Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2023

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

Brazil: Law & Practice

Japyassú Resende Lima and
Fabiana Lopes Pinto Santello
Lopes Pinto, Nagasse

practiceguides.chambers.com

BRAZIL

Law and Practice

Contributed by:
Japyassú Resende Lima and Fabiana Lopes Pinto Santello
Lopes Pinto, Nagasse see p.17

Contents

1. Basic National Regime

1.1 Laws

In Brazil, at least until 1988, there was no specific legislation on the protection and security of personal data. It was only with the Federal Constitution of 1988 that the theme was highlighted, especially with Article 5, X, which, however, referred to the initial concepts of "intimacy" and "private life". An expansion of the subject only came in 1996, with Law 9,296, which dealt with the inviolability of communications. But it still was not sufficient.

In 2011, came the Law of Access to Information (Law 12,527), whose objective was to present an indirect regulation of the constitutional rule of 1988. In 2012, a new advance arrived, with Law 12,737, which criminalised the invasion of personal communication devices for access to personal data. Two years later, it was the turn of Law 12,965, the "Civil Framework of the Internet", whose purpose was to reaffirm the right to privacy.

Only in 2018, with Law 13,709, the "General Data Protection Law", or LGPD has the country passed legislation objectively designed to regulate, protect, and discipline the processing and security of personal data. Based almost entirely on the General Data Protection Regulation (GDPR) of the European Union (EU) (EU Regulation 2016/679), the LGPD only entered into force in September 2020, except for its penalties, which could not begin to apply until August 2021.

Finally, in 2022, the protection of personal data was included in the Federal Constitution as a fundamental right, with special privileges (Article 5, LXXIX).

1.2 Regulators

The Brazilian regulatory model imitates the GDPR, with a "vertical centralisation". Regulation is part of a "hard core", usually represented by the Constitution, which runs along the central axis (legal framework) and ends in the branches (regulation and rules).

This architecture admits some radicality, in which the regulation assumes a "horizontal" profile, reaching not only those that directly engage with the processing of personal data, but the entities that exercise some regulation of the agents of treatment (LGPD, Article 5, IX).

Thus, there are two classes of regulators: the principal, which receives prerogatives from the primary source (the Constitution and LGPD), and the derivative, whose regulatory power stems from the fact that the activities of a given treatment agent are under its regulation.

The main Brazilian regulator is the *Autoridade Nacional de Proteção de Dados* (ANPD), as provided for in the LGPD and approved by Decree 10,474/20. Though initially thought of as an arm of the executive branch, since linked to the Presidency of the Republic, recently the ANPD has gained the status of a municipality and began to make up part of the structure of the Ministry of Justice, perhaps to strengthen its performance. Among derived regulators there are some entities, such as the *Banco Central do Brasil* (Law 4,595/64), the *Agência Nacional de Transportes Terrestres* (ANTT) (Law 10,233/01) and the *Comissão de Valores Mobiliários* (CVM) (Law 6,385/76).

Although the ANPD argues that the punitive measures referred to in the LGPD are of exclusive application by the main regulator, this is not exactly true, as there are penalties substantially

like those of the LGPD that can be imposed by the secondary regulator. Thus, the sanctions applicable by the ANPD can perfectly coexist with the sanctions imposed by the secondary regulator, especially if the facts assessed by both regulators are related to the protection of personal data.

1.3 Administration and Enforcement Process

Brazilian legislation on personal data establishes a process of sanctions and their means of challenge.

In a nutshell, the process is as follows.

- it begins with the supervisory process by the ANPD, which verifies the organisation's support for the LGPD.
- The process may be monitoring, guidance, prevention or repression (the penalties of Resolution 1 cannot be immediately applied).
- If the supervised agent does not adjust its procedures, the regulator may apply the sanctions.
- Even in this case, regulatory authorities and agents may sign a conduct adjustment, to be completed within a certain period.
- In the event of a penalty, the regulator must comply with the criteria:
  (a) compliance with the general interest;
  (b) adequacy between means and purposes, formalities essential to the guarantee of rights, simple forms;
  (c) respect for the rights of interested parties;
  (d) official operation of the administrative process (without prejudice to the actions of the interested parties); and
  (e) legal interpretation to ensure the fulfilment of the public purpose.
- The regulated organisation has means of defence; however, Resolution 1/20 begins by declaring (Article 38) that there is no way to appeal the decision of the regulator that opened the sanctioning process, which calls into question the right to appeal. First, the Constitution says that no law can exclude from judicial assessment an injury or threat to the law (Article 5, XXXV); second, the Constitution affirms (Article 5, LV) the principle of broad defence; and third, the Federal Administrative Procedure Law (Article 2, paragraph 1, X), applicable to proceedings before the regulatory authorities, determines that it is the right of the interested party to appeal as it deems necessary.
- According to the Notice of Infringement, the regulated agent has ten working days to defend itself, including for evidence and other elements; then, the regulated agent has ten more working days, before the Instruction Report, to respond to the evidence and other elements collected; finally, the agent will be called to comply with the decision, or to make a final appeal, within ten working days, addressed to the Board of Directors.
- If the regulated agent does not agree with the decision of the council, it may appeal to the judiciary.
- Since the ANPD is now part of the structure of the Ministry of Justice, discussion has gained momentum over whether, in the case of a final decision of the ANPD, and before taking the matter to the judiciary, the penalised agent could submit an improper hierarchical appeal – the legislation seems to allow this exit, but only time will tell.

1.4 Multilateral and Subnational Issues

The Brazilian system of protection and guarantee of personal data is recent (2018), but has been under discussion for more than a decade.

Although the legislation has a low level of interaction with the legislation of members of the Asia-Pacific Economic Cooperation (APEC), some issues are examined on both sides. The protection of personal data in cross-border or non-border trade, for example, is a discussion of direct interest of Brazil and APEC, considering the so-called "inherent risks" of unregulated transfer, equalisation of legal norms, alignment between commercial parties and alternative means of conflict resolution.

Another point that brings Brazil closer to discussions in international forums is related to cybercrimes, especially those that make personal data vulnerable. But Brazil has made little progress in this field, although it is the fifth country most affected by events related to this subject. Even with the publication of Law 14,155 (2021), which strongly criminalises crimes that use electronic devices, personal data is still a matter of high vulnerability.

Very recently, Brazil has expressed interest in joining the OECD, but to do so will have to move forward and make progress in terms of real and material initiatives in the protection of personal data and regulation of fair and legal processing acts. The case of the European Electronic Privacy Directive (Directive 2002/58/EC), amended in 2009, is emblematic: the EU is already discussing escalating the issue into even more complex legislation, but Brazil does not even have any fundamental guidelines on the subject.

1.5 Major NGOs and Self-Regulatory Organisations

The subject of data protection and security in Brazil is new, and so there are a limited number of independent bodies dedicated to maintaining industry standards in safeguarding data.

There has been no co-ordinated push in this area, but certain initiatives have emerged. This is the case of some platforms – such as the LGPD Third Sector Portal, whose objective is to publicise discussions and proposals on privacy and security in terms of data in the "third sector", and InternetLab, which promotes initiatives around personal data, especially those that circulate in "freedom-free" environments.

Regarding NGOs, Brazil does not yet have relevant active entities.

1.6 System Characteristics

Brazil has adopted the "omnibus" regime: legislation of higher origin, linked to a constitutional (federal) rule, regulates security, processing and privacy issues related to personal data.

The cultural and conceptual differences in a topic as complex as personal data and in a country as vast as Brazil have led the legislator to the "omnibus" regime, to reduce legislative disparities that could arise or prevent local decisions (especially in judicial terms) from "imploding" the fundamental concepts and principles related to personal data and its protection.

The problem, copying the European system, is that Brazil did not, unlike the old continent, have a conceptual legacy of privacy protection and its relationship with personal data. That is why it elected the option of a "national" law, a legal framework that is at the same time engine and booster, but with an inhibiting bias of local and sectoral initiatives.

Another aspect in favour of the Brazilian model is that, with a "national" law, regulation can occur vertically or horizontally, and cover all activities and all sectors, productive or not. The market may complain about Brazilian legislation, but it

is undeniable that the choice of "lex omnibus" derived more from an economic and historical context than from a government option.

This is the case, for example, of border initiatives, such as start-ups, SPACs, asset exploration funds and others, which, by their structure, cannot be regulated, in an aspect as important as personal data, by merely local or sectoral legislation.

1.7 Key Developments

Brazil has dealt with some pioneering initiatives, such as banking and financial regulation. This topic makes the legal sector more interested in personal data.

While legislation, since 2018, has made little progress, especially in terms of operationality, other countries are moving to expand the issue of personal data and create more layers of protection for owners.

Problems, such as the sharing of personal data, provided for in the LGPD (Article 5, XVI), in an environment of arrangement of instant payment, or within the scope of open banking, have brought headaches for regulators and the financial sector. A leakage of personal data linked to these agreements calls into question the theme of the "regulator of the regulator". This is because if the financial regulator cannot be the personal data regulator, someone needs to regulate that regulator with regard to personal data, mainly because the protection of that data is a fundamental right and the law that gives them security is a "national" law.

There are no relevant disputes involving these problems, but it is a matter of time before they arise. With financial regulators from all over the world, linked to international rules (IFRS, GAAP, CPSS/BIS, and TC/IOSCO), and the *Banco Central do Brasil*, the concern is not less. The use of personal data related to instant payment agreements, capital transfer, securities clearing and foreign exchange transactions can undermine the credibility of the financial ecosystem and undermine the national effort to improve personal data protection regulations.

1.8 Significant Pending Changes, Hot Topics and Issues

Pending changes and hot topics on the horizon over the next 12 months include:

- Schrems alternatives;
- anonymity of personal data;
- accompanied self-regulation;
- data compliance assessment and assisted compliance;
- chambers for the compensation of personal data;
- dispute resolution chambers for matters of personal data;
- codes for the retention of personal data;
- contracts for the representation of personal data;
- data and artificial intelligence (AI) and internet of things (IoT);
- data obtained during the COVID-19 pandemic (protected or "social interest");
- personal data in the banking sector;
- electronic data protection officers;
- e-privacy for personal data considered restricted by its holder;
- governance of cryptography;
- governance of personal data in a transnational environment;
- metaintelligence platforms
- proliferation policies; and
- processors on demand.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The idea of the "omnibus law" is related to the principle of "rational regulation": all behaviour of regulated agents tends to be more uniform, compatible and manageable than if the legislation adopted were that of the sectoral model. A relationship in which there is personal data being processed brings very important angles: the first is that this type of relationship can last longer than one thinks, and the second is that, if shared, personal data cease to "belong" to the universe and its holder, becoming part of the "data assets" and another part, at least for a while.

This all gives the relationships in which personal data are involved a characteristic that may not be present in other phenomena: "data communication". For example, if one of the parts of the relationship is in a place where there is regulation of the privacy of personal data, and the other in a different place, where the regulation does not exist or is different, or less or more intense. In fact, there is a legal asymmetry that is difficult to resolve. Equal asymmetry also occurs if the related parts are from non-analogue sectors, with differentiated regulations. For this, the "omnibus" rule works best.

Expanding the scope of personal data security and privacy standards is a justification that compensates for the potential difficulties of the omnibus system. It is worth remembering that centralised regulation does not always mean concentrated regulation; it is always feasible for regulation to allow a certain measure of "sectorisation" it it does not compromise the essential part of the rule and the role of the main regulator (classic).

Cases in the European Union (under the GDPR) China (under the PIPL) and Indonesia (with RUU Cipta Kerja), show that the model is more alive than ever, and can be considered even in the case of high regulatory concentration structures.

2.2 Sectoral and Special Issues

Sensitive Data

Brazil's legislation speaks of sensitive data explicitly, following, for example, the GDPR and standards of other countries, such as the United Kingdom. In it, there is not exactly a definition of sensitive data, but a reference framework in relation to which the data can be considered sensitive (Article 5, II).

The idea of sensitive data is that there are elements that relate directly to intimate and private aspects of the individual, so that they have the right to keep this data under strict reservation and to share it only for well-defined and objectively determined purposes.

For the controller, the processing of sensitive data may be necessary, but also very problematic. For example, it must be able to demonstrate that treatment is strictly necessary and feasible, and that it fulfils one of the legal bases of the LGPD (Article 11). In this scenario, this means that the treatment must be linked to a real and pressing need and that cannot be achieved by less invasive means.

In Brazil, this data can be divided into three classes:

- sensitive to individuals (eg, biometrics);
- sensitive to your intimate or private personal activities (eg, religious conviction); and
- sensitive to their specific personal condition (eg, health and life choices).

Other issues may include the following:

- Right to forget – recently, the Supreme Court (in Special Appeal 1,010,606) said that the right to forgetfulness is not compatible with Brazilian law, and for this reason argued that the passage of time, in isolation, is not a reason to prevent facts from being publicly disclosed.
- Navigation – the Brazilian legislation has chosen to consider navigation a private activity and therefore the data circulating in it about the individual are under protection and its collection (via cookies, FLoC, tracking, etc) should be preceded by a specific policy by the controller.
- Tracking navigation – this allows, for example, the collection of data to identify fake profiles, hate messages, fake news and the like. For the Civil Framework of the Internet of Brazil, the practice is prohibited, but some actions have been employed, such as the installation of applications, which, in practice, because they are a "choice" of the individual, can be used for tracking.
- A Bill (10,052) intends to address this situation, as it provides for the tracking of internet activities for the acquisition of goods and services, which can collect even more data from the holder.

2.3 Online Marketing

The boundary between unsolicited communications and irregular processing of personal data is merely symbolic.

In the EU, the "access to consumption" may require authorisation (not really a consent) from recipients, and the main recommendations remain that they do not use an individual's email for mass communications and not to use premarked boxes for an authorisation.

Brazil is actively preparing to regulate the practice, but only the state of São Paulo, by Law 17.334/21, has specific rules to avoid unwanted calls and unsolicited commercial messages (or capture of preferences and profiling). But in any case, the Consumer Protection Code (Law 8,038/90, Article 39, III) provides that the supply of unsolicited goods or services is "abusive practice" and therefore prohibited. More recently, Bill 310/22 wants to go further: it prohibits telemarketing companies from unwanted contact of people, including the use of robots.

Similarly, targeted advertising, especially if aimed at the most vulnerable people, such as children, adolescents and the elderly, is considered abusive and prohibited by consumer law.

2.4 Workplace Privacy

The work environment also benefits from the concept of privacy. But there is a problem: in times of remote work, a remnant of the pandemic, it is not so simple to define a "workplace", which can be as much the physical environment as anywhere where the worker performs their tasks, at home or in a public park. The consensus seems to be that the typical "workplace" is the physical point of the company or unit in which the worker provides their services.

Organisations have been concerned about the privacy of personal data, as workers displaced from their physical locations also need to manage this data for their activities, but outside the "aseptic" and protected environment of companies. Therefore, the number of companies that adopt strict privacy policies in the processing of personal data outside its walls only grows, with the signing of terms of confidentiality and non-disclosure of data, digital security commitments and secure management.

Codes of conduct and integrity in personal data privacy and internal notices of processing personal data have also become commonplace and in most cases there is no interpretation that this violates the privacy of workers. The Labour Court in Brazil has made clear that employees have an obligation not to violate the personal data of third parties, especially if this is what is expected of their activities in the company.

Another point of concern is e-discovery: employees have been caught practising e-discovery, and thereby having access to personal data considered "non-proprietary" (not belonging to the employer). The problem is more serious than it seems, because judicial, technical and legal evidence can be obtained by this method and then "marketed" to stakeholders. In addition, workers who manipulate large masses of personal data from their activities are subject to paid external capture so that, in the practice of electronic discovery, they provide strategic data to competitors or competitors of the employer.

2.5 Enforcement and Litigation

Regulators have at their disposal a still small arsenal (in Brazil) to open investigations into violations of the laws of security and privacy of personal data.

In the case of the LGPD, the regulator (ANPD) can directly interfere with an organisation's data processing activities, and there are three basic possibilities for this: (i) regulatory intervention, if the controller has been accused of systematically violating the rights of the data holder in terms of personal data; (ii) suspensive intervention (Article 52, X); and (iii) punitive intervention.

Typically, the regulator starts an investigation against the treatment agent and assesses the severity of the violations committed, ensuring the agent a broad defence and production of evidence. The main basis for this is the "conduct of the processing agent", the actions and measures it has adopted or failed to adopt (and that led to the vulnerability of its controls) and documentation in the processing of personal data. That is, even before the evidence of infringement, the regulator may consider the nature and severity of the conduct as a means of reaching the most advanced legal assessment of the facts.

The regulator generally considers violations as direct or indirect, and may include cross-sectional violations. Direct violations stem straight from the agent's conduct, indirect ones come from worsening the effects of their conduct, and the cross-sections consider the impact of the violation on other agents and other regulators.

The regulator may also apply the penalties provided for in the LGPD, usually under the "verticalisation" regime (from the least serious to the most severe). Even penalties may vary due to the nature and quality of the breach, because if the same breach can be considered and punished by more than one regulator (classic and derivative, for example), it is possible that the original penalty be aggravated by the secondary penalty (applied by a non-directly regulating body of personal data).

Private disputes for privacy or intimacy violations are quite common, including through so-called class actions, in which many actors (assets or liabilities) come together in search of legal rights or duties that apply to everyone. Increasingly, collective defence entities have been concerned about the issue of "indistinct privacy," a new concept called "collective privacy." In this case, there are no specific individuals directly affected by a privacy violation, but an indistinct group of them, harmed by the violation.

The leakage of personal data, for example, has served as a topic of discussion. Consumer relations organisations and prosecutors have already positioned themselves on this, especially in relation to the many data leaks related to the payment arrangements articulated by the *Banco Central*. Almost a thousand legal actions are taking place in the Brazilian courts on personal data, from leaks to abuse or misuse.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

According to the LGPD (Article 4, III), its rules do not apply if the processing of personal data is related exclusively to public security, national defence, state security or investigation and prosecution of criminal offences.

This means that, in principle, if the processing of data is directed to any of these purposes, the agent (usually public) will not be subject to the LGPD.

Thus, the government does not necessarily need to ask the regulator for the right to access databases for crimes and criminal prosecutions.

However, this does not mean that the authority that accesses the data is free to use it as it pleases. For example, the LGPD provides that the public administration that accesses the data may not transfer it to third parties, with some exceptions, and that the regulatory authority may act against the government if it violates the legal rules.

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

According to the LGPD (Article 4, III), its rules do not apply when the processing of personal data is objectively related to public security, national defence, state security or investigative activities and repression of criminal offences.

Thus, in principle, if the processing of data is intended for any of those purposes, the agent is not submitted to the LGPD.

Therefore, the public agent does not need to ask the regulator for permission to access databases on intelligence, state defence or national security.

As per **3.1 Laws and Standards for Access to Data for Serious Crimes**, the authority accessing the data is not free to use it as it likes or transfer it to third parties.

3.3 Invoking Foreign Government Obligations

Brazil has formally joined the Budapest Convention (Cybercrimes Convention). The document requires each country to maintain the legal authority to compel organisations based in its territory to disclose data (including personnel) that is in those companies' custody, regardless of whether the organisation also has custody of data from other countries.

This means that Brazil may, even without formal membership in any free-traffic agreement of personal data for certain purposes, such as the American Cloud Act, have to examine requests for capture and assignment of data. The Cloud Act (Clarifying Lawful Overseas Use of Data Act) was passed in 2018 by the US Congress, and is basically the result of the limits of the Stored Communications Act (1986). It dictates that US

data and communications companies must allow access to customer data, even if their repositories are outside US jurisdiction. This created a problem for the GDPR, which, two months after the Cloud Act, linked access to data stored in a foreign country to that country's prior court authorisation.

However, a request from a foreign government based on the Budapest Convention, or in an agreement like the Cloud Act, does not indiscriminately give a private organisation the right to seize the opportunity and request access to the personal data included in the government's request. This organisation, based in Brazil or another country, needs to use its own means to have access to the personal data it wants, and is still subject to scrutiny of legislation and the judiciary.

3.4 Key Privacy Issues, Conflicts and Public Debates

Although the Access to Information Act, prior to the LGPD, allowed access to data stored in database of the Ministry of Information, the government has been using the LGPD to deny access to personal data, including for projects of social interest.

A good example of this is the fact that the *Banco Central do Brasil* has signed two co-operation agreements with private entities representing financial institutions. The agreements provide that the monetary authority will share with the institutions a large and important database (the *Identidade Civil Nacional*), which includes sensitive data, such as biometrics of Brazilian citizens.

Different entities and the *Ministério Público Federal* (Federal Prosecutor's Office) are investigating this, and legal representations have been made, including to the *Tribunal de Contas da União* (TCU), which, however, did not see irregularities in those agreements.

4. International Considerations

4.1 Restrictions on International Data Issues

For the LGPD, the international transfer of personal data is a topic to be considered carefully. The argument is that such transfers may mean that data, once outside national jurisdiction, is lost (or dispersed) forever, especially in terms of regulation.

In legislation, international transfer is an exception, both actively (from Brazil out) and passively (from abroad to Brazil).

Such a transfer, according to the LGPD, is only possible:

- to countries or international bodies that ensure the appropriate degree of protection of personal data (similar) to that provided for in the LGPD;
- where it is intended for the protection of the life or physical safety of the holder or third parties;
- where it is the result of a commitment under an international co-operation agreement;
- if the national authority authorises it;
- if items II, V and VI of the LGPD Article 7 are met;
- if it is necessary for international legal co-operation between public intelligence, investigation and prosecution agencies;
- if it necessary for the execution of public order or the legal attribution of the public service;

- if the controller provides and proves the assurance of compliance with the principles, rights of the data subject and the regime for the protection of personal data provided for in this Law – conditions set out in the first four points; or
- if the data holder gives their specific consent.

The import of data via international transfer, although it is recommended that it pass the "entry criteria", is possible based on:

- judicialisation of the transfer–it is not treatment subject to the LGPD, (Article 4, IV);
- the use of the transfer;
- data filters;
- formalisation;
- level of conformity of the origin; and
- verification of the Brazilian destiny.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

An international transfer of personal data, in the LGPD (or GDPR), is a typical data treatment activity (or processing, according to the GDPR) and therefore needs to meet certain legal conditions, including derogations (specific authorisations upon knowledge of the risks involved).

These conditions include that:

- it must be done on an authorised legal basis;
- it must be under one of the possibilities of derogation (LGPD, Article 33; GDPR, Article 9, paragraph 2);
- it should be naturally informed;
- it must be under a legitimate purpose and not prohibited;
- it cannot include excessive data; and
- it must be subject to real measures to protect and contain risks.

In terms of multilateral mechanisms, the transfer of personal data should also be disciplined in a Personal Data Transfer Agreement (PDTA), with clauses that ensure the bilaterality of the data communication arrangement, in any modality. In addition, a data privacy notice is always recommended.

4.3 Government Notifications and Approvals

The legal hypotheses authorising the international transfer of personal data are in the LGPD (Article 33); other than that, the transfer cannot happen, even with derogations.

One of these hypotheses provides that the regulatory authority may authorise transfers, but this requires that the event meets one of the LGPD's viable legal basis. Although the government decided to make an international transfer of data, it is necessary that the case fit Article 33 of the LGPD, and even then it would be up to the regulator to evaluate the "transfer conditions", provided for in Article 35 of that Law.

Normally, public persons referred to in the Access to Information Act (Article 1) may ask the regulator, prior to an international transfer of personal data, to assess the degree of protection of personal data conferred by the country or international body that will receive the data.

4.4 Data Localisation Requirements

In the field of the personal data localisation, one of the points of interest is that the legislation has adopted the principle of irrelevance of location (Article 3), according to which the point at which the data are located is not significant for law enforcement.

But this depends on the certain conditions:

- the treatment operation must be carried out on national territory;
- the purpose of the treatment activity shall be to offer or provide goods or services or to process data from natural persons located in the national territory; or
- the personal data to be treated is collected in Brazil.

Data that, by its nature, purpose, quality, scope and content, must remain on Brazilian soil, cannot be transferred, as is the case for personal data used by research bodies in public health studies (LGPD, Article 13, paragraph 2).

4.5 Sharing Technical Details

Although the LGPD does not explicitly state that elements such as source codes, software and other technical elements should be shared with the government, it is necessary to understand the issue a little better.

First, it is possible for public and private entities to share personal data with each other, provided that the rules of Article 25 of the LGPD are complied with and that the data is used for public purposes, in pursuit of the public interest, for the enforcement of legal powers or in compliance with legal duties of public service.

Secondly, sharing does not necessarily mean violation of copyright protection, as in the case of algorithms, which are not always considered "intellectual products" (Law 9,610/98, Article 8, I). However, it is necessary to consider that the sharing of typical intellectual creations – such as source codes – can lead to legal disputes (Law 9,609/98, Article 2, paragraph 5).

4.6 Limitations and Considerations

Organisations collecting or transferring data in connection with foreign government requests are subject to the LGPD, provided that personal data has been collected in the national territory and that at least one treatment activity on them has been carried out in the country (Article 3).

Under Article 3 of the LGPD, it is not relevant whether the organisation is located in Brazil or abroad, because what determines the application of Brazilian law is the place where personal data was collected and where it was subject to some treatment.

However, in the case of international data transfer between an organisation and the entity that hired it, the transferee is subject to the transfer rules laid down in the LGPD, which means that a viable legal basis (Articles 7 and 11) and compliance with one of the conditions of LGPD's Article 33 will be required.

4.7 "Blocking" Statutes

These statutes are more widespread than before and their rules provide for limitations that, if they do not prevent practices involving personal data, at least create conditions that agents must comply with before acting.

It is true that locks do not always have to do with the security and privacy of personal data and sometimes this is not even the focus, but it is undeniable that one of its effects is to create obstacles to practices that might otherwise be allowed.

For example, the EU GDPR has already been understood as a blocking tool for transfers of personal data to extra-EU agencies, applying Article 49 (1) (d) when it comes to "important reasons in the public interest". This was made more evident with the US District Court's decision (July 2019), calling for the answer to whether the GDPR is a blocking statute under US law.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

Some of these topics are already addressed, directly or indirectly, by the Brazilian LGPD, such as biometrics, facial recognition, pictorial data collection, and personal distinction, profiling, metadata, reverse data, discretion of personal data and ROTMs.

Drones

Currently, there is no specific national legislation on drones and their relationship with personal data, except for the Special Civil Aviation Regulation 94/17, the Brazilian aeronautical regulation, which refers to the need to preserve the private life and intimacy of individuals.

Big Data

The mass (or intensive) acquisition of personal data is strongly impacted by the LGPD. Article 20 provides that it is the right of the holder not only to know on which viable legal basis decisions were taken on the treatment of their personal data, but also to request the reinvestigation, amendment or complementary action of those decisions and, if abuses are found, to obtain redress.

AI

Law 14,108, known as the IoT Law, is not a legal framework on the subject but it creates government tax incentives for IoT-focused technologies.

Brazil does not yet have a legal framework, or regulatory framework, in AI. At the moment, there is only one Bill on the subject (21/20).

Dark Patterns (DPs)

Such patterns, still little known, play a fundamental role in people's consumer choices. Through malicious techniques with the intention of inducing users of web services to make certain choices, manipulating their decisions, DPs have been a cause for concern since the Civil Framework of the Internet (Law 12,965/14).

Fiduciary Duty

The legislation says that a link is formed between controller and holder, and this requires that the controller not only following the legislation, but not frustrating the expectations of the holder.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Brazil does not yet have regulations on the theme of personal data governance, nor has it implemented a regular practice in this area, although the LGPD provides for one (Article 50) and recommends the introduction of practices of data governance in organisations.

What happens is that organisations create, by themselves, governance committees, usually linked to the DPO, so that issues such as risks, management and documentation can be addressed on a legal and technical basis.

Due to Brazil's very recent history in the protection of personal data, there are no specific cases on the subject involving repercussions and penalties. However, it is worth remembering that about 1,000 legal proceedings are ongoing on the subject, and the ANPD, at some point, should be involved in these cases.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

The subject of personal data is new, but a good number of due diligence processes are beginning to value the search for compliance in the treatment of personal data related to transactions between companies.

Investment planning and strategic partnership cases also require partner or invested companies to present an LGPD-related compliance diagnosis and, in many cases, another for the GDPR.

This may include:

- the analysis of operators and sub-operators;
- the value of the need to comply with other laws in the international transfer;
- the value of personal data;
- the value of the systems used in the treatment activities;
- collection of relevant data protection documents, such as policies, procedures, and guidelines;
- consultation on the history of incidents involving personal data and communications related to ANPD and other bodies, as well as with data subjects;
- information on judicial or administrative proceedings relating to the LGPD;
- measurement of the flow of service to the demands of the holders and those involved in the service;
- verification of the existing privacy framework, if there is a DPO and an active privacy committee; and
- verification of technical and organisational measures adopted in the treatment of personal data.

5.4 Due Diligence

In general, and as there is still no procedure book for cases of corporate business due diligence, many companies use the most common best practices, in particular the DTP (diligence transaction practice).

This can include:

- evaluation of the purpose of the treatment/use of the data;
- compliance check;
- service level agreement data;
- non-disclosure agreement data;
- FoT – Free over Transaction (the document, in a business transaction, that shows the data that the parties can freely handle);
- existence of a personal data policy; and
- DPOs and a data committee.

5.5 Public Disclosure

In Brazil, there is still no specific legislation that requires disclosure of an organisation's cybersecurity risk profile. The first reason is that, in terms of protecting personal data, the country needs to make significant progress before instituting a cybersecurity or personal data ranking; the second reason is that such a ranking depends on the maturity of the concepts and principles of data security and privacy.

The fact is that the activities of evaluation, measurement and monetisation of the risks of the treatment of personal data are new in Brazil. An example of this is vulnerability analysis for the classes and categories of manipulated data.

This type of study evaluates four pillars:

- conformity with safety legislation and standards;
- blanks for security incidents;

- resilience to potential threats (internal and external); and
- protection systems in place.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws

Recently, the EU passed the Digital Market Act (DMA), which is due to take effect in 2023 and will impact gatekeepers in the digital sector. Also in the EU, the Digital Services Act (DSA) is ready to take effect in 2024. In the USA, legislative efforts are ongoing, with the American Innovation and Choice Online Act (AICO), which has the support of the US Department of Justice.

As with the GDPR, the DMA and DSA will have repercussions in Brazil, and may even influence some initiatives, such as Bill 2.630, known as the Fake News Project. Thought to deal only with this topic, the Project is moving to include other issues, such as "digital free choice rights", "targeted advertising" and "content moderation", with or without the use of personal data. Another issue that will generate controversy is the moderation of content involving sensitive personal data, and the application of the rules for combined regulation, combining the regulatory agent for personal data and regulatory agents for digital services.

5.7 Other Significant Issues

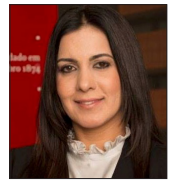
Other significant issues relevant to the regulation of cybersecurity in Brazil include:

- the service level agreement (SLA) applicable to the conformity of personal data and its treatment;
- personal data as a legacy in international business transactions;
- governance of algorithms;
- sharing of public databases and their effects on organisations;
- leadership of investigations of security incidents in the case of treatment agents and members of different organisations;
- DPO technical standards policies;
- permanent international transference of personal data;
- massive (or intensive) data treatment – regulation and limits;
- data treatment in environments regulated by other authorities – such as compatibilisation, determination and application of penalties; and
- critical data treatment vulnerabilities.

Lopes Pinto, Nagasse is based in São Paulo. The firm provides expertise across many areas, including corporate and business law, tax and planning, data protection (LGPD, GDPR and PIPL), contracts, regulation, digital assets, blockchain, transportation, logistics, labour, infrastructure, agribusiness, banking and finance, bioscience, civil law, corporate governance, compliance, tech law, and legal risks. The team of highly skilled professionals possesses in-depth experience of national and multinational companies and law firms, and the modus operandi of organisations and businesses. Lopes Pinto, Nagasse Advogados prides itself on being a highly ethical firm, focused on achieving results and providing excellent service to its clients. Since 2006, it is has been recognised as one of the most highly regarded law firms by Época, a Brazilian news and analysis magazine.

Authors

Japyassú Resende Lima is a partner at Lopes Pinto, Nagasse Advogados. He specialises in regulation, data protection (LGPD and GDPR), transportation, digital assets, blockchain, infrastructure, logistics, bioscience, agribusiness, compliance, corporate governance, and corporate law. He has a DLM (Université Bordeaux), LLM (Fordham University) and a Master's in digital business (UK) and regulatory law (USP/Université de Montreal). He also has a doctorate in law (Université de Sorbonne) and completed postgraduate studies in business law (ESADE), economic law (Duke University) and data privacy law (LSE). He is a member of the Order of Attorneys of Brazil and the International Bar Association.



Fabiana Lopes Pinto Santello is a founding partner at Lopes Pinto, Nagasse Advogados. She has completed both a doctorate and a Master's in tax law. She co-ordinates and lectures on corporate tax law at Fundação Armando Álvares Penteado (FAAP), and is also a director of communications at IASP. She is a published author in the field of tax and business law. She also speaks at national and international conferences and events on tax and other legal matters.

Lopes Pinto, Nagasse

Rua Helena, 235
4º andar
Vila Olímpia
São Paulo
Brazil
04552-050

Tel: +55 11 2665 9200
+55 11 98311 0108
Fax: +55 11 2665 9200
Email: contato@lopespinto.com.br
Web: www.lopespinto.com.br

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