is applicable only to documents signed within the ICP-Brasil framework, the MP 2,200-2 states that it does not prohibit the use of other means intended to prove the authorship of documents in electronic format, including those using certificates not issued by the ICP-Brasil, provided that such use is accepted in advance by the parties.

Therefore, agreements and documents in general can be signed with digital or electronic signatures. However, certain entities only accept documents signed using digital certified signatures issued by ICP-Brasil for validation purpose, such as government authorities and boards of trade. In this regard, Law No 14,063/2020 has emerged with the objective of expanding access to digital public services by reducing the bureaucracy of electronic signatures in documents. This Law amends MP 2,200-2 and provides for the use of electronic signatures in interactions with public entities, acts of legal entities, and in health issues, as well as on software licences developed by public entities.

The term “Digital Identity” has no standard definition in Brazil; however, it can be defined as the way in which an individual is represented and documented online. There are several distinct identifiers that can represent a digital identity, such as:

- name;
- date of birth;
- login credentials to online services;
- email;
- passport number;
- social security number;
- browsing behaviour; and
- online shopping.

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

Azevedo Sette Advogados was founded in 1967 and has a leading market team of over 500 professionals with extensive experience, solid academic backgrounds from distinguished educational institutions in Brazil and abroad. The staff works in Azevedo Sette Advogados' five offices located in São Paulo, Belo Horizonte, Brasília, Rio de Janeiro, and Recife to meet the client needs. In addition, the firm is supported by a broad worldwide network of correspondents and partners. Azevedo Sette Advogados works closely with its clients, providing ethical and effective legal solutions. The firm is always seeking creative and efficient ways to offer complete solutions that help clients reach

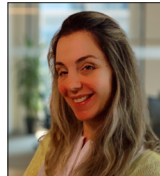
their goals in accordance with their needs and strategic planning. The firm assists more than 1,200 active clients monthly with activities ranging from industrial, services and commerce sectors to government, private investors, and investment funds. Azevedo Sette Advogados and its team are recognised as leaders in Brazil in multiple areas of law, in particular M&A, contracts, projects and infrastructure, civil litigation and arbitration, TMT, etc. The authors would like to acknowledge the contribution of Danielle Chipranski Cavalcante, Camila Sabino Del Sasso, Bruna Evellyn Pereira Bigas, Carolina Simioni Perdomo, Ingrid Bandeira Santos and Gabriela Soares Mussalam.

Authors



Ricardo Barretto Ferreira da Silva is a senior partner at Azevedo Sette Advogados. He works in the areas of corporate, tax, M&A, IP, TMT, privacy and data protection. He has held the

following positions, among others: co-founder, Vice President (1989-94) and President (1995-98) of the Brazilian Association of Technology, Information and Telecommunications Law; Chair of the Latin America Committee (1993-95); Member of the Board (1995-2001 and 2003-05), Secretary, Treasurer and Vice-President (2001-03) of the International Technology Law Association; Chairman of the Legislation Committee (1991-92); Member of the Council (1991-93); and legal advisor (1992-93) of the American Chamber of Commerce São Paulo. He has also edited and co-authored numerous publications and articles on varied topics.



Juliana Gebara Sene Santos Ikeda is a partner in the TMT Advisory area of the São Paulo office, focusing on IP. She has over 15 years of experience in providing legal assistance to

national and international clients in consultations involving contractual and brand protection issues. She has co-authored articles and books in the areas of IP, technology and regulation.

BRAZIL LAW AND PRACTICE

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



Lorena Pretti Serraglio is co-ordinator of the privacy and data protection area of the São Paulo office. She is a consultant for the Special Data Protection Commission of the Federal

Council of the Brazilian Bar Association. Lorena is co-author of several articles and books, one of which was elected by the Superior Court of Justice as an essential work for the understanding of privacy and data protection in Brazil. She is a professor of digital law at the Digital Marketing Graduate Programme at Senac São Paulo and is also a speaker on digital law, cybersecurity and data protection. Lorena is a reference for technology companies.



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. She has co-authored articles in the area of telecommunications and related subjects.

Azevedo Sette Advogados

1327, Presidente Juscelino Kubitschek Avenue
11th floor
International Plaza II Building
04543-011
São Paulo/SP
Brazil

Tel: +55 11 4083.7600
Fax: +55 11 4083.7600
Email: barretto@azevedosette.com.br
Web: www.azevedosette.com.br

Azevedo Sette
ADVOGADOS

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com