Data Protection & Privacy

Contributing editor
Wim Nauwelaerts

GETTING THE

Brazil

Ricardo Barretto Ferreira and Paulo Brancher
Azevedo Sette Advogados

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Although there are several rules related to data privacy in Brazil, so far there has been no consolidation of all the applicable rules into a single law. The Brazilian Federal Constitution states that the privacy, private life, honour and image of persons are inviolable, and that the right to compensation for economic and non-economic damages resulting from violation thereof is guaranteed. It also states that the confidentiality of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, upon court order, in the event of, and in the manner established by law for, purposes of criminal investigation or criminal procedural discovery.

Moreover, the Brazilian Internet Bill of Rights (Law 12,965/2014) (the Internet Law) and Resolution 3/2009 of the Internet Steering Committee in Brazil (www.cgi.br) establish principles for ensuring privacy and data protection. Under the Internet Law, any collection, use, storage or processing of personal data through the internet is subject to the users' express consent and must be limited to the purposes that justified it. The recently enacted Decree 8,771 of 11 May 2016, which regulates the Internet Law, establishes rules on the request of registration data by public administration authorities, as well as on the security and confidentiality of records, personal data and private communications.

In addition to constitutional protection, privacy and data protection are mentioned in specific and different laws, including, but not limited to, the Consumer Protection Code (Law 8,078/1990), the Civil Code (Law 10,406/2002), the Law on Public and Private Archives and the Bank Secrecy Law (Complementary Law 105/2001).

There is an important bill of law (PL 5,276/2016) for personal data protection and privacy in progress in the Brazilian Congress that is intended to meet the OECD guidelines and the European Union's data protection standards. This bill of law has received all sorts of suggestions and comments by the civil society and gone through discussions in various Commissions of the Brazilian Congress for a long time already. There is no expectation as to when this process will be finished.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no specific authority in charge of data protection in Brazil, although the Decree 8,771/2016 provides that supervision and verification of infringements of its rules (including data protection rules) will be conducted in a tripartite manner. The National Telecommunications Agency (Anatel) will act under Law 9,742/1997 (Telecommunications Law), the Consumer General Secretariat, subordinated to the Ministry of Justice, will act in relation to the Consumer Protection Code, and the Administrative Council for Economic Defense (CADE), will do it in case of violations against the economic order. Such bodies, as well as other bodies and entities of the federal public administration, will act in a collaborative manner following the guidelines fixed by the Internet Steering Committee (www.cgi.br).

3 Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The Internet Law, without prejudice to other civil, criminal or administrative provisions, provides that any breach of data protection or privacy regarding the collection, storage, custody and treatment of records, personal data or communications by internet connection or applications providers will be subject, as applicable, to the following sanctions, that may be applied on an individual or cumulative basis:

- warning for a corrective action;
- a fine of up to 10 per cent of the revenues of the economic group in Brazil in its most recent financial year;
- temporary suspension of its activities; and
- prohibition of certain activities.

The disclosure of proprietary information can also be classified as a crime of secret disclosure or violation of professional secrecy, or both, with a penalty of detention or a fine, or both. Law 12,737/2012, which provides for cybercrime, also establishes a penalty of three months' to one year's detention and a fine for those who break into a third-party computer device to obtain or destroy data or information without the express or implied consent of the corresponding owner.

The Brazilian Consumer Protection Code determines a penalty of imprisonment or fine, or both, to those who block or hinder access by the consumer to information about him or her contained in files, databases or records, or those who are expected to know that information relating to the consumer as contained in any file, database, record or registration is incorrect and, nevertheless, fail to immediately rectify it. The same statute sets forth administrative penalties imposed by the authorities in charge of protecting consumer rights, and such penalties include fines, intervention and counter-advertising.

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

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

As mentioned below, so far Brazil has no consolidated and specific law regarding data protection. General principles and rules such as the Federal Constitution, the Internet Law, the Civil Code and the Consumer Protection Code apply to all Brazilian citizens. Moreover, there are special provisions that apply only to certain sectors and areas of activity.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Brazilian Federal Constitution ensures the secrecy of correspondence, telegraphic, data and telephone communications, except upon court order, in the cases provided for in the law for the purposes of criminal investigation or procedure.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas?

Some of the specific data protection rules applicable to special sectors and areas of activity are listed below:

- the Internet Law (Law 12,965/2014), Decree 8,771/2016 and Resolution 3/2009 of the Internet Steering Committee in Brazil (www.cgi.br) establish principles and rules for ensuring privacy and data protection in the use of internet in Brazil, mainly regarding the activities developed by the internet service providers;
- the Consumer Defence Code (Law 8,078/1990) provides for several rights of consumers as regards personal information in 'consumer databases and reference files', such as the right to access and modify or correct their data, wherever they are, and the right to ask for and obtain the deletion of such data;
- the Positive Credit Registry Law (Law 12,414/2011) permits the collection of 'positive' credit information (ie, fulfilment of contracted obligations) but prohibits the register of excessive information (ie, personal data which is not necessary for analysing the credit risk) and sensitive data;
- the Brazilian Telecommunications Law (Law 9,472 1997) grants privacy rights to consumers in relation to the telecommunications services;
- the Bank Secrecy Law (Complementary Law 105/2001) requires that financial institutions (and similar entities) hold financial data of individuals and entities in secrecy, except under judicial order issued for purposes of investigation of any illegal acts or criminal procedural discovery;
- the Civil Code (Law 10,406/2002) grants general privacy rights to any individual and the right to claim against any attempt to breach such rights by any third party; and
- Resolution 124/2006 of the National Supplementary Health Agency imposes a fine on healthcare insurance companies of up to 50,000 reais for the breach of personal information related to the health conditions of a patient.

7 PII formats

What forms of PII are covered by the law?

There are no restrictions on the scope of protection for private information.

8 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

No. Brazilian law shall apply to all cases where PII belongs to a Brazilian individual. Moreover, the Internet Law sets forth that any process of collection, storage, custody and treatment of records, personal data or communications by connection and applications service providers, in which at least one of these acts occurs in the national territory, shall comply with Brazilian law and regulations regarding rights to privacy, confidentiality of personal data and secrecy of private communications and records. The aforementioned provision applies even if the activities are carried out by a legal person located abroad, as long as the services are offered to the Brazilian public or at least one member of the same economic group owns establishments in Brazil.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners?

As a general rule, all processing or use of PII is covered by the Brazilian privacy and data protection laws and regulations. However, considering that so far there is no consolidated and specific law regarding the matter, the situation shall be verified on a case-by-case basis under Brazilian law.

Legitimate processing of PII

10 Legitimate processing - grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The general rule under Brazilian law is the need for express consent of the individual regarding the use and processing of their PII. Also, the Internet Law assures internet users of:

- express consent on the collection, use, storage and processing of personal data, which should occur irrespective of the other contractual terms; and
- clear and complete information on the collection, use, storage, treatment and protection of their personal data, which can only be used for purposes that justify their collection, are not forbidden and are specified in the service agreement or terms of use.

11 Legitimate processing - types of PII

Does the law impose more stringent rules for specific types of PII?

Brazilian law does not make express distinction between personal and sensitive data. Nevertheless, information regarding religion, sexual orientation, political position, health, etc, can be construed as sensitive data, and its improper use or collection can be deemed to be a crime depending on the case (eg, racism, discrimination).

According to the Brazilian Consumer Protection Code, consumer-related databases must not contain negative information for a period exceeding five years.

See question 6.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Under specific circumstances, notification may be required under Brazilian law. The Consumer Protection Code, for instance, imposes a notification in writing to the consumer for the opening of a file, record or any personal or consumer data, in cases where such record has not been requested by the consumer.

13 Exemption from notification

When is notice not required?

In particular cases, personal data may be disclosed by service providers if so required by a court order and according to the law, without notice to the corresponding individual. In these cases, the judge will be responsible for taking the necessary measures to ensure confidentiality of the information received and to safeguard the privacy, private life, honour and image of the user.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

As already mentioned, as a general rule, the collection and use of personal data requires prior, clear and express consent of the individual. Also, the Federal Constitution assures Brazilians and foreign nationals the right

individuals have the right to access all data stored about themselves, and request changes, corrections and even removal from a certain database.

Taking into consideration that consumers and employees are construed as the weaker party of a relationship under the Brazilian framework, the collection and use of their PII require a more careful degree of control.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

As a general rule, the PII collected or stored must be objective, necessary and accurate, otherwise the individual may demand immediate correction or exclusion of such data from the databases and also request compensation for damages.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

According to the Brazilian Consumer Protection Code, consumer-related databases must not contain negative information about a consumer for a period exceeding five years.

Moreover, the Internet Law establishes that 'application service providers' (incorporated as legal entities, and that exercise their activities in an organised manner, professionally and with economic purposes) must keep records of access to internet applications (ie, the set of information regarding date and time of use of a particular internet application from a particular IP address) under secrecy, in a controlled and safe environment, for a minimum term of six months, in accordance with the regulation (not enacted yet). In the provision of internet connections, it is incumbent on the autonomous system administrator to keep records of the connection logs (the set of information regarding the initial and final date and time of internet connection, its duration and the IP address used by the terminal for sending and receiving data packets) under the same conditions, but for at least one year. Both periods may be extended upon the request of the police, administrative authority or public prosecutors.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The Internet Law grants individuals the right to have clear and complete information about the collection, use, storage, processing and protection of their personal data, which can only be used for purposes that justify their collection, are legal and are provided for in the corresponding service agreement. The law also forbids the custody of PII that may be construed as excessive considering the initial purposes for which consent was given.

In addition, Decree 8,771/2016 provides that administrative authorities must request registration data with specification of the data owners stating the legal grounds of their express competence and the reason for access thereof, any non-specific request being forbidden. Moreover, public federal administration bodies are required to adopt transparency measures and publish statistical reports on registration data requests.

The Consumer Protection Code follows the same principles: the collection and processing of personal data are justifiable depending on the services to be provided.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

All use of PII should be clearly communicated and authorised by any individual whose data will be collected or stored, or both. In this regard, it is worth mentioning that a Brazilian telecommunications company was fined 3.5 million reais by the Department of Consumer Protection of the Brazilian Ministry of Justice for abusive practices against consumers under the Brazilian Protection Code, and breach of good faith and privacy because it collected, monitored, used and redirected data traffic from internet users for business purposes and without the appropriate and express consent from such consumers.

Security

19 Security obligations

What security obligations are imposed on PII owners and service providers that process PII on their behalf?

The Internet Law brings a few security requirements, which are specifically provided by Decree 8,771/2016. Internet service providers must follow guidelines for security standards in the handling of personal data and private communications, such as:

- definition of responsibilities and authentication mechanisms so as to ensure individualisation of the persons who will have access to and handle data, as well as create detailed access logs;
- creation of detailed inventory of access to connection records and access to applications containing time, duration, identity of the designated employee or responsible for the access in the company and the accessed file; and
- the management solutions of records through techniques that ensure the inviolability of data, such as the use of encryption. The safeguard and availability of connection logs and access data, as well as PII and the content of private communications, must meet the requirements of preservation of intimacy, privacy and image of the parties directly or indirectly involved.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

There is no specific provision that requires notification to the regulator or individuals in the case of security breaches. However, considering the finality principle, and all other rights granted to those individuals whose data are being collected, it is assumed and expected that any security breaches that may harm those rights will lead to the individuals being informed. In that way, individuals may take actions to maintain the privacy of their personal data or information, without extinguishing the provider's liability for any damages arising from such security breach.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

There is no specific regulation on this matter in Brazil.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

The internal processes required are the ones already mentioned, regarding safety and transparency of activities. All individuals must know which data are being collected, where and how they are being stored and what they are used for.

Registration and notification

23 Registration

Are PII owners and/or processors of PII required to register with the supervisory authority? Are there any exemptions?

As per our answer to question 2, so far there is no authority in charge of data protection in Brazil.

24 Formalities

What are the formalities for registration?

No specific registration is required for owners and processors of PII under Brazilian law in addition to the formalities needed for the exercise of a company's activities in Brazil.

Update and trends

The Brazilian law currently in force does not provide legal certainty on the processing of personal data by private entities. The Internet Law is a great step towards data protection and privacy in the internet environment; however, it does not assure privacy and data protection as a whole. This is principally because it is applied only to internet connection providers and internet application providers, and does not encompass several important issues such as the processing of sensitive data, interconnection and transfer of personal data. The bill of law aims to solve this lack of legal certainty.

According to the bill of law, personal data processing activities shall comply with several principles, such as purpose, transparency, security, free access by the data subject, prevention of damages and non-discrimination.

Consent is the key issue to legitimate personal data processing. The bill of law expressly provides that personal data processing is only allowed under free, express, specific and informed consent. This means that generic consent for personal data processing shall be invalid and anyone that obtains personal data by error, fraud, state of need or coercion is subject to penalties.

The bill of law also establishes special rules on sensitive personal data processing, which can only take place under special consent, or without consent in certain circumstances, such as the fulfilment of legal obligation.

International transfer is only allowed by the bill of law for countries that provide a level of protection for personal data that is equivalent to the level established in the Brazilian law. If personal data is transferred to a country that does not provide an adequate level of protection, special consent is required.

Security measures and good practices are also required by the bill of law, and private legal persons shall be subject to administrative penalties for any breaches of the standards established in the law, which may be applied by a regulatory agency created by the Brazilian government.

In view of this, despite the fact that there is no expectation as to when the bill of law will be approved, Brazilian and foreign companies that process personal data have attempted to implement policies on privacy and personal data protection, and ultimately maintain transparent corporate governance.

25 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

See question 24.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

See question 24.

27 Public access

Is the register publicly available? How can it be accessed?

See question 24.

28 Effect of registration

Does an entry on the register have any specific legal effect?

See question 24.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The Brazilian legal framework does not contain specific rules regarding the transfer of PII to outsourced processing services. All the aforementioned Brazilian principles, rules and limitations also apply in this case and therefore the express consent of the individual for the collection, transfer and use of its PII is needed.

It is worth mentioning that the Internet Law does not allow for the connection service providers' liability for retaining connection logs being transferred to third parties.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

See question 29.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

As a general rule, the transfer of PII outside the jurisdiction is not forbidden but Brazilian law must be observed.

In this regard, the Internet Law establishes that the Brazilian law and the regulations regarding rights to privacy, confidentiality of personal data and private communications and records apply even if the internet service as the services are offered to the Brazilian public, or at least one member of the service providers' economic group owns establishments in Brazil.

32 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

There is no specific authority in charge of data protection in Brazil.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

There is no specific law in this regard in Brazil; however, based on general principles of law, such transfers cannot impair the applicability of the Brazilian rules or regulations, if such rules or regulations are applicable to such specific PII.

Rights of individuals

34 Access

Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

As mentioned in question 14, the Federal Constitution assures Brazilian and foreign nationals the right to rectify their data.

In addition, the Consumer Protection Code provides that individuals have the right to access all data stored about themselves and request changes, corrections and even its removal from a database. Preventing or hindering a consumer's access to information about him or her, or failing to immediately correct inaccurate information, shall subject the person responsible to detention of up to one year or a fine, or both, and also compensation for damages arising from such inaccuracy.

35 Other rights

Do individuals have other substantive rights?

See question 34.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals who have their PII violated are entitled to pain and suffering and property damages by filing a suit before the Brazilian courts. In this regard, the Brazilian Superior Court of Justice reached a consensus that petitioners are not required to provide evidence of pain and suffering as a result of violation of their privacy, since 'harm is presumed upon violation

of such protected legal interest'. On the other hand, property damages – such as incidental damages and loss of profit – require proof that such damages actually occurred.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals who have their PII violated are entitled to claim their rights before the Brazilian courts, and, depending on the situation in which the violation occurred, individuals may also be entitled to claim certain rights before the consumer protection departments and regulatory agencies as well.

Public prosecutors and authorised associations under the law may also file class actions in the case of extensive violation of collective ('diffuse') interests, including consumer and privacy violations. If such proceeding is successful, courts may impose significant indemnifications to be paid to specific public funds, in addition to any individual indemnifications paid to the individuals.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

There are no further exemptions or restrictions.

Supervision

39 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

There is no specific authority in charge of data protection in Brazil. However, as a rule, administrative orders can be the subject matter of appeals to the Brazilian courts.

Specific data processing

40 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Taking into consideration that the use of 'cookies' is construed to be a monitoring tool, use should be subject to the individual's express consent.

41 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

There are no specific rules in this regard in Brazil, and the general principles and rules shall apply. The Brazilian Advertising Self-Regulatory Council reflects well the need to apply to advertisements on the Internet the same policy adopted for 'conventional' advertisements.

42 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services

Cloud computing services have no specific regulation in Brazil. However, all principles and rules for data protection and cybersecurity are applied thereof.

Azevedo Sette
ADVOGADOS

Ricardo Barretto Ferreira barretto@azevedosette.com.br
Paulo Brancher brancher@azevedosette.com.br

Av. Pres. Juscelino Kubitschek, 2041
Torre E, 16º andar
04543-011, São Paulo
Brazil

Tel: +55 11 4083 7600
Fax: +55 11 4083 7601
www.azevedosette.com.br