THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2022
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADER
Katie Hodgetts

SENIOR BUSINESS DEVELOPMENT MANAGER
Rebecca Mogridge

BUSINESS DEVELOPMENT MANAGERS
Joey Kwok

BUSINESS DEVELOPMENT ASSOCIATE
Archie McEwan

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Leke Williams

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Louise Robb

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.TheLawReviews.co.uk

ISBN 978-1-80449-116-4

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON LLOYD

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

KALUS KENNY INTELEX

KHODEIR AND PARTNERS

K&K ADVOCATES

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 9

BRAZIL

Ricardo Barretto Ferreira, Lorena Pretti Serraglio, Isabella da Penha Lopes Santana, Carolina Simioni Perdomo and Bruna Evellyn Pereira Bigas[1]

I OVERVIEW

The concept of protection of privacy is not an innovation in Brazil. The privacy, private life, honour and image of individuals were considered as inviolable as well as fundamental rights by the Brazilian Federal Constitution of 1988 (the Brazilian Federal Constitution).[2]

After many years of legislative discussions, in 2018 the Brazilian General Data Protection Act (Law No. 13,709/2018 (LGPD)) was enacted.[3] This Law is considered the most important data protection law in our jurisdiction, and represents a big advance and an important step for Brazil, to guarantee the protection of individuals, define limits to data processing for companies and enable the expansion of Brazil's digital economy.

The LGPD came into force in September 2020, during the covid-19 pandemic and after a legislative race. At the end of 2020, the regulatory authority was constituted and its regulatory agenda was published, specifying the topics for discussion and the dates on which each will be addressed. The National Data Protection Authority (ANPD or Authority) is fully functioning and has already issued guidelines regarding the processing of personal data, as will be mentioned in the topic below.

The rights given in Article 5 of the Brazilian Federal Constitution are classified as fundamental rights. As described above, privacy is considered a fundamental right and, recently, the right to data protection was included in this list by the Constitutional Amendment 115 of 2022,[4] which added the item LXXIX to Article 5.

II THE YEAR IN REVIEW

The covid-19 pandemic continued to emphasise the exponential growth of technology in people's daily lives, in companies' activities, in governmental roles, and in the fight against coronavirus. Other privacy-related challenges have arisen, as vaccination status and body

1 Ricardo Barretto Ferreira is a senior partner, Lorena Pretti Serraglio is a senior associate and Isabella da Penha Lopes Santana, Carolina Simioni Perdomo and Bruna Evellyn Pereira Bigas are associates at Azevedo Sette Advogados. The authors would like to thank the following for contributing to this chapter: Juliana Sene Ikeda, partner at Azevedo Sette Advogados.

2 Brazilian Federal Constitution of 1988 (CF/1988). Available at www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

3 Brazilian General Data Protection Act (Law No. 13,709/2018). Available at www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

4 Constitutional Amendment No. 115/2022. Available at http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1.

temperature are considered as sensitive personal health data. Technology has continued to be an important ally in the practice of medicine, in the home office, in online education and in relationships as a whole.

In Brazil, taking into account the context of the LGPD's effectiveness and as companies rush to adapt to the Law's provisions, the ANPD has taken shape and is acting with an initial awareness-raising and educational agenda.

In early 2021, the ANPD published Ordinance No. 11/2021,[5] making public its regulatory agenda for the 2021–2022 biennium, which includes the main data protection issues such as the LGPD for small and medium-sized enterprises, data subjects' rights, data breaches and international transfers. In compliance with the published agenda, in March 2021 the ANPD published Ordinance No. 1, with the Authority's internal regulation, outlining its entire organisational structure for compliance with its legal attributions, and its activities and the main items that will be analysed in the coming months.

In February 2021, the ANPD took another important step in publishing explanations and notification requirements of data breaches on its website,[6] clarifying what constitutes a data breach, what needs to be communicated to the ANPD and in which situations to communicate breaches to data subjects. The web page also includes a template of the communication form.

In May 2021, the ANPD followed up with the publication of two important and robust documents that will guide the actions of the Authority and public and private companies in the processing of personal data, namely: the Guidance on Definitions of Processing Agents and Data Protection Officer;[7] and the Enforcement Rule,[8] which addresses inspections and application of administrative sanctions imposed by the Authority.

The first document considers the concepts of personal data processing agents (controller and processor) and data protection officers (DPO). The guideline intends to establish non-binding directives, developing topics such as legal definitions, respective liability regimes, concrete cases and examples, and frequently asked questions. The ANPD, along with the Superior Electoral Court, has also published, in 2021, a Guideline on the Application of the LGPD by Processing Agents under the Electoral Context,[9] which aims to instruct processing agents that participate in the electoral process. Its purpose is to seek to ensure the protection of data, the individual's privacy, and the fairness of the electoral process, without obstructing the communication between candidate and citizen, which is necessary for the democratic process.

In October 2021, the ANPD issued the Guideline on Information Security for Small Processing Agents,[10] which is defined as a 'guide of good practices addressed to small-size processing agents that, due to the size and possible limitations, often do not have people specialized in security of the information among their staff, and need to improve it in relation to the processing of personal data'.

5 Available at https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313.

6 Data Breach Reporting. Available at https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

7 Guidance on Definitions of Processing Agents and Data Protection Officers. Available at https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf.

8 Enforcement Rule. Available at https://www.gov.br/participamaisbrasil/norma-de-fiscalizacao-da-anpd.

9 Guideline on the Application of the LGPD by Processing Agents under the Electoral Context. Available at https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf.

10 Guideline on Information Security for Small Processing Agents. Available at https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf.

Last but not least, in January 2022 the Authority issued a Guideline on the Processing of Data by Public Agents,[11] which seeks to outline parameters that can assist public entities and bodies in the adequacy and implementation of activities with the LGPD.

Furthermore, the Provisional Measure No. 1,124/2022 altered the nature of the Authority, which until then was only a body of the federal public administration with a transitory legal nature. With the conversion of the Provisional Measure into law, the ANPD will be considered a special independent governmental agency, as defined by Brazilian law as an autonomous administrative entity, decentralised from the Public Administration and not hierarchically subordinated to ministries or the Presidency, placing ANPD on the same level as the Brazilian Central Bank, ANATEL, and other Brazilian agencies. In practice, this will give ANPD more autonomy in terms of its actions and decisions, and more confidence in relation to external bodies, an opportunity in which Brazil will be able to appear on lists of countries with an adequate level of data protection practices.

To be effectively converted into law, the Provisional Measure must go through a process of analysis and approval by the Brazilian National Congress, which can last for 60 days, extendable for an equal period. During this period there will be a recess of the Parliament's work, with the interruption of its activities from 18 July to 31 July, in addition to a presidential election, which may cause a delay in the deliberations on the matter. The current ANPD's Regulations will remain in force and applicable until the Provisional Measure is converted into law, which is expected to occur at the end of August 2022.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The Brazilian Federal Constitution establishes the inviolability of its people's privacy, private life, honour and image as fundamental rights. Recently, the protection of personal data was also considered a fundamental right, through an amendment to the Federal Constitution. For all these standards, the right to compensation for property or moral damages resulting from their violation is ensured.[12] Also, Brazil has a civil regulatory framework for use of the internet: Law No. 12,965/2014 (the Brazilian Internet Law),[13] which establishes principles, guarantees, rights and obligations for the use of the internet in Brazil. Decree 8,771 of 11 May 2016[14] establishes procedures related to data retention and protection by connection and application providers, and points out transparency and enforcement measures concerned with personal data and private communications.

Brazil has enacted the LGPD, which provides for the processing of personal data, including in digital media, by a natural person or legal entity of public or private law, with the purpose of protecting the fundamental rights of freedom and privacy and free development of the personality of the natural person.

11 Guideline on the Processing Data by Public Agents. Available at https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_eleitoral.pdf.

12 Article 5, X, of Brazilian Federal Constitution.

13 Brazilian Internet Law. Available at www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

14 Decree 8,771 of 11 May 2016. Available at www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm.

The LGPD[15] contains core definitions related to data protection, such as:

a personal data: information regarding an identified or identifiable natural person;

b sensitive personal data: personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organisation membership, data concerning health or sex life, genetic or biometric data, in relation to a natural person;

c data subject: a natural person to whom the personal data that are the object of processing refers to;

d controller: natural person or legal entity, of public or private law, that has the competence to make the decisions regarding the processing of personal data; and

e processor: natural person or legal entity, of public or private law, that processes personal data in the name of the controller.

Furthermore, there are other sectoral laws related to the privacy and protection of personal data, including, but not restricted to:

a Law No. 8,078/1990 (the Consumer Protection Code),[16] which sets out data protection principles in consumer relations;

b Law No. 9,472/1997 (the Telecommunications Act),[17] which guarantees measures related to privacy and protection of personal data of telecommunication services users;

c Law No. 10,406/2002 (the Civil Code),[18] which grants the inviolability of the private life of the natural person; and

d Law No. 12,414/2011 (the Positive Credit Registry Act),[19] which is responsible for the formation and consultation of databases with data on credit history, of natural or legal persons.

The Regulatory Authority was created by Provisional Measure No. 869/18 (later converted into Law No. 13,853/2019) and has published several guidelines to guide data subjects, data controllers, and data processors.[20]

ANPD's Resolution No. 2[21] was created in January 2022 to establish guidelines for small processing agents.

ii General obligations for data handlers

Under the LGPD,[22] processing agents have a duty to process personal data for legitimate, specific, explicit and informed purposes for the data subject. Also, the processing must be compatible with the purpose communicated to the data subject and limited to the minimum necessary to achieve its purposes. Other duties relate to an assurance of easy consultation by data subjects about the processing, with clear and precise information, in addition to ensuring

15 Article 5 of LGPD.

16 Consumer Protection Code. Available at www.planalto.gov.br/ccivil_03/leis/l8078.htm.

17 Telecommunications Act. Available at www.planalto.gov.br/ccivil_03/leis/l9472.htm.

18 Civil Code. Available at www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm.

19 Positive Credit Registry Act. Available at www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.

20 ANPD publications. Available at www.gov.br/anpd/pt-br/documentos-e-publicacoes.

21 Resolution No. 2 made by ANPD. Available at www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper.

22 Article 6 of LGPD.

the accuracy, clarity, relevance and updating of the personal data processed. Also, processing agents must use technical and administrative measures that are able to protect personal data from unauthorised accesses and accidental or unlawful situations and must adopt measures to prevent the occurrence of damages as a result of the processing of personal data.

Processing agents are obliged to have one of the following legal bases[23] for the processing to be lawful:

a consent of the data subject;
b compliance with a legal or regulatory obligation by the controller;
c processing and shared use of data must be necessary for the execution of public policies provided in laws or regulations;
d carrying out studies by research entities, ensuring, whenever possible, the anonymisation of personal data;
e it must be when necessary for the execution of a contract or preliminary procedures related to a contract of which the data subject is a party, at the request of the data subject;
f regular exercise of rights in judicial, administrative or arbitration procedures;
g protection of life or physical safety of the data subject or third party;
h protection of health, in a procedure carried out by health professionals or by health entities;
i it is necessary to fulfil the legitimate interests of the controller or third party;
j protection of credit; and
k ensuring the prevention of fraud and the safety of the data subject, in processes of identification and authentication of registration in electronic systems.

In addition to the general duties imposed on data handlers described above, new rules on legal bases might be created.

iii Data subject rights

The LGPD establishes in its Chapter III the systematisation of the rights of data subjects, which can be exercised at any time and upon express request of the data subject, or his or her legally constituted representative. The requested processing agent shall attend without costs to the data subject, within the periods and under the terms as provided in the regulation, by Article 18, Paragraph 5 of the LGPD. Among other things, the LGPD provides for the following rights:

a confirmation of the existence of the processing;
b access to data and information concerning the processing of data subjects, which must be made available in a clear, adequate and ostensible manner;
c correction of incomplete, inaccurate or outdated data;
d anonymisation, blocking or erasure of unnecessary or excessive data or data processed in non-compliance with the provisions of the LGPD;
e portability of the data to another service or product provider, through an express request and subject to commercial and industrial secrecy;

23 Articles 7 and 11 of LGPD.

f erasure of the personal data processed with the consent of the data subject, when permissible; and

g access to information about public and private entities with which the controller has shared data.[24]

Although the above rights are explicitly stated in the LGPD, several of them lack regulation, such as the right to access (Article 9), the right to portability (Article 18, V) or even the right to review automated decisions (Article 20, V). To address these regulatory gaps, the ANPD has determined in its regulatory agenda that it will address the rights of data subjects in the first half of 2022 through a resolution; however, up to this point, the ANPD has not released the resolution on this matter.

iv Specific regulatory areas

In addition to the LGPD, Brazil has other regulations and laws that address the issue of data protection in specific sectors.

In the financial sector, Resolution No. 4.893/2021[25] (which repealed Resolution 4,658/2018[26]) issued by the Brazilian Central Bank (BACEN) provides that the financial institutions shall adopt procedures that take into account the quality of the access controls aimed at protecting the data and information of the institution's customers, issuing requirements for the contracting of processing services and data storage. BACEN also provides for the implementation of Open Banking in Brazil, since 2020, through Joint Resolution No. 1,27 which provides for the sharing of personal data of consumers with financial institutions and other institutions authorised to offer products and services.

The Superintendence of Private Insurance issued Resolution No. 382 in March 2020,[28] listing the protection of personal data as one of the principles to be adopted by insurance companies, capitalisation companies, open private pension entities and their intermediaries. In December 2020, Circular No. 619[29] was issued guiding entities to draw up a data and information security and confidentiality policy, to guide their activities. In July 2021, the Superintendence regulated guidelines, technical requirements, operational procedures, and the minimum scope of data for the implementation of Open Insurance in Brazil, pursuant

24 Article 18 of LGPD.

25 Brazilian Central Bank Resolution No 4.893/2021. Available at https://www.in.gov.br/en/web/dou/-/resolucao-cmn-n-4.893-de-26-de-fevereiro-de-2021-305689973.

26 Brazilian Central Bank. Resolution No. 4,658/2018. Available at https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf.

27 Brazilian Central Bank. Joint Resolution No 1/2020. Available at https://www.in.gov.br/en/web/dou/-/resolucao-conjunta-n-1-de-4-de-maio-de-2020-255165055.

28 Superintendence of Private Insurance. Resolution No. 382/2020. Available at http://www.in.gov.br/web/dou/-/resolucao-n-382-de-4-de-marco-de-2020-247020888.

29 Superintendence of Private Insurance. Circular No. 619/2020. Available at https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/23958.

to Resolution No. 415[30] and Circular No. 635[31] (amended by Circular No. 661/2022),[32] in addition to Circular No. 638[33] that provides for minimum cybersecurity requirements to be observed by entities.

The National Agency for Supplementary Health Services enacted Act No. 443/19,[34] which provides for the adoption of minimum corporate governance practices, with an emphasis on internal controls and risk management, for the purposes of solvency of healthcare plan operators. With the declaration of a pandemic caused by the coronavirus, in April 2020, bill No. 1,998/2020[35] was presented (still in the legislative process) with the aim of authorising and defining the practice of telemedicine throughout the Brazilian territory. Because of the importance of the topic, in May 2022, the Federal Council of Medicine (CFM) released Resolution No. 2,314/2022,[36] replacing the previous standard (a 2002 CFM Resolution)[37] about the use of communication technologies for the provision of medical services. Both texts are not conflicting and seek a common objective which is to guide the practice of telemedicine to protect patients' personal data.

Furthermore, the ANPD signed some important technical cooperation agreements: (1) in March 2021 with the National Consumer Secretariat (SENACON)[38] to among other matters enable cooperation in personal information control actions within the scope of personal data control relationships; (2) in May 2021[39] with the Administrative Council for Economic Defence (CADE) aimed at combating activities that may be harmful to the economy and promoting and disseminating the culture of free competition in services that process personal data; and (3) in November 2021 with the Superior Electoral Court (TSE)[40] to adopt joint actions to promote the proper application of the LGPD and its guidelines during the electoral process.

30 Superintendence of Private Insurance. Resolution No. 415/2021. Available at https://www.in.gov.br/en/web/dou/-/resolucao-cnsp-n-415-de-20-de-julho-de-2021-333272165.

31 Superintendence of Private Insurance. Circular No. 635/2021. Available at https://www.in.gov.br/en/web/dou/-/circular-susep-n-635-de-20-de-julho-de-2021-333254618.

32 Superintendence of Private Insurance. Circular No. 661/2022. Available at https://www.in.gov.br/en/web/dou/-/circular-susep-n-661-de-11-de-abril-de-2022-392869925.

33 Superintendence of Private Insurance. Circular No. 638/2021. Available at https://www.in.gov.br/en/web/dou/-/circular-susep-n-638-de-27-de-julho-de-2021-335760591.

34 National Agency for Supplementary Health Services. Act No. 443/19. Available at http://www.ans.gov.br/component/legislacao/?view=legislacao&task=TextoLei&format=raw&id=MzY3MQ==.

35 Chamber of Deputies. Bill No 1.998/2022 proposed by Federal Deputy Adriana Ventura. Available at https://www25.senado.leg.br/web/atividade/materias/-/materia/153033.

36 Federal Council of Medicine. Resolution No 2.314/2022. Available at https://www.in.gov.br/en/web/dou/-/resolucao-cfm-n-2.314-de-20-de-abril-de-2022-397602852.

37 Federal Council of Medicine. Resolution No 1.643/2002. Available at https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1643.

38 Technical Cooperation Agreement No 1/2021. Available at https://www.defesadoconsumidor.gov.br/images/docs2020/acordo_anpd_senacon_assinado.pdf.

39 Technical Cooperation Agreement No. 5/2021. Available at https://www.gov.br/anpd/pt-br/assuntos/noticias/act-tarjado-compactado.pdf.

40 Technical Cooperation Agreement No 4/2021. Available at https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/comunicacao/noticias/arquivos/acordo-de-cooperacao-tecnica-tse-anpd-lgpd-em-23-11-2021/@@download/file/TSE-acordo-cooperacao-tecnica-anpd-lgpd.pdf.

v Technological innovation

Developers of new technologies must incorporate privacy and data protection in their design. The concept of privacy by design is based on the LGPD principles that ensure technical, administrative and security measures to protect personal data, as well as the effectiveness of such measures in observance of personal data protection rules.

Behavioural advertising

Although there is no specific legislation, the Consumer Protection Code[41] contains provisions that grant overall consumer protection against fraudulent and abusive advertising and coercive or unfair commercial methods, as well as against unfair or imposed practices and terms in the supply of products and services. In addition, the Internet Management Committee in Brazil (CGI.br) has developed a website that contains guidelines for best practices to inform the user and network administrator about spam, its implications and ways to protect against and combat it.[42] Furthermore, the Brazilian Advertising Self-regulation Code[43] regulates the ethical rules applicable to advertising and propaganda.

Facial recognition and biometrics

Regarding facial recognition technologies, although there is no specific regulation of such technologies, there is a series of legislative bills pending in legislative houses, such as Bill No. 4,612 of 2019,[44] which provides for the development, application and use of facial and emotional recognition technologies, as well as other digital technologies designed to identify individuals and predict or analyse behaviours.

Artificial intelligence

At the beginning of 2020, a request for a public audience on artificial intelligence was approved by the Commission of Science, Technology, Innovation, Communication and Informatics. The objective is to instruct two bills: one of these introduces the National Policy on Artificial Intelligence (Bill No. 5,691/2019)[45] and the other sets out the principles for the use of artificial intelligence in Brazil (Bill No. 5,051/2019).[46] Furthermore, Legislative Bill No. 21/20[47] aims to establish the legal framework for the development and use of artificial intelligence by public authorities, private companies, entities and natural persons. The Bill determines that respect for human rights and democratic values, equality, non-discrimination, plurality, free initiative and data privacy must be fundamental in the use of artificial intelligence.

41 Chapter III: Basic Consumer Rights, of Consumer Protection Code.

42 Anti-Spam Working Committee (CT-Spam). Available at https://www.antispam.br/index.html.

43 Brazilian Advertising Self-regulation Code. Available at http://www.conar.org.br/codigo/codigo.php.

44 Legislative House. Bill No. 4,612 of 2019. Available at https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455.

45 Federal Senate. Bill No. 5,691/2019. Available at https://www25.senado.leg.br/web/atividade/materias/-/materia/139586.

46 Federal Senate. Bill No. 5,051/2019. Available at https://www25.senado.leg.br/web/atividade/materias/-/materia/138790.

47 Legislative Bill No. 21/20. Available at https://www.camara.leg.br/propostas-legislativas/2236340.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

The Brazilian Internet Law, in its Article 11, provides that in any operation of collection, storage, retention and processing of personal data or communications data by connection providers and internet application providers, where at least one of these acts take place in the national territory, Brazilian law must be mandatorily respected, including with regard to the rights to privacy, protection of personal data and secrecy of private communications and logs.

Paragraphs 1 and 2 of Article 11 establish that the provision applies to data collected in the national territory and to the content of the communications in which at least one of the terminals is placed in Brazil, even if the activities are carried out by a legal entity located abroad, provided that it offers services to the Brazilian public, or at least one member of the same economic group is established in Brazil.

In a similar way, the LGPD[48] applies to any processing operations carried out by a natural person or a legal entity of public or private law, irrespective of the means, the country in which its headquarters are located or the country where the data are located, provided that:

a the processing operation is carried out in the national territory;

b the purpose of the processing activity is to offer or provide goods or services or the processing of data of individuals located in the national territory; or

c the personal data being processed were collected in the national territory.

The LGPD's Article 33 provides that international transfer of personal data to foreign countries or international organisations of which the country is a member is only allowed when:

a it is to countries or international organisations that provide a level of protection of personal data that is adequate to the LGPD's provisions;

b the controller offers and proves guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided by the LGPD, in the form of:
- specific contractual clauses for a given transfer;
- standard contractual clauses;
- global corporate rules; or
- regularly issued stamps, certificates and codes of conduct;

c the transfer is necessary for international legal cooperation between public intelligence, investigative and prosecutorial agencies, in accordance with the instruments of international law;

d the transfer is necessary to protect the life or physical safety of the data subject or a third party;

e the national authority authorises the transfer;

f the transfer results in a commitment undertaken through international cooperation;

g the transfer is necessary for the execution of a public policy or legal attribution of public service, which shall be publicised;

h the data subject has given their specific and highlighted consent for the transfer, with prior information about the international nature of the operation, with this being clearly distinct from other purposes; or

48 Article 3 of LGPD.

i it is necessary for the controller to comply with a legal or regulatory obligation, for the execution of a contract or preliminary procedures related to a contract of which the data subject is a party (at the request of the data subject) or for the regular exercise of rights in judicial, administrative or arbitration procedures.

The level of data protection in the foreign country or international organisation shall be evaluated by the ANPD. Furthermore, the definition of the content of standard contractual clauses, as well as the verification of specific contractual clauses for a particular transfer, global corporate rules or stamps, certificates and codes of conduct will be carried out by the ANPD in the second phase of its regulatory agenda,[49] scheduled for the first half of 2022, a procedure that is moving forward. Recently, the ANPD opened a public consultation on the matter.

V COMPANY POLICIES AND PRACTICES

Article 50 of the LGPD suggests that data controllers and processors should create standard data protection policies and procedures to mitigate liability. Article 51 of the LGPD also provides that the ANPD should establish technical standards in connection with data privacy issues. However, until this date, ANPD only published cybersecurity guidelines for small processing agents.[50]

Notwithstanding the above, it is considered the best practice for companies (also to mitigate liability) to have a broad number of policies and procedures in place for compliance purposes, as set out below:

a a data privacy policy, which regulates data processing by the company. There may be two different policies in place: one about data protection in general (relating to customers, clients, etc.) and another specifically related to data protection inside the company (regarding company's employees, which should provide training mechanisms, for example). The rules established by this policy have to comply with all the rules provided by the LGPD and the Brazilian Internet Law, as applicable;

b an information security policy and an information and communications technology policy, which establish internal rules for the use of technology devices (computers, mobiles, etc.), cybersecurity standards and guidelines, among other provisions;

c specific policies related to areas that usually process a lot of personal data (e.g., human resources departments, with guidelines on the processing of personal data of candidates pre-hire, during the admission phase and during the employment relationship);

d an employees' monitoring policy, establishing terms, conditions and limits for monitoring employees and their work tools;

e a 'bring your own device' policy, regulating the terms and conditions in the case of employees using their own devices for work activities;

f privacy policies and terms of use for the company websites;

g a cookies policy; and

h a data breach policy and response plan to set forth company procedures in the event of a data security breach, among other things.

49 ANPD's regulatory agenda for the 2021–2022 biennium, established by Ordinance No. 11/2021. Available at https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313.

50 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf.

VI DISCOVERY AND DISCLOSURE

The Brazilian Internet Law establishes rights and guarantees for all users of the internet in Brazil, such as the inviolability and confidentiality of the flow of users' communications through the internet and their stored private communications, except by a court order.

According to Article 22 of the aforementioned Law, any interested party may request a judge to order the entity responsible for keeping the records to provide the connection or access logs to internet applications, for the purpose of creating evidence in civil or criminal legal procedures. This request should contain, under penalty of inadmissibility:

a justified evidence of the occurrence of the offence;
b motivated justification of the usefulness of the requested records for investigation; and
c the period of time to which the records correspond.

It is important to highlight that the judge needs to take the necessary measures to ensure confidentiality of received information, as well as the preservation of intimacy, private life, honour and image of the data subject. The judge may determine the secrecy of justice,[51] including with respect to requests for record retention.

Furthermore, the Brazilian Code of Criminal Procedure (Law No. 3,689/1941)[52] states that judges may request information, including personal data, during criminal investigations and criminal proceedings. Pursuant to Article 3-B, XI, items (a) and (b), examining judges have the power to decide on requests to disclose personal data of users of electronic communications services, including internet, email, telephone and financial data.

Regarding the interception of telephone communications, this may be determined for evidence in criminal investigations and proceedings by the examining judge, *ex officio* or upon request of the competent police authority or the representative of the public prosecution. The interception should comply with the provisions of Law No. 9,296/1996,[53] and will depend on an order of the competent judge of the main action,[54] under the secrecy of justice.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The ANPD was created by Law No. 13,853/2019,[55] and is an entity that is a part of the federal public administration, pertaining to the Presidency of the Republic. According to Article 55-J of the LGPD, the ANPD has the following duties, among others:

a to prepare guidelines for the National Policy for the Protection of Personal Data and Privacy;

51 'Secrecy of justice' refers to a situation in which judicial procedures or policy investigations, usually available to the public, are kept under secrecy. This usually happens when there is a risk of exposure of private information related to the defendant or investigated; or when the procedure has confidential documents, such as bank statements or phone tapping, for example.

52 Law No. 3,689/1941. Available at www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

53 Law No. 9,296/1996. Available at www.planalto.gov.br/ccivil_03/LEIS/L9296.htm.

54 The 'main action' is the action in the procedure that brings the main purpose of the litigation. This main action is independent (i.e., it exists by itself).

55 Law No. 13,853/2019. Available at www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm.

b to supervise and apply sanctions in the case of processing of data carried out in violation of legislation, through an administrative process that ensures to the adversary broad defence and the right to appeal;

c to promote in the population the knowledge of the norms and public policies on the protection of personal data and security measures;

d to promote cooperation actions of an international or transnational nature with personal data protection authorities of other countries; and

e to edit simplified and differentiated rules, guidelines and procedures, including deadlines, so that micro and small companies, as well as incremental or disruptive business initiatives that self-declare as start-ups or innovation companies, can adapt to the LGPD.

Despite this, other government authorities are already acting on behalf of the data protection principles. To illustrate this, the major consumer defence body in Brazil (Procon) and public prosecution (Special Unit of Data Protection and Artificial Intelligence – Espec)[56] are notifying, investigating and even applying fines[57] to companies that act in an unlawful or abusive manner, based on other laws, such as the Brazilian Consumer Code. In addition, the ANPD has confirmed the following cooperation agreements:

a at the end of March 2021, with the National Consumer's Office (SENACON),[58] attempting to improve investigations and better address consumers' rights in data breaches; and

b at the beginning of June 2021, with CADE,[59] aiming to promote free competition culture in services that claim the protection of personal data.

In May 2021, WhatsApp committed to collaborate with CADE, the Public Prosecutor's Office (equivalent to the US Department of Justice), the ANPD and SENACON in relation to concerns raised by these public bodies about the messaging app's new privacy policy.[60]

ii Recent enforcement cases

Considering that the provisions of the LGPD on administrative sanctions entered into force in August 2021, no sanctions have been imposed by the ANPD to date.

However, other agencies have already imposed fines on the grounds of sectoral legislation. In this regard, in August 2019, Google and Apple were fined close to 18 million reais by Procon-SP, owing to abusive clauses in the terms of use and privacy policy of the FaceApp application, as well as only being available in the English language, in violation of

56 Brazilian Special Unit of Data Protection and Artificial Intelligence. Available at https://www.mpdft.mp.br/portal/index.php/conhecampdft-menu/nucleos-e-grupos/espec.

57 The *FaceApp* case. Available at https://www.procon.sp.gov.br/aplicativo-de-envelhecimento-2/ and https://www.uol.com.br/tilt/noticias/redacao/2019/08/30/procon-sp-multa-google-e-apple-por-forma-como-disponibilizaram-o-faceapp.htm.

58 For additional information, see: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-senacon-assinam-acordo-de-cooperacao-tecnica.

59 For additional information, see: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-cade-assinam-acordo-de-cooperacao-tecnica.

60 For additional information, see: https://www.gov.br/anpd/pt-br/assuntos/noticias/whatsapp-se-compromete-a-colaborar-com-cade-mpf-anpd-e-senacon-em-relacao-a-nova-politica-de-privacidade.

consumer rights.[61] In the same year, another significant case resulted in a fine being imposed by the Consumer Protection and Defence Authority on Facebook for improperly sharing data from 443,000 Brazilian users in the *Cambridge Analytica* case.[62]

Also, the Brazilian judiciary provided recent enforcement cases related to privacy and data protection. In May 2020, the Federal Supreme Court granted a writ of prevention suspending the effectiveness of Provisional Measure 954 on data sharing of telecommunication users with the Brazilian Institute of Geography and Statistics for the production of official statistics during the covid-19 pandemic. The trial contributed to the expansion of debates on the acknowledgment of the fundamental right to personal data protection in the Brazilian jurisdiction.[63]

In September 2020, a lower court of São Paulo found for the plaintiff and ruled that sharing consumers' personal data with companies outside the contractual relationship violates provisions of the LGPD, as well as constitutional principles, such as the right to privacy.[64] Real estate company Cyrela was awarded 10,000 reais for pain and suffering in the same decision, which prohibited the defendant from passing on the personal data to third parties. The decision considered not only the provisions of the LGPD, but also of the Brazilian Federal Constitution and the Consumer Protection Code.

In May 2021, the São Paulo Appeals Court[65] fined ViaQuatro, the company that manages the yellow subway line of São Paulo, 100,000 reais. The Court confirmed that the payment is for collective pain and suffering – to be destined to a collective investment entity – and ordered the deactivation of the facial recognition system for data subjects using the yellow subway line of São Paulo. The decision was based on the LGPD, recognising data as sensitive biometric personal data and acknowledging the need to obtain consent from the data subjects and provide details of the processing, in compliance with the principle of transparency. The case is currently on court appeal.

In addition, other protective bodies are acting on the grounds of the LGPD. After wide media coverage, Procon-SP notified a data bureau that it is seeking clarification on the alleged leak of 220 million Brazilian citizens' personal data.[66] The data bureau provided its response in April 2021 in which it claims not to have identified any irregularity. However, the investigation has not yet been closed.

Another case under investigation by Procon-SP relates to Brazil's main telecommunication companies' potential leak of more than 100 million telephone numbers.[67]

In April 2021, Procon-SP notified Facebook to confirm the news of a data leak that allegedly exposed information – such as full names, telephone numbers, dates of birth and email addresses – of more than 500 million users, including more than 8 million Brazilians, in

61 For additional information about the case, access: https://www.procon.sp.gov.br/aplicativo-de-envelhecimento-2/.

62 For additional information about the case, see *Consultor Jurídico*, available at https://www.conjur.com.br/2019-dez-30/governo-multa-facebook-compartilhamento-dados.

63 For additional information, see: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902.

64 Legal Procedure No. 1080233-94.2019.8.26.0100. Available at https://esaj.tjsp.jus.br/pastadigital/abrirDocumentoEdt.

65 Legal Procedure No. 1090663-42.2018.8.26.0100. Available at https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=2S000WSPS0000&processo.foro=100&processo.numero=1090663-42.2018.8.26.0100&uuidCaptcha=sajcaptcha_f41c326cd0ef4332b1f94f3763353773.

66 Report available at https://www.procon.sp.gov.br/serasa-complementa-resposta-sobre-vazamento-de-dados/.

67 Report available at https://www.procon.sp.gov.br/procon-sp-notifica-claro-oi-tim-vivo-e-psafe/.

online hacker forums.[68] The agency required responses on Facebook's measures to contain the leak, strategies to deal with the damage and prevent further failures, as well as the lawfulness of processing the personal data of Brazilian citizens and the measures adopted to comply with the LGPD.

In June 2021, the Brazilian Consumer Protection Institution (IDEC) notified Raia Drogasil, a drugstore group, to present information regarding the collection and use of customers' biometrics data.[69] IDEC is currently investigating this group's activities, following complaints. Consumers reported that they were barred from taking advantage of promotions unless they registered their fingerprints. The extrajudicial notification also required that the group ceased the collection of fingerprints and Individual Taxpayers Registry Numbers and explained the purpose of the data collection.

Recently, the ANPD opened an investigation into a security incident involving the Ministry of Health's ConecteSUS application. The application is used by Brazilian citizens for, among other purposes, keeping records of their vaccinations. In the covid-19 pandemic scenario, the application ended up being offline for a few days, which caused great damage to the population. The case has not yet been closed.

iii Private litigation

Before any judicial remedies, interested parties and authorities may seek for administrative remedies for breaches of privacy and data rules. The LGPD provides for the data subject's right to petition, regarding their data, before the ANPD.

Furthermore, the Brazilian Federal Constitution[70] provides that the right to judicial assistance is a fundamental guarantee for individuals, as it is universal, inalienable, unavailable and unwavering.

For civil procedures, the Brazilian liability is subjective and the data subject shall prove the commitment of an unlawful conduct (by an act or an omission), the damage and the causal link. For consumer affairs-related cases, the law foresees that the agent is submitted to strict liability, provided that the liability exceptions are more restrict in these cases.

The LGPD provides that the controller or processor that, as a result of carrying out the activity of processing personal data, cause material, moral, individual or collective damage to third parties, in violation of legislation for the protection of personal data, is obligated to redress it.[71]

The LGPD also provides that the judge, in a civil lawsuit, may reverse the burden of proof in favour of the data subject when, at its discretion, the allegation appears to be true or when production of evidence by the data subject would be overly burdensome. Lawsuits for compensation for collective damages may be filed collectively in court, subject to the pertinent legislation.[72]

68 For additional information, see: https://www.procon.sp.gov.br/procon-sp-notifica-facebook-3/.

69 For additional information, see: https://idec.org.br/idec-na-imprensa/idec-notifica-raia-drogasil-dono-da-droga-raia-sobre-biometria-digital.

70 Article 5, XXXV of Brazilian Federal Constitution.

71 Article 42, preamble, of LGPD.

72 Article 42, Sections 2 and 3, of LGPD.

Regarding class actions, collective interests are mostly regulated by the Brazilian Law of Public Civil Action (Law No. 7,347/1985),[73] which foresees the protection of diffuse and collective interests related to the environment, the consumer, goods and rights of artistic, aesthetic, historical, tourist and landscape value, among other goods and rights listed in its article.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As per its Article 3, the LGPD shall apply to any data processing operation performed by any person or entity, public or private, provided that the processing operation is carried out in the Brazilian territory; the processing operation entails the offer or provision of goods or services or data processing for individuals located in Brazil; or data collection that was carried out within Brazilian territory. The applicability hypotheses are independent of each other and the presence of only one of them is enough for the LGPD to have an effect on the agent responsible for the processing.

Thus, in general, all foreign companies that process, in any way, personal data from Brazilian individuals should comply with the LGPD. Also in this regard, the Brazilian Internet Law had a very similar provision (Article 11), which resulted in the same conclusion.

These provisions were clearly provided by such laws because in the past there were many judicial discussions involving the data processing of Brazilian individuals occurring abroad. Some foreign companies tried to avoid the enforcement of Brazilian laws and judicial orders, arguing that the data processing was performed outside Brazil. To avoid this kind of problem, these recent legal provisions reiterate that any action involving personal data from Brazilian subjects or from individuals located in Brazil shall trigger the application of Brazilian laws.

IX CYBERSECURITY AND DATA BREACHES

The Brazilian Internet Law provides that the discipline of internet use in Brazil should preserve the stability, security and functionality of the network, via technical measures consistent with international standards and by encouraging the use of best practices. Decree No. 8,771/2016, which regulates the Internet Law, also establishes some guidelines on security standards that connection and application providers must observe when processing personal data and private communications, such as strict control over access to data, authentication mechanisms for access to records, inventories of access to records and use of record management solutions such as encryption or equivalent measures.

Furthermore, the LGPD[74] provides that processing agents shall adopt technical and administrative security measures and are able to protect personal data from unauthorised access and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing.

73 Brazilian Law of Public Civil Action (Law No. 7,347/1985). Available at www.planalto.gov.br/ccivil_03/leis/l7347orig.htm.

74 Article 6, VII of LGPD.

As well as the general provisions of the Brazilian Internet Law and the LGPD, there are several sectoral laws and regulations concerning cybersecurity requirements for specific regulated sectors, including:

a Resolution No. 4,893/2021 of BACEN,[75] which provides for the cybersecurity policy and the requirements for contracting data processing and storage and cloud computing services to be observed by institutions authorised to operate by BACEN. This Resolution entered into force on 1 July 2021;

b Resolution No. 85/2021 of BACEN,[76] which provides for the cybersecurity policy and the requirements for contracting data processing and storage and cloud computing services to be observed by payment institutions authorised to operate by the Central Bank of Brazil. This Resolution entered into force on 1 August 2021;

c Ordinance No. 271/2017,[77] which provides the Information Security and Communications Policy of the Ministry of Health; and

d Ordinance No. 1,966/18,[78] which defines information and communication security standards within the Ministry of Health.

Also, in the public sector:

a Decree No. 9,637/2018 approves the National Information Security Policy[79] within the federal public administration, to ensure the availability, integrity, confidentiality and authenticity of information at the national level; and

b Decree No. 10,222/2020 approves the National Strategy of Cybersecurity (E-Ciber),[80] a government plan on the main actions, nationally and internationally, that it intends to apply in the cybersecurity area.

Regarding data retention, there are no specific periods provided; however, the LGPD[81] establishes that the ANPD may provide standards about the retention period of records, especially considering the need for the data and transparency to the data subjects. Also, there are many diverse specifications related to the retention period of records in sectoral laws, such as the legal obligation of storage of connection records by connection providers for one year and the storage of access records by application providers for six months, according to the Brazilian Internet Law,[82] for example.

75 Resolution No. 4,893/2021. Available at https://www.in.gov.br/en/web/dou/-/resolucao-cmn-n-4.893-de-26-de-fevereiro-de-2021-305689973.

76 Resolution No. 85/2021. Available at https://www.in.gov.br/en/web/dou/-/resolucao-bcb-n-85-de-8-de-abril-de-2021-313194098.

77 Ordinance No. 271/2017. Available at http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/20598014/do1-2017-01-30-portaria-n-271-de-27-de-janeiro-de-2017-20597844.

78 Ordinance No. 1,966/18. Available at http://bvsms.saude.gov.br/bvs/saudelegis/gm/2018/prt1966_18_07_2018.html.

79 Decree No. 9,637/2018. Available at www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm.

80 Decree No. 10,222/2020. Available at www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm.

81 Article 40 of LGPD.

82 Article 15 of Brazilian Internet Law.

As regards data breach reporting requirements, the LGPD[83] establishes that the controller should communicate to ANPD and the data subject the occurrence of any security incident that may cause risk or relevant harm to data subjects. This activity may be executed by the DPO, as the DPO is the person indicated by the controller to act as a communication channel between the controller, the data subjects and the ANPD.

In February 2021, the Authority added brief explanations and notification requirements of data breaches to its website.[84]

The ANPD defines a data breach as any confirmed adverse event related to a breach in the security of personal data. The website also provides a template form for reporting incidents to the Authority. The ANPD also indicates the steps it takes upon notification of a data breach: (1) internal assessment of the incident (nature, category, number of holders affected, probable consequences); (2) communication to the DPO; (3) communication to the controller, if the affected entity is the data processor; (4) communication to the ANPD and the data subjects, if applicable; and (5) preparation of internal documentation following the principle of accountability.

The ANPD also indicates that if the incident is reported by the data processor, the Authority will analyse it on a subsidiary basis. The Authority indicates that more objective criteria for notifying the data subject may be issued in the future, but that for the moment the controller should adopt a cautious stance, communicating the incident to the data subjects if there is any risk of relevant damage to them, such as when the incident involves sensitive personal data, children's personal data or image violation, among others.

Finally, the Authority recommends that the incident be reported within two working days of the data controller becoming aware of it, pending the Authority issuing binding regulations to that effect.

X OUTLOOK

The entry into force of the EU's General Data Protection Regulation[85] in 2018 contributed to the endorsement of the LGPD in the same year in Brazil, as the same way as it has already had a significant impact on Brazilian companies that process the personal data of persons located in the European Union, or that transfer data internationally. In this regard, the free flow of data between EU countries and Brazil is conditioned by the level of adequacy of data protection, which must be similar to that in the EU. Furthermore, Brazilian companies have been conducting adaptation projects to comply with the data protection legislation through the adoption of best practices for processing personal data grounded on LGPD authoritative hypotheses and personal data protection principles.

The LGPD came into force in September 2020, with the exception of the administrative sanctions, which entered into force in August 2021. However, the efficacy of some of the provisions provided by the LGPD requires regulation by the ANPD, which is expected to take place, according to the ANPD regulatory agenda for the 2021–2022 biennium, established by Ordinance No. 11/2021.[86]

83 Article 48 of LGPD.

84 Data Breach Reporting. Available at https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

85 Available at https://gdpr-info.eu/.

86 Available at https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313.

The ANPD is expected to issue a resolution on the international transfer of personal data during the next few months of 2022, which will have a major positive practical impact on organisations, particularly with regard to the possibility of developing and using their global corporate rules. The issuance of standard contractual clauses will also greatly facilitate cross-border data processing. Another subject that has generated a lot of expectation is the publication of a resolution about data protection impact assessments, as the LGPD has left some gaps about this important assessment. Finally, another big issue is that related to the rights of data subjects, which will also be subject to a resolution by the Regulator. All of these issues may be the subject of the ANPD later this year.

Appendix 1

ABOUT THE AUTHORS

RICARDO BARRETTO FERREIRA

Azevedo Sette Advogados

Ricardo Barretto Ferreira da Silva was co-founder and managing partner of two renowned law firms (CFF and BKBG) (1975–2004 and 2004–2016) before becoming a senior partner and head of TMT legal practice at Azevedo Sette Advogados.

He graduated from São Paulo University Law School in 1973 and carried out graduate research work in taxation and corporate laws at the University of North Dakota, United States (1974).

Ricardo is an attorney with experience in corporate, tax, M&A, intellectual property, technology, media, telecommunications, privacy and data protection. Among other things, he has been co-founder, vice president (1989–1994) and president (1995–1998) of the Brazilian Information Technology and Telecommunications Association; chair of the Membership Latin America Committee (1993–1995); and board member (1995–2001 and 2003–2005), secretary, treasurer and vice president (2001–2003) of the International Technology Law Association.

Ricardo has had various articles published in Brazil and abroad on IP, IT, media, telecoms, privacy, data protection, outsourcing and copyright.

LORENA PRETTI SERRAGLIO

Azevedo Sette Advogados

Lorena Pretti Serraglio is coordinator of the privacy and data protection area. She also works in the areas of technology, media and telecommunications. She is a consultant for the Special Data Protection Commission of the Federal Council of the Brazilian Bar Association. Lorena has an MBA in Electronic Law from Escola Paulista de Direito. She graduated from the Internet Governance School of the Internet Steering Committee in Brazil and in personal data protection and privacy at Data Privacy Brasil. Lorena is the 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 also a speaker on digital law, cybersecurity and data protection. Lorena coordinates projects to help clients comply with the Brazilian Data Protection Act (LGPD) and elaborates opinions, contracts and memoranda in the areas of digital law, privacy and data protection. She is recognised by Análise Advocacia in the specialties of digital law and compliance and she is a reference for

technology companies, in addition to being a regional highlight in the State of São Paulo. She is also recognised by *The Legal 500* international ranking in the areas of cybersecurity and data protection.

ISABELLA DA PENHA LOPES SANTANA

Azevedo Sette Advogados

Isabella da Penha Lopes Santana is a technology, media and telecommunications lawyer, with focus on digital law and data protection. She is a specialist in digital law and compliance by IBMEC, an MBA candidate in Cybersecurity at IGTI, certified as data protection officer by Fundação Getúlio Vargas of Rio de Janeiro, certified in ethics and law in data analytics by Microsoft and in Computer Science for Lawyers (CS50) by Harvard University. She is a researcher of the Oscar Sala Chair in the study group Human-Algorithm Interactions at the University of São Paulo. She participates in LGPD compliance projects and in the preparation of opinions, contracts and memoranda in the areas of digital law, privacy and data protection. She is an author and co-author of several articles and books in the area of technology, privacy and data protection and artificial intelligence, one of which was elected by the Superior Court of Justice as the indicated bibliography on artificial intelligence.

CAROLINA SIMIONI PERDOMO

Azevedo Sette Advogados

Carolina Simioni Perdomo is a technology, media and telecommunications lawyer, with focus on digital law and data protection. Carolina graduated from Toledo Prudente – University Centre. She participates in LGPD compliance projects and in the preparation of opinions, contracts and memoranda in the areas of digital law, privacy and data protection. She has co-authored several articles in the area of cybersecurity, privacy and data protection. She graduated in the Data Protection and Privacy – Theory and Practice course from the Data Privacy Institute and is a member of the 2022 Youth Brazil Programme, focused on training the next generation of internet leaders, provided by the Internet Steering Committee in Brazil in cooperation with the Internet Society and other institutions.

BRUNA EVELLYN PEREIRA BIGAS

Azevedo Sette Advogados

Bruna Evellyn Pereira Bigas is a privacy and data protection lawyer. She also works in the areas of technology, media and telecommunications. Bruna has an MBA in electronic law from Escola Paulista de Direito. She has a degree in personal data protection and privacy from Data Privacy Brasil. Bruna works on projects to help clients comply with the Brazilian General Data Protection Law (LGPD) and prepare opinions, contracts and memoranda in the areas of digital law, privacy and data protection.

AZEVEDO SETTE ADVOGADOS

11th Floor
1327 Av Pres Juscelino Kubitscheck
São Paulo 04543-011
Brazil
Tel: +55 11 4083 7600
Fax: +55 11 4083 7601
barretto@azevedosette.com.br
lserraglio@azevedosette.com.br
ilsantana@azevedosette.com.br
cperdomo@azevedosette.com.br
bbigas@azevedosette.com.br
www.azevedosette.com.br

ISBN 978-1-80449-116-4