Non-final version of Britto Gaspar; Walter. The personal data architecture of Brazil; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

THE PERSONAL DATA ARCHITECTURE OF BRAZIL

Walter Britto Gaspar

Abstract

This article explores the legal framework governing data flows in Brazil, with a primary focus on personal data collection and processing. It examines the intricate network of laws, regulations, institutions and guidance documents shaping the landscape of data protection within the country. Historically, Brazil's approach to data protection was fragmented, with various sector-specific regulations coexisting alongside different institutional frameworks. The recent enactment of the General Data Protection Law marked a significant shift, unifying data protection rights under a single comprehensive statute. However, this transition has introduced complexities as the LGPD interacts with pre-existing legal and bureaucratic structures. Furthermore, the article addresses the broader context of data governance in Brazil, encompassing ongoing discussions surrounding privacy, data protection, technological innovation, and surveillance. Notably, the draft artificial intelligence bill is examined as a pertinent example of legislation that intersects with data collection and flow concerns, reflecting the evolving nature of data-related regulations. The conclusion underscores the challenges and opportunities facing the National Data Protection Authority, the key regulatory body overseeing data protection in Brazil. It emphasizes the necessity of cooperation and coordination with existing institutional mechanisms to ensure a coherent and effective data protection framework. The article highlights potential areas of contention, including disputes over jurisdiction, and emphasizes the importance of the Authority's prompt responses to maintain clarity and prevent fragmentation within the data protection ecosystem.

Non-final version of Britto Gaspar; Walter. The personal data architecture of Brazil; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

CONTENTS

Non-final version of Britto Gaspar; Walter. The personal data architecture of Brazil; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

1. THE PERSONAL DATA ARCHITECTURE OF BRAZIL

1.1. Introduction: Legal architecture of data flows in Brazil

This chapter is concerned with the legal architecture of personal data flows in Brazil. In particular, it will deal with the legal instruments involved in the collection and processing of personal data in the country, as well as the institutions involved in that processing. This entails looking at the laws that may influence personal data processing operations as well as other types of norms and guidance documents. Each of these will be presented, their main points highlighted to explain how they fit in the personal data protection architecture.

Reference should also be made to legal instruments that deal with information security in its various instances, be it when data is stored or in transit, by public or private actors. This is an aspect of data architectures that runs in parallel to personal data protection, but in many ways overlaps with it – since information security deals with aspects of data processing that are instrumental to the realization of the right to data protection.

Brazil currently does not have an overarching data security law such as China's or South Africa's, although there have been many normative, policy and planning documents on the subject so far and the country has signed and internalised the Budapest Convention on cybercrime[1]. The most recent effort in this direction was the enactment of a new National Cybersecurity Policy, rooted in concepts of national sovereignty and protection of fundamental rights; and the resulting discussions around the creation of a National Cybersecurity Authority to unify regulation, inter-agency coordination and oversight of the subject nationally[2]. This cybersecurity blueprint makes up a backdrop for the personal data architectures described and discussed herein.

Brazil has had a long, but sparse trajectory on these subjects up until recently. Unification of personal data protection rights under one overarching law is a recent development in the Brazilian legal landscape. This means new legislation enters a field populated not only by other specific laws, but also by other institutions in general, including bureaucratic bodies and processes, specialized judicial actors, and law enforcement practices. All this unfurls in the face of ongoing public discourse that in many ways reflects global dichotomies between protection of rights and structures of vigilance [3].

---

[1] 'Convenção de Budapeste é promulgada no Brasil', Ministério da Justiça e Segurança Pública, 17 April 2023, https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil; Luca Belli et al., *Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano*, 1st ed. (Rio de Janeiro: FGV Direito Rio, 2023), https://cyberbrics.info/ciberseguranca-uma-visao-sistemica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/.

[2] 'CNCiber (Comitê Nacional de Cibersegurança)', Gabinete de Segurança Institucional, accessed 27 March 2025, https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber/CNCiber; Rafael Bucco, 'Governo publica nova Política Nacional de Cibersegurança', TeleSíntese, 27 December 2023, https://telesintese.com.br/governo-publica-nova-politica-nacional-de-ciberseguranca-com-anatel-no-comite/; Redação, 'Criado o Comitê de Cibersegurança', TeleSíntese, 14 February 2024, https://telesintese.com.br/criado-o-comite-de-ciberseguranca-cnciber/; 'O que é a Política Nacional de Cibersegurança, marco no combate aos crimes virtuais', Secretaria de Comunicação Social, 29 December 2023, https://www.gov.br/secom/pt-br/fatos/brasil-contra-fake/noticias/2023/12/o-que-e-a-politica-nacional-de-ciberseguranca-marco-no-combate-aos-crimes-virtuais.

[3] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London: Profile Books, 2019).

Non-final version of Britto Gaspar; Walter. The personal data architecture of Brazil; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Beyond all that, new norms are being discussed or implemented on topics that intertwine with data architectures. One relevant recent example is the draft artificial intelligence bill[4], currently awaiting discussion at the country's Chamber of Deputies after approval in the Federal Senate. Although focused on AI applications, due to the very nature of these technologies, it will touch upon matters of personal data collection and flow.

It should be noted, as well, that Brazil is a presidential democracy with regular elections and a normative framework surrounding the Federal Constitution of 1988, with a comprehensive approach to fundamental rights rooted in human dignity. The Constitution upholds human rights among its principles in international relations and ensures internal validity of international human rights treaties approved under special proceedings at the same level as constitutional amendments. Brazil has been classified as "Free" under Freedom House's Freedom in the World report[5] for the last five years, with a highlight of the polarized electoral process and political scenario of the most recent presidential elections, in 2022. It has been classified as "Partly free" in the Freedom on the net report[6] by the same entity in the last five years, noting provisions contained in the country's "fake news" bill, actions taken against disinformation during elections and issues related to the economic exclusion of minorities, among others. All in all, Brazilian institutions, including regular elections, have been through tempestuous times lately, but the country has managed to maintain its Constitutional democratic system.

In terms of the protection awarded to personal data under this framework, there have been significant developments in recent years. Even before the General Data Protection Law fully entered into force, in 2020, in a case discussing the legality of sharing telecommunication services' customer data with the National Statics Institute (IBGE), an important judicial interpretation was set. The case evidenced the existence of an autonomous fundamental right to personal data protection under the Brazilian Constitution – echoing, in BRICS, the significance of the Puttaswamy v. Union of India case in India, which recognized the existence of an autonomous fundamental right to privacy in the country's Constitution – as a consequence of the protection of human dignity (art. 1, III; art. 5, X), the right to *habeas data* (art. 5, LXIX), the protection of due process (art. 5, LIV) and the protection of private life (art. 5, X)[7]. This was later reinforced by the inclusion of section LXXIX to article 5 of the Constitution via amendment n. 115 of 2022, adding the protection of personal data as a fundamental right.

All these factors shall be dealt with in the following discussion, focused on the legal architecture of personal data protection in Brazil – its accomplishments so far and challenges to come.

1.2. The pre-LGPD Normative framework

The Brazilian normative landscape regarding data protection has seen significant advance lately with the enactment of the country's General Data Protection Law (LGPD, in the Portuguese abbreviation)[8] and creation of its National Data Protection Authority (ANPD). However, there existed a previous legal

[4] Walter Britto Gaspar, Eduardo Mattos, and Luca Belli, 'Non-Official Translation of the Brazilian Artificial Intelligence Bill, n. 21/2020', CyberBRICS, 25 October 2021, https://cyberbrics.info/non-official-translation-of-the-brazilian-artificial-intelligence-bill-n-21-2020/.

[5] Freedom House, 'Brazil: Freedom in the World 2023 Country Report', Freedom House, 2023, https://freedomhouse.org/country/brazil/freedom-world/2023.

[6] Freedom House, 'Brazil: Freedom on the Net 2023 Country Report', Freedom House, 2023, https://freedomhouse.org/country/brazil/freedom-net/2023.

[7] Bruno Ricardo Bioni and Renato Leite Monteiro, 'A Landmark Ruling in Brazil: Paving the Way for Considering Data Protection as an Autonomous Fundamental Right', Future of Privacy Forum, 9 June 2020, https://fpf.org/blog/a-landmark-ruling-in-brazil-paving-the-way-for-considering-data-protection-as-an-autonomous-fundamental-right/.

[8] Luca Belli et al., 'The Brazilian General Data Protection Law (LGPD). Unofficial English Version', Cyberbrics, January 2020, https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/.

structure regarding privacy rights and information rights, which paved the way to the current architecture.

1.2.1. The Federal Constitution and the Civil Code

Firstly, it is relevant to stress that the civil and constitutional legal orders in Brazil give space and importance to personality rights, among which is the right to privacy. In fact, the Brazilian Civil Code (law n. 10.406/02) has a chapter (c. II, arts. 11 – 21) dedicated to "personality rights", and within it one finds, alongside image rights, bodily autonomy and other personality rights, specific protection to private life on article 21[9]:

> Art. 21. Private life of the natural person is inviolable, and the judge, upon request by the interested party, shall adopt the necessary procedures to avoid or stop any act contrary to this norm.

In the 1988 Federal Constitution[10], this is reflected in a series of fundamental rights: inviolability of intimacy, private life, honour and image (art. 5, X); inviolability of the homestead (art. 5, XI); and secrecy of communications, correspondence, data communication and telephone communications (art. 5, XII). The latter gave rise to debate among Brazilian legal doctrine on the extent of the right to privacy of data: whether it was to be restricted to data in transit or also apply to stored data. In other words, if protection was given to communications or to data itself[11].

This controversy hints at the limited reach of dealing with issues of data protection solely on privacy grounds: the challenges of the information age, summarized by Zuboff[12] as surveillance capitalism, require an approach that tackles data processing in a more adequate manner. This would become increasingly clear in Brazilian legal practice and public discourse, with issues involving not only secrecy of intimate data, but of control over personal data flows arising.

One more instance where the subject of personal information is detailed in the Constitution is the fundamental right to *habeas data*, that is, the right to access information concerning oneself and to correct erroneous information (art. 5, LXXII). Habeas data is further regulated in a specific law (n. 9.507/97)[13]. *Habeas data* responded to a mounting demand for control of the use of personal data, especially in face and in tune with the country's re-democratization process. It was also influenced by earlier foreign specific data protection concerns – especially, in the United States, the National Data Centre debate in the 1960s-1970s[14]. The constitutional remedy has a very limited scope, though, directed at knowledge and correction of personal data held in public or public interest databases, and thus was equally inept at responding to the full scheme of data protection issues presented by a connected society.

---

[9] Brasil, 'Código Civil (l. n. 10.406/02)', 10 January 2002, http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm.

[10] Brasil, 'Constituição Federal', 1988, http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

[11] Danilo Doneda, *Da Privacidade à Proteção de Dados Pessoais: Fundamentos Da Lei Geral de Proteção de Dados*, 2ª (São Paulo: Thomson Reuters Brasil, 2019), 262; Danilo Doneda, 'Panorama Histórico Da Proteção de Dados Pessoais', in *Tratado de Proteção de Dados Pessoais*, ed. Danilo Doneda et al. (Rio de Janeiro: Forense, 2021), 11–12.

[12] *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

[13] Brasil, 'L. n. 9507/97', 1997, http://www.planalto.gov.br/ccivil_03/leis/l9507.htm.

[14] Doneda, 'Panorama Histórico Da Proteção de Dados Pessoais'.

1.2.2. A New Fundamental right to Data Protection

These would have been the sole mentions of privacy or, by interpretative extension, data protection in the Brazilian Constitution up until recently. However, in October 2021 the Brazilian Senate unanimously approved a constitutional amendment project [15], promulgated into Constitutional Amendment n. 115 on February 2022 [16], that adds an autonomous right to data protection into the roster of fundamental rights in art. 5th of the Constitution, thusly:

> Art. 5º All are equal before the law, without distinction of any nature, being assured to Brazilians and foreigners residing in the Country inviolability of their right to life, liberty, equality, security and property, in the following terms:
>
> LXXIX – it is assured, as dictated by law, the right to personal data protection, including in digital media.

This makes Brazil the BRICS country with the best-defined independent constitutional right to data protection, whereas others, such as India and South Africa, derive it from the right to privacy. The amendment also determines that the Federal government is responsible for organizing and enforcing personal data processing and protection, as well its sole competence for proposing legislation on the matter.

This development comes shortly after the enactment of an overarching data protection law in the country and the creation of its National Data Protection Authority, as will be discussed in following, and indicates the result of strengthening awareness of the need for specific personal data protection regulation. There are, however, still other laws that pre-date the General Data Protection Law which merit mention beforehand.

1.2.3. The Brazilian Consumer Code

One noteworthy legal reference is the Brazilian Consumer Code [17]. Article 43 of the code establishes the rights of the consumer regarding databases containing their information. Similar to the Habeas Data legal remedy, access and rectification rights are granted to the data subject. However, the consumer code also establishes duties to the controller of such data (the provider of goods and/or services):

1. A duty to inform that the data is being registered;
2. A duty to inform the origin of the data, *i.e.*, when, how and why it was collected;
3. A duty to provide access in a manner that is "objective, clear, truthful" and using "easily understandable language"; and
4. A limit of five years to store negative records concerning consumers.

All these foreshadow rights, duties and principles that would later be important in the rise of the LGPD and currently make up the personal data protection framework of Brazil and other countries. This sort

---

[15] Agência Senado, 'Senado Federal Aprova Proposta de Emenda à Constituição 17 (PEC 17/2019) Que Inclui a Proteção de Dados Pessoais No Rol de Direitos e Garantias Fundamentais', Gov.br, 26 October 2021, https://www.gov.br/anpd/pt-br/assuntos/noticias/senado-federal-aprova-proposta-de-emenda-a-constituicao-17-pec-17-2019-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-e-garantias-fundamentais.

[16] José Carlos Oliveira, 'Promulgada PEC Que Inclui a Proteção de Dados Pessoais Entre Direitos Fundamentais Do Cidadão', Portal da Câmara dos Deputados, 10 February 2022, https://www.camara.leg.br/noticias/850028-promulgada-pec-que-inclui-a-protecao-de-dados-pessoais-entre-direitos-fundamentais-do-cidadao/.

[17] Brasil, 'L. n. 8078/90', 11 September 1990, http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

of consumer data protection is another unique characteristic of Brazil in comparison to other BRICS countries.

1.2.4. The Access to Information Law

Another important reference is the Access to Information Law [18]. Although it is focused on access to information regarding the public administration, this law contains norms on access to personal information contained within these public records. As such, it contains the first legal definition of "personal data" (in this case, named "personal information") in the Brazilian legal order: personal information is "that [information] related to an identified or identifiable natural person" (art. 4, IV). This definition is in line with that which would later be given in LGPD[19] and is similar to that of other BRICS countries, including China and India[20].

Besides that, the law also builds a personal information micro-system based on the secrecy by default of such data, which can only be exempted by the subject's explicit consent or in few hypotheses:

1. When there is a specific law which would allow access to such information;
2. For medical treatment of the subject, given that they are incapable of giving consent;
3. For statistical and scientific research of "evident general or public interest", with a legal basis, and barred the identification of the subject;
4. When it be necessary to comply with judicial orders;
5. When necessary to defend human rights; and
6. To protect an overwhelming general and public interest.

Of interest, still, is the determination that those who access such information shall be responsible for its misuse; and that this access restriction shall not be used to defend against scrutiny related to irregularities or to bar historical research of greater relevance.

It is interesting to note how the system put forth in the Access to Information Law brings to the fore some matters that would later be tension points in the application of LGPD. The question of how liability should be applied to the various actors in the chain of data processing is still open [21]. This is especially true regarding artificial intelligence applications which use personal data – where there are attempts to establish a subjective liability scheme and strong opinions to the contrary due to the technical and political disparity between data subjects and controllers [22]. Additionally, it provides a first attempt at balancing the rights of access to public interest information and of privacy and data

[18] Brasil, 'L. n. 12527/11', 18 November 2011, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

[19] Gabriel da Silva Barros, Lorena dos Santos Silva, and Clarissa Schmidt, 'Public Records and Personal Data: The Access from the Perspective of the Brazilian General Personal Data Protection Law and the Brazilian Access to Information Law', *Revista Do Arquivo*, no. 09 (October 2019): 22–39.

[20] Art. 4 of China's PIPL defines it as "various kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously"; Section 2, (t), of the Indian Digital Personal Data Protection Act defines it as "any data about an individual who is identifiable by or in relation to such data".

[21] Maria Celina Bodin De Moraes, 'LGPD: Um Novo Regime de Responsabilização Civil Dito "Proativo"', *Civilistica.Com* 8, no. 3 (2019): 1–6; Bruno Bioni and Daniel Dias, 'Responsabilidade Civil Na Proteção de Dados Pessoais: Construindo Pontes Entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa Do Consumidor', *Civilistica.Com* 9, no. 3 (22 December 2020): 1–23.

[22] André Lucas Fernandes, 'Os Erros Do PL 21/2020, Que Regula a Inteligência Artificial', JOTA, 1 November 2021, https://www.jota.info/opiniao-e-analise/artigos/pl-21-2020-inteligencia-artificial-01112021; Consultor Jurídico, 'Especialistas Questionam Artigo Do PL Do Marco Legal Da IA', ConJur, 27 October 2021, https://www.conjur.com.br/2021-out-27/especialistas-questionam-artigo-pl-marco-legal-ia.

protection, listing the cases where the prerogative of the data subject of controlling access to their data are excepted.

The credit scoring law [23] regulates the creation of credit score databases. This law shows a greater proximity to modern-day concepts of data protection [24], with mention to sensitive information[25] and adequacy, necessity and purpose limitation (although not under these denominations, the concepts are implicit in linking processing activities to the intended purpose and prohibiting excessive information) included among its articles.

Additionally, the law establishes information duties (art. 3) comparable to those enacted by the consumer code, the right to access and rectification, to solicit cancelling of the record, to be informed of credit analysis criteria and to request revision of solely automated decisions (art. 5). Finally, it establishes strict liability for damages caused by database administrators, data sources and consultants of the database (art. 16).

1.2.5. The Marco Civil da Internet

Finally, the *Marco Civil da Internet* (MCI), or Internet Civil Framework[26], a law created to regulate various aspects of Internet use – from net neutrality to liability of content intermediaries – was built with a basis on data protection, containing specific provisions on the matter. It establishes privacy and data protection as separate principles of Internet use in Brazil (art. 3) and establishes the inviolability of intimacy and private life and of the secrecy of communications (in flow and stored) as rights of the internet user, summarizing in one article (art. 7) many aspects of the discipline of privacy described so far in other laws.

Article 7 also determines that processing and sharing of personal data by controllers is dependent on the subject's "free, explicit and informed" consent. It further mentions purpose limitation and a duty of exclusion of data when the purpose for its collection (the contract between the internet application provider and the internet user) ends. Finally, it sets record-keeping periods of connection records and records of access to internet applications to one year and six months, respectively.

The MCI marks a crucial step in internet regulation in Brazil, prioritizing fundamental rights at a time when the foundations of the current data-based platforms and markets were being set. Its role as a "Constitution" of the internet is reflected in this substantive aspect as well as in its process of discussion, based on rounds of online participatory consultations at a time when this had seldom been attempted. It is a unique feature of the Brazilian personal data architecture among BRICS countries, indicating the country's early involvement with digital rights discussions.

A significant step toward modern-day data protection schemes, the Framework's focus on consent as the legal basis for data processing would prove a limited approach, due to the complexity of implementing meaningful consent in fast-paced internet relations[27]. This point would later be

[23] Brasil, 'L. n. 12414/11', 9 June 2011, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.
[24] Doneda, 'Panorama Histórico Da Proteção de Dados Pessoais'.
[25] Defined as those relating to "social or ethnic origins, health, genetic information, sexual orientation and political, religious and philosophical convictions", art. 3, §3.II.
[26] Brasil, 'L. n. 12965/14', 23 April 2014, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
[27] Luíza Couto Chaves Brandão, 'O Marco Civil Da Internet e a Proteção de Dados: Diálogos Com a LGPD', *Cadernos Adenauer* XX, no. 3 (2019): 35–48.

addressed by LGPD through an expansion of legal bases and of information, transparency, and accountability duties, among others.

1.2.6. A multifaceted data protection framework

The access to information law, the consumer code, and the credit scoring law, alongside the *habeas data* constitutional remedy and law and the Internet Civil Framework, are commonly referenced as a basis for the Brazilian data protection framework prior to the LGPD. However, there are many normative instances where personal information is involved. One impactful example is given by Louzada [28], discussing the genetic profile databases in Brazil.

These profiles are used in law enforcement and investigations; thus, the General Data Protection Law – which excludes such activities from its gamut – would not regulate them. However, due to the LGPD's extension of part of its data protection framework even to those areas excluded from its scope (art. 4, §1), the genetic profile databases niche would need to abide by the LGPD's overarching principles and ensure some of the rights contained therein.

This would likely involve changes to the current normative landscape (composed of a specific law, n. 12.564/2012, and a decree published by a Steering Committee). There are currently considerable gaps in regulation, which would need to be addressed. First, there is no provision as to the immediate discarding of the biological sample after the profile is registered. There is also a lack of purpose limitation rules and procedures and a need for better communication of the purposes and procedures involved in the collection of these materials. There is a need for better documentation of the whole production chain of these genetic profiles and there is a need of more specified and secure procedures regarding the security and quality of samples extracted; among others [29]. This case is but an example of potential harmonization efforts needed in the future because of the new regime implemented by the LGPD.

One other area where personal data are regulated and heavily transacted is banking. Besides the 2001 baking information secrecy law (n. 105/01), Brazil recently began implementing an open banking scheme aimed at operationalizing interoperability and portability between financial institutions. This was put in motion via a joint regulation by the National Monetary Council and the Brazilian Central Bank [30] and is implemented via APIs that allow sharing data such as identification and account information between registered institutions. The system is based on the user's "free, informed, previous and unambiguous" consent (art. 2, VIII) and excludes sensitive data from the data-sharing scheme.

Other notable instances are:

- The digital medical charts regulation, through which patient's medical records are allowed to be digitized, granted the appropriate security measures are in place. The regulation is published by the National Medicine Council [31] and the information security and secrecy standards are published by CFM in partnership with the Brazilian Society of Health Informatics

[28] 'Princípios Da LGPD e Os Bancos de Perfis Genéticos: Instrumentalizando a Garantia de Direitos No Processo Penal', *Revista Do Advogado*, no. 144 (2019): 90–98.
[29] Louzada.
[30] BCB and CMN, 'Res. Conj. n. 01/20', 1 May 2020, https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res_Conj_0001_v1_O.pdf.
[31] CFM, 'Res. CFM n. 1821', 23 November 2007, https://www.normasbrasil.com.br/norma/resolucao-1821-2007_105431.html.

[32]. These include using digital identity certification under the National Digital Identity Certification Structure; audits and security certifications and seals; and a series of security requirements according to the type of system being implemented.

- Notary offices and public registry laws and regulations. These entities operate under oversight and are regulated by the judicial branch, via the National Justice Council (CNJ). Laws and regulations in the area cover the digitization of documents and registries, data security standards and liability schemes, among others [33].
- Electoral processes. These are regulated by the Superior Electoral Tribunal (TSE), which, even before the LGPD, had already enacted some provisions on the processing of personal data. Specifically, donation or purchase of databases containing contact information of potential voters was restricted and the means of massive electoral propaganda as well, including reference to consent in the inclusion in mailing lists and opt-out options [34].

In conclusion, the many normative developments in the last decades[35] point to a progressive path from a framework focused on intimacy and private life to one focused specifically on data protection aspects adapted to information society challenges. Detailed information duties, purpose limitation, adequacy and necessity rules, and the establishment of qualified consent as the basis for personal data-intensive relations gradually joined access and rectification rights. As stated by Gomes [36], the "traditional" data protection rights already present in sectoral regulations were joined by "new" rights brought about by LGPD (and corresponding duties), such as data portability, revocation of consent, anonymization, among others. The LGPD would come into play to unify all these aspects and add further norms to cater to the needs of a society of ubiquitous connection, considering both demands for the protection of fundamental rights and for innovation and flexibility in data flow schemes.

1.3. The General Data Protection Law

In 2018, Brazil enacted an overarching data protection law which covers all personal data processing activities by natural or legal purposes[37]. In 2019, the country's National Data Protection Authority was created. This makes up a new, unified data protection framework in the country, in the sense that all previous and subsequent regulation must adapt to the architecture put forth by the LGPD.

This means there are bound to be areas where balancing efforts will be necessary. LGPD recognizes this by stating that its sanctions do not substitute those stated in other laws, whether civil, administrative, or penal in nature (art. 52, §2). It does, however, represent a true architecture of data

[32] CFM and SBIS, 'Cartilha Sobre Prontuário Eletrônico', 2012.

[33] Rodrigo Ichikawa Claro Silva and Ana Cláudia Corrêa Zuin Mattos do Amaral, 'Ônus e Bônus Da Evolução Tecnológica No Tratamento de Dados Por Serventias Notariais e Registrais', in *Proteção de Dados: Fundamentos Jurídicos*, ed. Tarcisio Teixeira and Américo Ribeiro Magro (Salvador: JusPodivm, 2020), 139–65.

[34] Walter Britto Gaspar, Eduardo Magrani, and Samara Castro, 'Vácuos Eleitorais, Desinformação e a Desgovernança de Dados', *Estadão*, 15 June 2020.

[35] One potential regulatory subject that merits mentions is the recent move toward legislating neurorights, that is, those rights related to the use of data derived from brain functions, for example via brain-machine interfaces. Chile is a frontrunner in this regulatory area, having approved legislation inscribing neurorights into its Constitution María Izabel Cornejo Plaza, 'Neuroderechos en Chile: consagración constitucional y regulación de las neurotecnologías', *Somos Iberoamérica* (blog), 1 February 2023, https://www.somosiberoamerica.org/tribunas/neuroderechos-en-chile-consagracion-constitucional-y-regulacion-de-las-neurotecnologias/.. In Brazil, proposed bill n. 522/2022 would alter the LGPD to include neural information as sensitive personal data Brasil and Câmara dos Deputados, 'PL 522/2022', 9 March 2022, https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317524..

[36] 'Novos Direitos', *GV Executivo* 18, no. 4 (2019): 35–37.

[37] An unofficial translation of the LGPD is available at: https://cyberbrics.info/brics-data-protection-laws, accessed April 1st, 2025.

protection in Brazil, since it lays out the foundations, principles, duties, and rights to be observed whenever personal data are processed.

A few preliminary aspects of the law should be highlighted. First, the definition of "personal data" is similar to that already commented, mentioning "identified and identifiable" natural persons – a feature of all BRICS countries' personal data architectures, except for South Africa, which also extends this protection to juristic persons. Personal data processing is allowed under ten legal bases (art. 7), including consent, legitimate interests of the controller or third parties, for the protection of health (public health and the subject's life and wellbeing), for the execution of contracts, among others. There is a specific legal basis for processing done for the execution of public policies and another for research purposes.

Sensitive personal data have a more restricted list of legal bases, excluding legitimate interests and the execution of contracts (art. 11). It is important to note that sensitive personal data are defined in a closed list, being those related to "racial or ethnic origin, religious conviction, political opinion, enlistment in labour union or religious, philosophical or political organisation, data referring to health or sexual life, genetic data or biometric data" (art. 5). Creating a separate category of personal data afforded special protection is a characteristic shared by almost all BRICS' personal data architectures, except for the Indian law. This approach varies among BRICS countries. China's PIPL presents an illustrative list of sensitive personal data – defined as data "that can easily lead to the infringement of the personal dignity of natural persons or the harm of personal or property safety once leaked or illegally used" (art. 28, PIPL). Russia and South Africa, similarly to Brazil, refer to closed lists of types of data, but with varying scopes – Russia's FZ-152 law contains a shorter list, whereas South Africa's POPIA goes beyond that of Brazil in some aspects. These discrepancies may present challenges when structuring legal interoperability schemes between BRICS countries' personal data architectures.

Another point of note is the treatment given to personal data of minors, which is subject to the same legal bases, but, as per art. 14 of the law, needs to be processed exclusively in the minor's best interest. This wording is aligned with how Brazilian law approaches rights of minors, an aspect that has been recently reiterated by the ANPD in an official announcement[38].

As mentioned earlier, LGPD does not apply to criminal enforcement and investigation activities, as well as public security, national defence and State security, referencing the enactment of specific legislation on these subjects. A Commission of Jurists brought together by the Brazilian Chamber of Deputies in 2019 is developing this proposed legislation, commonly called "Penal" or "Criminal" LGPD. A first draft was released, but there is yet no clear timeline of its parliamentary debate and possible enactment[39].

LGPD also excludes other hypotheses, such as data processing made for strictly personal purposes; for journalistic, artistic, and academic purposes; and of data that is stored in Brazil from countries with an equal level of protection and which are not transferred to other controllers in Brazil. On this point, comparison among BRICS countries reveals significant variety, with India, Russia and China containing the broadest exemptions (with general exemptions such as due to national sovereignty, security, and public interest, and few oversight mechanisms).

Finally, an important preliminary note is that the law has extraterritorial application. This means it will apply even to those controllers or operators not located in Brazil. Extraterritorial application is

[38] ANPD, 'Enunciado n. 1 de 2023' (2023), https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf.
[39] STJ, 'Comissão Entrega à Câmara Anteprojeto Sobre Tratamento de Dados Pessoais Na Área Criminal', Portal do STJ, 5 November 2020, https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx.

triggered when: the processing operation aims at providing goods or services in Brazil; the data processed are relative to people located in Brazil; or the data processed have been collected in Brazil.

1.3.1. Structure and content of the LGPD

LGPD is framed by ten data protection principles – eleven if counting amongst them "good faith" ("*boa-fé*"), mentioned in the *caput* of article 6. These are similar to those of the European General Data Protection Regulation (GDPR), which served as inspiration to the Brazilian law, and also echoes those of other BRICS countries' personal data protection laws This explicitly principles-based approach is not found only in the Indian Digital Personal Data Protection Act of 2023, which does not contain a section dedicated to principles of data protection, although elements of the following principles (i.e., purpose limitation, data minimization and accuracy, security etc.) are reflected in data principals' rights and data fiduciaries' obligations throughout the Act. The LGPD's personal data protection principles are:

(i) Purpose (legitimate, specified and explicitly informed to the data subject, barred further processing for incompatible purposes);
(ii) Adequacy (the data processed must be related to the stated purpose);
(iii) Necessity (data minimization, barring the collection and processing of excessive data);
(iv) Free access (a data subject must be allowed to access their own data in an easy and inexpensive manner);
(v) Quality (data must be up to date, correct and clear);
(vi) Transparency (the data subject must be clearly informed of the processing and the processing agents involved);
(vii) Security (adequate technical and administrative measures must be taken toward a secure data environment);
(viii) Prevention (necessary measures to prevent incidents involving the data must be taken);
(ix) Non-discrimination (data processing must not be done in a discriminatory manner or toward discriminatory purposes); and
(x) Accountability and responsibility (the data controller must be able to demonstrate compliance with the law).

The mention to "good faith" is important since it references a long-standing interpretative tradition of contracts in Brazilian civil law whereby juridical dealings are to be interpreted according to a series of contextual elements, such as the behaviour of the contracting parties, the habits and current market practices and the context of the negotiation of the contract. It is interesting to note that a mention to "good faith" is also present in China's Personal Information Protection Law (PIPL), art. 5[40], when listing principles for the processing or personal information.

This matters in analysing how data protection principles are observed in practice since the law seeks to adopt a regulatory approach that allows personal data flows and does not impose disproportionate barriers to them. From a perspective of contextual privacy[41], it makes sense to consider the legitimate expectations of the parties involved, their relative positions towards each other in terms of information and power and the reasonable intent of each party when entering into a personal data-intensive relation to measure the degree of compliance with data protection law. As summarized by Bioni [42]:

[40] People's Republic of China, 'Personal Information Protection Law' (2021), https://personalinformationprotectionlaw.com/PIPL/article-5/.
[41] Bruno Ricardo Bioni, *Proteção de Dados Pessoais: A Função e Os Limites Do Consentimento*, 2nd ed. (Rio de Janeiro: Forense, 2020).
[42] 229.

> Contextual privacy resides exactly in the trust deposited by the issuer of information to their recipients, in the legitimate expectation that their personal data will be used and shared according to the context of a pre-established relationship or the original purpose that originated the publicization of the data; particularly, in the hope that the flow of their personal information will not hamper and betray their capacity to fully and freely develop their personality and social participation.

In other words, besides the precise obedience to all duties and rights granted by the law, and besides observance of the ten principles listed in the paragraphs of article 6, context matters in interpreting the relations regulated by LGPD. This is further reinforced by the law's risk-based approach to data protection regulation, embracing a paradigm of prevention and mitigation as well as considering such measures when determining sanctions.

Heavily inspired by the GDPR[43], many aspects of LGPD look akin to the European regulation. There are, however, also aspects unique to the Brazilian legal context, as well as possible connections to personal data architectures of other BRICS countries.

The law creates specific data subject rights, including access, rectification, deletion and opposition (traditionally named "ARCO rights" in Latin American data protection schemes). These are similar in content to those found in GPDR (chapter 3) and PIPL (chapter IV), with the rights to access, correct or complete, delete and copy data present in all three.

Portability is another right granted to the data subject by LGPD. Related to this, there are provisions that data processed by public authorities should follow interoperability standards (art. 25) and that the Authority may provide interoperability standards to enable portability (art. 40). In spite of this, interoperability standards do not feature in the Authority's 2021-2023 Strategic Plan [44], leaving portability rights under a degree of uncertainty for the time being. On this point, the Authority might find inspiration in China's legal framework, where portability is also present in PIPL art. 45 and was recently specified in the Network Data Security Management Regulation. According to the latter, portability is available under the following conditions: "(i) verifying the true identity of the data subject; (ii) the legal basis for processing the concerned personal information must either be consent or contract necessity; (iii) the transfer is technically feasible; and (iv) the transfer will not harm the legitimate rights and interests of others"[45].

Finally, a few other highlights of the Brazilian data protection law are as follows. The law dedicates a full chapter to data processing employed by public authorities. In summary, this kind of processing

[43] GDPR's influence over LGPD and other national data protection laws is well documented. Besides the aforementioned similarity in data protection principles, the LGPD draws on GDPR in terms of user rights (including, e.g., data portability), definitions (e.g., of personal data and of sensitive, or special category, data), data retention and deletion requirements, record-keeping, its extraterritorial scope and others. The LGPD is, however, broader and less proscriptive in its text than the GDPR, leaving much to the interpretation of the Brazilian National Data Protection Authority. See Raymond H Geistel, 'GDPR, PIPL & LGPD: Privacy Regulations & Policies Across the Globe', *Cybersecurity Undergraduate Research*, ODU Digital Commons, 11 (22 November 2021); Laila Neves Lorenzon, 'Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement', *Revista do Programa de Direito da União Europeia* 1 (15 March 2021): 39–52; Abigayle Erickson, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD', *Brooklyn Journal of International Law* 44, no. 2 (1 July 2019): 859.

[44] ANPD, 'Planejamento Estratégico 2021-2023' (Brasília, 2021).

[45] Carolyn Bigg et al., 'CHINA: Enhanced and Clarified Data Compliance Obligations on Handlers of "Network Data", Covering Personal Information and Important Data, and Operators of Online Platforms from 1 January 2025', Privacy Matters, 16 October 2024, https://privacymatters.dlapiper.com/2024/10/china-enhanced-and-clarified-data-compliance-obligations-on-handlers-of-network-data-covering-personal-information-and-important-data-and-operators-of-online-platforms-from-1-january-2025/.

must be attached to a public interest purpose, a specific public agency's mandate and under strict transparency rules. Public-private partnerships are regulated by the same chapter, enacting a general rule that forbids data transfers from public entities to private entities, as well as shared used of data between them, except in a closed, albeit extensive, list of hypotheses (art. 26 and 27). As stated before, some obligations are made immediate in the case of public authorities, such as the interoperability of databases, communication of the agreements involved in public-private partnerships to the Authority and the nomination of a data protection officer[46]. Others, however, lack sufficient specificity or result in counter-intuitive interpretations – e.g., the aforementioned extensive exemptions to public-private sharing of personal data in art. 26 and 27 and their use of undefined concepts.

International transfers of personal data under the LGPD are allowed in a few instances, which play a comparable role to the legal bases mentioned earlier. The law mentions adequacy decisions by the Authority on foreign countries' protection level as well as safeguards offered by the controller, such as specific or standard contractual clauses, global corporate norms, and seals and certificates. Other hypotheses are given, related to the execution of public policies, international agreements and protection of life and wellbeing.

One note on this aspect of the law is that its text, as is, does not fully clarify these hypotheses. For adequacy decisions, global corporate rules and contractual safeguards, the Authority has enacted further regulation specifying their requirements and giving detailed contours of these cases. ANPD Resolution n. 19, of August 2024, brings a more detailed set of international transfer rules, as well as model contractual clauses to be used[47].

In other instances, the wording of the law is unclear, and the Authority will need to exercise its interpretative capacity to make the rules enforceable. For example, when the law authorizes foreign transfers that "result in a commitment undertaken in an international cooperation agreement" (art. 33, VI), the strict wording creates a state of uncertain legality between the time of the transfer of data and the signature of said agreement – it will only have been legal if the commitment is undertaken under the agreement. This seems excessively complex and prone to confusion or misuse, and a better wording would potentially have focused on the instrumentality of said data to the negotiation process and left out considerations of whether it results in a commitment. A second controversy comes when data transfers are authorized if "necessary for international judicial cooperation between public intelligence, investigation and enforcement agencies" (art. 33, III). Further specification of what kinds of activities fall under this hypothesis is necessary, since the law excludes from its application criminal investigation and enforcement activities, public security, and national and State defence, as pointed out earlier.

One last, but not less important, point relates to collective litigation in data protection rights under the LGPD. Zanatta[48] recounts how Brazil has a "very strong tradition of diffuse and collective rights, which left a mark in the institutional and judicial development of the last 30 years in the country" (p. 204). This collectivization, as the author calls it, takes the form of Civil Public Actions (*Ações Civis Públicas*, or ACP; Zanatta also refers to the denomination "Privacy Class Actions", p. 203). In the LGPD, they are

[46] In general, the law demands a DPO for any processing operation; however, a recent regulation by the Authority (Eduardo Mattos et al., 'Application of LGPD to Small-Sized Processing Agents: Non-Official Translation of the ANPD Regulation', CyberBRICS, 31 March 2022, https://cyberbrics.info/application-of-lgpd-to-small-sized-processing-agents-non-official-translation-of-the-anpd-regulation/.) has excepted this rule for small and medium businesses and start-ups – see Curzi et al. 'LGPD Regulation for Small Agents: Highlights, Advances and Future Paths', CyberBRICS, 30 March 2022, https://cyberbrics.info/lgpd-regulation-for-small-agents-highlights-advances-and-future-paths/.

[47] Brasil [ANPD], 'Resolução CD/ANPD n. 19/2024', Diário Oficial da União, 23 August 2024, https://www.in.gov.br/web/dou.

[48] 'A Tutela Coletiva Na Proteção de Dados Pessoais', *Revista Do Advogado* Nov, no. 144 (2019): 201–8.

legitimized by articles 22 and 42, §3, which recognize the possibility of collective action against violations of data protection rights. This is a unique feature of the Brazilian data protection architecture in comparison with other BRICS countries.

The next section will highlight some of the notable cases involving this class of action in the realm of data protection, before and after LGPD went into force. However, it is important to note that this process of collectivization is a reflection of the nature of the rights under protection, which, although referring to individuals, have profound collective roots and consequences due to the very risks involved in the operationalization of digital markets[49].

These are the general aspects of the Brazilian LGPD. One can see a linear progression from strict privacy conceptualizations under intimacy and private life doctrines, rooted in the intimate sphere and the right to be let alone, and a broadening of this approach in successive laws in response to technological advancements, to a point where a specific personal data protection framework proves necessary. This is all rooted in the idea of allowing the full realization of personality, largely translated into digital identities in the form of personal data and thus requiring special protection. The following section will discuss some recent developments in the institutional framework of data protection in Brazil and how they relate to the rights of the data subject.

1.4. Regulatory developments

There are many moving parts in the data protection framework in Brazil. Existing public agencies need to coordinate their activities under the new law and with a new National Data Protection Authority given ample control capacities. The Authority has entered a field rich with other institutional actors – courts, prosecutors, consumer protection agencies and other regulatory agencies – and will need to coordinate with them, as well as provide guidance as to how the law should be interpreted and concrete instruments for private actors to comply and mitigate risks.

1.4.1. The Initial Application of LGPD

From a judicial perspective, the State Prosecution of the Federal District (MPDFT) had a proactive role in data protection beginning in 2018, when it created a Specialized Unit on Data Protection and Artificial Intelligence [50]. With LGPD not yet in force, the State Prosecution conducted some high-profile investigations into cybersecurity incidents involving personal data of Brazilian citizens – one involving Netshoes [51], an e-commerce service, one against Uber [52] and one against Banco Inter [53]; all regarding undue access to personal data of users of these services. Since LGPD entered into force, the agency has prosecuted two notable cases of commercialization of personal information databases: against Infortexto Ltda., a company which offered structured databases of personal data of Brazilian citizens;

[49] Zanatta, 202.
[50] MPDFT, 'P. N. PGJ n. 539/18', 12 April 2018, https://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pessoais/Portaria_PGJ_n2018_0539.pdf.
[51] MPDFT, 'Rec. n. 01/18 (Netshoes)', MPDFT, 25 January 2018, https://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pessoais/Recomendacao_Comissao_Protecao_Dados_2018_01.pdf.
[52] MPDFT, 'Port. n. 01/18 (Uber)', MPDFT, 6 February 2018, https://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pessoais/Instauracao_de_PP_Uber.pdf.
[53] Alberto Alerigi Jr, 'Banco Inter Faz Acordo de R$1,5 Mi Com Ministério Público Em Caso de Vazamento de Dados', uol.com.br, 19 December 2018, https://www.uol.com.br/tilt/noticias/reuters/2018/12/19/banco-inter-faz-acordo-de-r15-mi-com-ministerio-publico-em-caso-de-vazamento-de-dados.htm.

and Serasa Experian, a Brazilian credit protection agency that owns one of the biggest consumer databases in the world [54].

The Federal Prosecution (MPF) has also had an important role asserting data protection rights since the enactment of LGPD. In 2021, it published a joint recommendation alongside ANPD, the National Consumer Protection Office (SENACON) and the Brazilian Competition Bureau (CADE) regarding the change in Whatsapp's privacy rules [55]. This prompted the messaging service to delay the mandatory rollout of the new rules and, in the end, to decide not to cut access to the app to any users who did not accept the new terms [56]. The MPF also demanded information from the Health Minister regarding a personal data breach under investigation involving the "ConecteSUS" system, used to register vaccination and other health data connected to the use of the Brazilian Unified Health System (SUS)[57].

Finally, the agency has published technical studies and opinions on matters related to data protection in Brazil, such as the announced plans to privatise SERPRO, the Federal Data Processing Service – which, among other things, holds in its databases the tax information of all Brazilian citizens, including government authorities[58]; and the proposed "Criminal LGPD" draft[59]. Recently, it has been called by a coalition of civil society organisations to investigate and prosecute "Córtex" [60], a system spearheaded by a branch of the Justice and Public Security Ministry with the potential to unify 160 databases and provide persistent electronic monitoring of 360 thousand people [61].

---

[54] MPDFT, 'MPDFT Ajuíza 1ª Ação Civil Pública Com Base Na LGPD', MPDFT.mp.br, 22 September 2020, https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/12384-mpdft-ajuiza-1-acao-civil-publica-com-base-na-lgpd; MPDFT, 'MPDFT Obtém Decisão Que Suspende a Venda de Dados Pessoais Pela Serasa Experian', MPDFT, 23 November 2020, https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/12586-mpdft-obtem-decisao-que-suspende-a-venda-de-dados-pessoais-pela-serasa-experian; Matheus Garzon, 'Após Ação Do MPDFT, Justiça Manda Tirar Do Ar Site Que Vende Dados Pessoais', Metrópoles, 22 October 2020, https://www.metropoles.com/distrito-federal/justica-distrito-federal/apos-acao-do-mpdft-justica-manda-tirar-do-ar-site-que-vende-dados-pessoais.

[55] Convergência Digital, 'Cade, ANPD e MPF Alertam WhatsApp Que Compartilhamento Compulsório Viola a LGPD', Convergência Digital, 7 May 2021, https://www.convergenciadigital.com.br/Internet/Cade%2C-ANPD-e-MPF-alertam-WhatsApp-que-compartilhamento-compulsorio-viola-a-LGPD-56891.html?UserActiveTemplate=mobile%2Csite.

[56] ANPD, 'Após Esforço Interinstitucional, WhatsApp Se Compromete a Atender Às Recomendações Sobre Sua Política de Privacidade', Gov.br, 23 August 2021, https://www.gov.br/anpd/pt-br/assuntos/noticias/apos-esforco-interinstitucional-whatsapp-se-compromete-a-atender-as-recomendacoes-sobre-sua-politica-de-privacidade.

[57] André Rigue and Julyanne Juca, 'MPF Pede à PGR Que Solicite Esclarecimento a Queiroga Sobre Ataque Ao ConecteSUS', CNN Brasil, 18 December 2021, https://www.cnnbrasil.com.br/nacional/mpf-pede-a-pgr-que-solicite-esclarecimento-a-queiroga-sobre-ataque-ao-conectesus/.

[58] The MPF's position was that it would not only violate LGPD, but also pose considerable national security risks)PGR, 'Privatização Do Serpro Contraria Legislação e Ameaça Segurança Nacional, Afirma MPF Em Nota Técnica', MPF.mp.br, 25 February 2021, http://www.mpf.mp.br/pgr/noticias-pgr/privatizacao-do-serpro-contraria-legislacao-e-ameaca-seguranca-nacional-afirma-mpf-em-nota-tecnica..

[59] The MPF's position was that it would impose disproportionately restrictive obligations on data transfers between authorities, among other issues PGR, 'MPF Alerta Para Restrições Previstas No Anteprojeto de Lei de Proteção de Dados Para a Persecução Penal', MPF.mp.br, 1 March 2021, http://www.mpf.mp.br/pgr/noticias-pgr/mpf-alerta-para-restricoes-previstas-no-anteprojeto-de-lei-de-protecao-de-dados-para-a-persecucao-penal..

[60] Gabriela do Vale, 'Sociedade Civil Pede Ao MPF Investigação Do Sistema Córtex', TeleSíntese, 10 February 2022, https://www.telesintese.com.br/sociedade-civil-pede-ao-mpf-investigacao-do-sistema-cortex/.

[61] Conectas Direitos Humanos et al., 'Rep. Sistema Córtex', February 2022, https://www.telesintese.com.br/wp-content/uploads/2022/02/representacao-controle-externo-da-atividade-policial.pdf.

1.4.2. Continuing Fragmentation, despite the ANPD

On the other side of the bench, the National Data Protection Authority will also need to coordinate efforts with the various judicial decision-making bodies and instances. A joint research project conducted by the Brazilian Institute of Teaching, Research and Development (IDP) and JusBrasil looked at 274 decisions of lower courts in all Brazilian states from September 2020 and August 2021. Their analysis concludes, among other aspects, that many of these courts have applied LGPD as a complement to other legislation and has not engaged deeply with data protection doctrine or theory. Most discussions revolved around the first two chapters of the law, containing introductory aspects, definitions, principles, foundations and legal bases for personal data processing, followed by data subjects' rights in third place and legal bases for sensitive data processing in fourth [62].

Additionally, the São Paulo state court (TJSP) presented a substantially larger number of decisions compared to other state courts and other instances [63]. Although this is not discussed in the findings, this may be related to the fact that São Paulo is a state where the consumer protection unit (Procon-SP) has been very active in matters of data protection, as well as the Brazilian Consumer Defence Institute (IDEC). IDEC proposed a Civil Public Action against the operator of one of the state's subway lines (ViaQuatro) for its plan to implement facial recognition on the stations. A final decision fined ViaQuatro in 100 thousand reais and forbade the company from reactivating its facial recognition initiative [64]. In 2022, IDEC and others moved a new ACP against the state's general subway operator, "Metrô de SP", to bar the use of facial recognition, requesting the immediate suspension of the system and an indemnification of at least 42 million reais [65].

Another study, conducted by the Opice Blum law firm, specialized in digital rights, focused on 2021 and revealed more data on the first steps of LGPD in courts. The study analysed 465 decisions in courts in seven states and three federal and regional courts. A few interesting findings were:

(i) The greater concentration of decisions at the São Paulo State Court is also verified in this study;
(ii) 77% of all decisions did not result in condemnations;
(iii) Almost 40% of the cases analysed involved security incidents;
(iv) Around 90% of decisions considered that moral damages reparation required proof of damage, *i.e.*, damages were not considered *in re ipsa*;
(v) When sanctions are applied, they go from 600 reais to 100 thousand reais, with most (88%) between 2 thousand and 11 thousand reais [66].

FGV's E-commerce studies centre (NEEC) also conducted research that supplements these findings, confirming a significant concentration of cases regarding consumer relations and LGPD at the São Paulo

[62] Laura Schertel et al., 'LGPD Nos Tribunais', JusBrasil, October 2021, https://www.jusbrasil.com.br/static/pages/lgpd-nos-tribunais.html.
[63] Schertel et al.
[64] IDEC, 'Idec Obtém Vitória Contra Reconhecimento de Emoções No Metrô de SP', idec.org.br, 10 May 2021, https://idec.org.br/noticia/idec-obtem-vitoria-contra-reconhecimento-de-emocoes-no-metro-de-sp.
[65] Idec, 'Ação Quer Vedar o Uso de Tecnologias de Reconhecimento Facial Pelo Metrô de São Paulo', idec.org.br, 3 March 2022, https://idec.org.br/release/acao-quer-vedar-o-uso-de-tecnologias-de-reconhecimento-facial-pelo-metro-de-sao-paulo.
[66] Opice Blum, 'Relatório Anual de Jurimetria 2021', 27 January 2022, https://images.jota.info/wp-content/uploads/2022/01/relatacc83c2b3rio-anual-jurimetria-24-01-versacc83o-final.pdf; Letícia Paiva, 'LGPD: 77% Das Decisões Não Resultaram Em Condenação Em 2021', Jota, 27 January 2022, https://www.jota.info/justica/lgpd-condenacao-77-das-decisoes-nao-27012022.

State Court and reiterating the issue of *in re ipsa* moral damages derived from personal data incidents as a pivotal legal debate [67].

The issue of the application of the law in courts will be informed by the institutional arrangements that come up while the Authority attempts to exercise its legal capacities. This is due to the determination that the Authority give the final interpretation of the LGPD (art. 55-J, XX; art. 55-K, sole paragraph), as well as its executive capacities as overseer of the law's application, such as requesting information, publishing regulation and technical opinions, analysing data subject requests and applying sanctions, even regarding public bodies' processing activities (art. 55-J). This is seemingly in conflict with, firstly, judicial instances' independent analysis and interpretation of facts and law; and, secondly, with the independence of the judicial branch ensured by the separation of powers. The latter is made especially evident when considering that the Authority is not structured as an independent entity, but as a branch of the Federal administration.

LGPD does not resolve this conflict, as it solely mentions the need to coordinate actions with other authorities, and will need to be dealt with in the future. One institution that ANPD will need to coordinate with on this is the National Justice Council, a judicial organ constitutionally (Federal Constitution, art. 103-B, §4) and legally (Civil Procedure Code, art. 196) competent over administrative proceedings of the judicial branch in Brazil [68].

1.4.3. The role of the Supreme Court

Even before the Authority was in place and the LGPD was in effect, the country's Supreme Court had also held an important and impactful judgement on the matter of the constitutional standing of data protection in Brazil. IBGE, the Brazilian Institute of Geography and Statistics, was authorized, via presidential order n. 954/2020 (MP 954/20), to obtain from telecommunications companies the contact information of 200 million individuals. The justification was that the institute would need to conduct the national census via telephone due to the covid-19 pandemic. This was seen by many as a highly disproportional measure, since in person interviews for the census are usually conducted with a statistically representative sample of households, besides the evident deviation of the telecoms' original purpose for collecting and processing those data.

A complete narration of the case would require at least a chapter of its own, but Bioni and Monteiro [69] portray the impact of the judgment. In addition to establishing data protection as an autonomous fundamental right rooted in informational self-determination under the Brazilian Constitution and highlighting the importance of procedural guarantees to its realization [70], the case also marked a decisive change in the position of the Court [71]:

---

[67] Erica Bakonyi, 'LGPD em números. Resultados e tendências no contexto "E-commerce"' (2ª reunião do NEEC, Rio de Janeiro, January 2023), https://direitorio.fgv.br/sites/default/files/arquivos/apresentacao-lgpd-em-numeros-neec.pdf; NEEC, '2ª Reunião do Núcleo de Estudos em E-Commerce', Reuniões do NEEC (Rio de Janeiro: FGV Direito Rio, January 2023), https://direitorio.fgv.br/sites/default/files/2023-01/direito_rio_livro_neec_ap3_v3.pdf.

[68] CDTV, *9º E-Fórum TIC Na Justiça* (CDTV Youtube, 2021).

[69] 'A Landmark Ruling in Brazil: Paving the Way for Considering Data Protection as an Autonomous Fundamental Right'.

[70] Gaspar Pisanu, Rafael A. F. Zanatta, and Mariana Marques Rielli, '"Please Do Not Share": Brazilian Supreme Federal Court Rules in Favor of Privacy', Access Now, 14 May 2020, https://www.accessnow.org/brazilian-supreme-federal-court-rules-in-favor-of-privacy/.

[71] Bioni and Monteiro, 'A Landmark Ruling in Brazil: Paving the Way for Considering Data Protection as an Autonomous Fundamental Right'.

> In previous case-law, the Court struggled to recognize stored data, such as subscribers data, as data protected by Art. 5, XII. Long standing precedents only granted such type of protection to data in motion, like ongoing telephone calls or data being transmitted. Acknowledging the need to update this understanding in light of new technologies and the impact that the misuse of data can have upon individuals and the society, another argument was presented: the need to recognize the right to protect personal data as an autonomous fundamental right.

One more data protection case currently in the Supreme Court's docket is Direct Unconstitutionality Action n. 6649, which refers to Presidential Decree n. 10.046. This Decree creates a general shared data regime between government agencies, including biometric data, family life and labour information, among other aspects of individual identity. The constitutionality of the Decree is put in question for violation of the constitutional provisions regarding privacy and by referring to the same Court's decision on the IBGE case, described above [72]. The case is still ongoing, and its results might inform how personal data processing and sharing by governmental entities is interpreted – including by the ANPD.

1.4.4. A Complex Relation with the Judiciary

Still in the area of ANPD's relations with the judicial branch, one particularly sensitive subject might be the publicity of judicial proceedings and decisions. There is notice of efforts to institute secrecy of such proceedings based on the LGPD [73] and the country's Supreme Court has recently accepted a case where the matter is at hand. The latter is particularly interesting because it discusses the subject of publicity of judicial proceedings applied not to courts, but to private judicial aggregators, i.e., sites specialized in indexing judicial decisions [74]("Escavador" and "JusBrasil" being two prominent examples in the Brazilian market).

The issue of access to information in opposition to data protection rights has also been emerging in other areas. The Superior Electoral Court (TSE) has recently been called to decide on whether campaign donation data, among other information involving personal data of people participating in electoral campaigns, should be made secret due to data protection concerns. The President of the Court, however, recently declared that, although the issue is complex and merits a long and wide discussion, and that case-by-case analysis should reveal instances where the balance favours privacy, the rule, for the time being, is for transparency in favour of the public interest [75].

There have also been cases where the Executive branch refuses to provide public interest information based on the LGPD. Machado [76] describes how the fear of LGPD's sanctions has been moving public servants toward caution and secrecy in sharing public interest data, such as the educational microdata

---

[72] Gilmar Mendes, ADI 6649 (23 December 2020); OAB, 'Petição Inicial, ADI 6649', STF, 18 December 2020, https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754736097&prcID=6079238#; Estela Aranha, 'Decretos 10.046 e 10.047 de 2019, Parecer Da Comissão de Proteção de Dados e Privacidade' (Rio de Janeiro, 2020).

[73] Dânton Zanetti, 'Proteção de Dados Pessoais e Publicidade Processual: Um Contrassenso?', Migalhas, 15 April 2021, https://www.migalhas.com.br/depeso/343796/protecao-de-dados-pessoais-e-publicidade-processual-um-contrassenso.

[74] Severino Goes, 'Decisão Abre Debate Sobre Direito à Informação e Uso Da LGPD', ConJur, 18 May 2021, https://www.conjur.com.br/2021-mai-18/decisao-abre-debate-direito-informacao-uso-lgpd.

[75] José Marques, 'Fachin Descarta TSE Impor Sigilo Sobre Dados de Doações Eleitorais', Folha de S. Paulo, 23 February 2022, https://www1.folha.uol.com.br/poder/2022/02/fachin-descarta-tse-impor-sigilo-sobre-dados-de-doacoes-eleitorais.shtml?origin=folha.

[76] 'Há Retrocessos Na Lei Geral de Proteção de Dados', Folha, 28 February 2022, https://www1.folha.uol.com.br/colunas/cecilia-machado/2022/02/ha-retrocessos-na-lgpd.shtml?origin=folha.

yearly published by INEP, a research institute linked to the Education Ministry, since the 1990s [77]. These are invaluable data to allow oversight regarding the quality of education in the country.

Other similar situations abound, some of which were recounted during a Chamber of Deputies' public hearing on balancing the Access to Information law and LGPD, held in 2021. The examples brought to the fore in the occasion included refusals to provide information to the MPF in the course of investigations; the establishment of a 100-year secrecy rule over various public interest information; and refusals to provide data to journalists conducting investigations and to other interested parties under personal data protection justifications [78]. Resolving the necessary balancing of the application of LAI and LGPD will require coordination with various organs and entities and a careful look at regulatory and technical solutions to providing access to information while preserving privacy.

1.4.5. Blending LGPD with Consumer law and Competition law

Another field where the National Data Protection Authority will need to seek coordination and cooperation proactively is consumer protection. SENACON, a specialised office subject to the Justice and Public Security Ministry, oversees the National Consumer Protection System. This system is composed of a variety of units of "Procons", state or municipal offices of consumer protection responsible for processing consumer requests, amounting to 981 units in the Brazilian territory [79].

Some of these units have been particularly active in personal data protection, such as São Paulo state's Procon (Procon-SP). Besides publishing a basic data protection guide to inform the general public [80], the unit has under its belt cases and notifications against Serasa[81]; some of the major telephone companies in the country[82]; and TikTok[83]. Coordinating understandings with these entities shall prove invaluable to executing ANPD's vision for the application of LGPD.

ANPD has made cooperation agreements with SENACON, CADE [84] and NIC.br. The latter is the operational branch of the Internet Steering Committee in Brazil (CGI.br), and the partnership is aimed at building know-how and sharing information [85]. It also has a technical cooperation agreement with

---

[77] Maria Angélica Minhoto, Pedro Arantes, and Soraya Smaili, 'A Quem Interessa Impedir o Acesso Aos Microdados Do Inep?', Folha, 24 February 2022, https://www1.folha.uol.com.br/blogs/sou-ciencia/2022/02/a-quem-interessa-impedir-o-acesso-aos-microdados-do-inep.shtml.

[78] Câmara dos Deputados, 'Fiscalização Financeira e Controle - Execução Da LGPD/LAI', Câmara dos Deputados (YouTube), 16 November 2021, https://www.youtube.com/watch?v=jA5yIsFkSZM; Lara Haje, 'Acesso à Informação Não Pode Ser Prejudicado Por Conta de Lei de Proteção de Dados, Dizem Especialistas', Portal da Câmara dos Deputados, 18 November 2021, https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de-protecao-de-dados-dizem-especialistas/.

[79] SENACON, 'Sindec Boletim - 2019' (Brasília, 2019).

[80] PROCON-SP, EPDC, and Gov. do Estado de SP, 'Lei Geral de Proteção de Dados: O Que Você Precisa Saber', December 2020, https://www.procon.sp.gov.br/wp-content/uploads/2021/02/Cartilha-LGPD-2021.pdf.

[81] For a data breach involving the personal data of 220 million Brazilian citizens PROCON-SP, 'Procon-SP Notifica Serasa', Procon.sp.gov.br, 28 January 2021, https://www.procon.sp.gov.br/procon-sp-notifica-serasa/..

[82] Also for a data breach, this time involving data of 100 million mobile phones PROCON-SP, 'Procon-SP Notifica Claro, Oi, Tim, Vivo e Psafe', Procon.sp.gov.br, 17 February 2021, https://www.procon.sp.gov.br/procon-sp-notifica-claro-oi-tim-vivo-e-psafe/..

[83] Requesting information on the company's safeguards regarding children's data on the platform PROCON-SP, 'Notificação TikTok', Procon.sp.gov.br, 14 May 2020, https://www.procon.sp.gov.br/notificacao-tik-tok/..

[84] João Paulo Vieira Tinoco and Mauricio Koki Matsutani, 'CADE Firma Parceria Com ANPD - Congresso Em Foco', Congresso em Foco, 10 October 2021, https://congressoemfoco.uol.com.br/tipo/patrocinado/salve-seus-dados/cade-firma-parceria-com-anpd/.

[85] ANPD, 'Convênios e Transferências', ANPD, 17 January 2021, https://www.gov.br/anpd/pt-br/acesso-a-informacao/repasses-e-transferencias-de-recursos-financeiros.

the Superior Electoral Court [86], and the two have published a guide to data protection during election times [87]. The Authority has also recently published guidance to small and micro enterprises regarding cybersecurity [88], guidelines on the definition of processing agents [89] and guidelines for data processing by the public administration [90].

In terms of regulation, added to norms creating governance bodies and bylaws and setting regulatory agendas, it has published six norms. One deals with its regulatory process, establishing guidelines such as social participation and simplification of processes [91]; one on its inspection, control and sanctioning activities [92]; one establishing a special data protection regime for small and micro enterprises and start-ups [93]; one on communication of security incidents[94]; one on the role of data protection officer[95]; and one on international data transfers[96]. These norms were created following public hearing processes held via digital participation platforms as well as live online sessions.

The first two determine organizational and procedural aspects of the Authority's functions, with highlight to the significant space given to preventive and pedagogic action toward data protection risks and controllers' activities. The third regulation implements a series of adaptations of the law to the context of smaller companies and start-ups: an exemption to the indication of a DPO, longer procedural deadlines in administrative processes, and simplified recording and security policy requirements, among others [97]. The definition of the scope of the regulation was careful to exclude from this simplified regime entities whose data processing might "significantly affect fundamental rights and interests of data subjects" (art. 4.I.b), among other criteria aimed at ensuring a balance between protection and flexibility.

ANPD's activities have been conducted in parallel to ongoing discussions on its independence and institutional format. In 2022, a Presidential Decree, later confirmed into law by the National Congress, transformed the Authority from an organ of the Federal Government into an independent authority – called a "special autarchy" in Brazilian public law. This ensures the Authority's technical, administrative and financial autonomy, stability of its directors' mandates, and legitimizes it as a party in moving collective rights actions involving data protection issues in the Brazilian judiciary[98]. Despite this new

---

[86] ANPD, 'ANPD e TSE Assinam Acordo de Cooperação Técnica', ANPD.gov.br, 24 November 2021, https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-tse-assinam-acordo-de-cooperacao-tecnica.
[87] ANPD, 'Em Ano Eleitoral ANPD e TSE Publicam Guia de Eleições', ANPD.gov.br, 3 January 2022, https://www.gov.br/anpd/pt-br/assuntos/noticias/em-ano-eleitoral-anpd-e-tse-publicam-guia-de-eleicoes.
[88] ANPD, 'Guia Orientativo de Segurança Da Informação Para Agentes de Tratamento de Pequeno Porte' (Brasília, 2021).
[89] ANPD, 'Guia Orientativo Para Definições Dos Agentes de Tratamento de Dados Pessoais (Operadores e Controladores) e Do Encarregado' (Brasília: ANPD, May 2021).
[90] ANPD, 'Tratamento de Dados Pessoais Pelo Poder Público (Guia Orientativo)' (Brasília, January 2022), https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf.
[91] ANPD, 'Portaria Nº 16, de 8 de Julho de 2021', DOU, 8 July 2021, https://www.in.gov.br/en/web/dou/-/portaria-n-16-de-8-de-julho-de-2021-330970241.
[92] ANPD, 'Resolução CD/ANPD Nº 1, de 28 de Outubro de 2021', DOU, 28 November 2021, https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513.
[93] ANPD, 'Resolução CD/ANPD Nº 2, de 27 de Janeiro de 2022', DOU, 27 January 2022, https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper; Non-official translation by Mattos et al., 'Application of LGPD to Small-Sized Processing Agents: Non-Official Translation of the ANPD Regulation'.
[94] Imprensa Nacional, 'Resolução CD/ANPD Nº 15', DOU, 24 April 2024, https://www.in.gov.br/web/dou.
[95] Imprensa Nacional, 'Resolução CD/ANPD Nº 18', DOU, 16 July 2024, https://www.in.gov.br/web/dou.
[96] Imprensa Nacional, 'Resolução CD/ANPD Nº 19', DOU, 23 August 2024, https://www.in.gov.br/web/dou.
[97] Curzi et al., 'LGPD Regulation for Small Agents: Highlights, Advances and Future Paths'.
[98] Fabricio da Mota Alves, 'ANPD como autarquia federal: o que muda para a proteção de dados?', JOTA Jornalismo, 14 June 2022, https://www.jota.info/artigos/anpd-como-autarquia-federal-o-que-muda-para-a-protecao-de-dados-no-brasil.

form, ANPD still struggles with budgetary limitations, as other independent autarchies do, since their budgetary plan is subjected to the regular annual national budget plan, leaving them vulnerable to budget cuts and retention of funds by the Executive[99].

1.4.6. Automated Personal Data Processing

Artificial intelligence regulation in Brazil has been an ongoing and controversial discussion for some time. Initial efforts to enact a dedicate Artificial Intelligence Act were met with initial opposition to the contents of the proposed text and to the hastened legislative discussion process. In response, a commission of jurists was created to discuss and propose a new version of the proposed act. Its results have been exhaustively discussed and recently approved in the Brazilian Senate, awaiting further appreciation by the Chamber of Deputies. In the absence of specific regulation, and considering the superposition of AI use cases and the need to process personal data, data protection regulation in Brazil is a relevant legal source for AI, be it in general personal data protection rules and principles as explained so far, or in its specific terms regarding automated processing of personal data.

Article 20 of LGPD creates a right to revision of solely automated decisions which "affect their [the data subject's] interests, including decisions aimed at determining their personal, professional, consumer and credit profiles and aspects of their personality" (art. 20). This right was originally meant to provide human revision of such decisions, but a presidential veto removed it, and the final wording did not mention revision by natural persons.

Importantly, the right also includes (paragraph 1) a duty to inform the data subject on the criteria and procedures adopted to take an automated decision that can impact any interest of the data subject (paragraph 2), the possibility of an audit by ANPD, conditional to the failure to provide said information and focused on investigating discriminatory decision-making. The detailed contours of this right, including technical matters related to explainability of AI systems, are still to be determined by the Authority.

Besides these normative aspects, Brazil has had a period of dispersed AI public investments and programmes followed by the implementation of a Brazilian AI Strategy, which was heavily criticised for lacking strategic and planning elements. This was followed by a revision effort to produce a new AI Strategy, which was announced recently, but has not yet resulted in a new document; and the publication of a Brazilian AI Plan, which amounts to a public investment plan divided between immediate actions and structural actions. This plan is heavily focused on developing capacity in algorithms and computational capacity. It is, however, merely a guiding document, with no binding power[100].

In summary, Artificial Intelligence regulation in Brazil is less of and architecture and more of a blueprint. Even where it sits on the more solid foundations of an actual law – the automated processing part of LGPD – it lacks precise technical definition.

---

[99] Plenário, Acórdão 240/2015 (Tribunal de Contas da União 11 February 2015); Paulo Sampaio, 'A Independência Real Das Agencias Reguladoras No Brasil', *Revista de Direito, Estado e Telecomunicações 5*, no. 1 (2013): 135–74, https://www.academia.edu/4220021/A_Independencia_Real_das_Agencias_Reguladoras_no_Brasil.

[100] Germano P. Johansson Neto, Viviane C. Farias da Costa, and Walter Britto Gaspar, 'Brazil's Artificial Intelligence Plan (PBIA) of 2024: Enabler of AI Sovereignty?', *The African Journal of Information and Communication (AJIC)*, no. 34 (28 December 2024): 1–15, https://doi.org/10.23962/ajic.i34.20424.

1.5. Conclusion

A unified Brazilian data protection system is a recent development. Before the LGPD, many sectoral regulations were the basis not only for privacy and data protection rights in particular instances, but also for institutional structures built around these rights. On top of that, the path from strict privacy interpretations to data protection rights has followed hand in hand with this normative progression. This amounts to a scenario with many moving parts, rooted interests and established bureaucracies revolving around the subject.

This paper aimed to present a general image of the complexity of this scenario, from rules to institutional actors and their interests. Note was given to rising issues and cases related to personal data protection in an attempt to highlight tension points that will need to be addressed by the Authority in its administrative and regulatory capacities.

The new data protection system and its main guardian and operator, the National Data Protection Authority, need to build the avenues for cooperation with these pre-existing institutional arrangements. Some issues might prove controversial and harder to resolve, such as competence disputes. However, the Authority has demonstrated a pro-active stance in seeking out relevant institutional actors to coordinate visions and build understanding.

The administrative capabilities of the Authority are extensive, and on top of its regular attributions it must provide clarity to the many unanswered questions left open in the LGPD. If it takes too long to answer, uncertainty and recourse to other decision-making bodies might ensue, which could fragment the personal data protection system in the long run. Time will tell how these relations will unfurl.

Looking at the broader context of BRICS personal data architectures may provide insights into these challenges. The administrative and enforcement structures built in other BRICS countries vary significantly – from an authority structured as an organ of government, in Russia, to an independent authority without normative powers, as the Data Protection Board of India.

Brazil's ANPD is independent, however its capacity is constrained by budgetary limitations. Since its creation, it has demonstrated an increasingly active stance, having enacted nine sanctions via administrative sanctioning processes, one against a private company[101]; acted on matters of relevant national impact, such as cases involving the sharing of data between WhatsApp and its parent company, Meta[102]; usage of personal data of Meta's user base for AI training; and the establishment of a pay-for-biometric data scheme by Tools for Humanity[103]; and enacted regulations on international data transfers, the role of the *Encarregado*, communication of security breaches, and sanctioning process. Overall, its more prolific work outside of actual sanctions applied might reflect a more preventative and educational focus, as well as its budgetary. However, some areas and cases still require more careful attention and further regulation and control.

---

[101] Coordenação-Geral de Fiscalização, Relatório de instrução nº 1/2023/CGF/ANPD, Fabrício Guimarães Madruga Lopes (ANPD 2023).

[102] ANPD, 'ANPD conclui a análise de adequação da nova Política de Privacidade do WhatsApp à LGPD', Autoridade Nacional de Proteção de Dados, 11 May 2022, https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-conclui-a-analise-de-adequacao-da-nova-politica-de-privacidade-do-aplicativo-a-lgpd; ANPD, 'Após esforço interinstitucional, WhatsApp se compromete a atender às recomendações sobre sua política de privacidade', Autoridade Nacional de Proteção de Dados, 20 August 2021, https://www.gov.br/anpd/pt-br/assuntos/noticias/apos-esforco-interinstitucional-whatsapp-se-compromete-a-atender-as-recomendacoes-sobre-sua-politica-de-privacidade.

[103] Conselho Diretor, Votos no recurso em processo administrativo de fiscalização nº 00261.006742/2024-53, Miriam Wimmer (ANPD 2025).

One such issue is automated decision-making, which has rapidly become more relevant since the enactment of LGPD due to the widespread use of popular generative AI tools. Their indiscriminate use of personal data, including sensitive data, scraped from the internet, without notice, record or any further necessary caution, is an issue that has been faced by authorities in many countries[104], but has fallen on deaf ears in Brazil[105]. On this point, a look to the Chinese efforts to rein-in AI and algorithmic recommendation might provide an interesting reference: companies are required to provide transparency and explainability to the State controller, including code and plain-language explanations, of how algorithmic recommendation tools work; and to label generative AI content and ensure legitimate sources are used in training of such models[106].

Another crucial matter is the specification of technical elements that are mentioned, but not exhaustively defined, in the LGPD. This includes interoperability as well as anonymization standards. These gaps are present in other BRICS countries' data architectures, with the exception of China, that has published specifications on the matter of data portability and interoperability. They could be paths for future collaboration, with specification of BRICS technical standards.

Brazil's personal data architecture, however inspired by the GDPR, is rooted in a long tradition of personality rights and digital rights, with the notable case of the MCI as a landmark in terms of legislative process and innovative contents at its time. Its adoption of a GDPR-style data protection law did not create a clean slate, but rather a fruitful and complex frame where the fundamental right to data protection has been since given form and structure. This is still an ongoing process and among its many moving parts special note is given to the country's Data Protection Authority, which has had to deal with significant challenges and changes since its inception and still struggles to find the right balance between orienting and sanctioning.

In conclusion, this chapter aimed to present and discuss a double coordination challenge for the Brazilian personal data architecture as it stands today. Internally, the main actor in interpreting and implementing the vision of data protection rights of LGPD, the National Data Protection Authority, needs to simultaneously resolve issues of regulatory coordination with other authorities, fill in the legal gaps left by the law, give clarity to data controllers and establish its supervisory role in face of data protection violations. Some of these goals have been more actively pursued than others, as we have shown. Externally, the country needs to find tools to coordinate its own personal data architecture with other relevant commercial and diplomatic partners, such as the BRICS countries. Many convergences and divergences were highlighted in this chapter, that give hints as to what opportunities and challenges for legal interoperability of BRICS personal data architectures exist.

---

[104] Stephanie Borg Psaila, 'Governments vs ChatGPT: Investigations around the World - Diplo', *DiPLO* (blog), 20 April 2023, https://www.diplomacy.edu/blog/governments-chatgpt-investigations/.

[105] Luca Belli, Walter Britto Gaspar, and Natalia Couto, 'Por que o ChatGPT descumpre a LGPD', *Jota* (blog), 25 August 2023, https://www.jota.info/opiniao-e-analise/artigos/por-que-o-chatgpt-descumpre-a-lgpd-parte-2-25082023; Luca Belli, 'Por que o ChatGPT descumpre a LGPD e por que peticionei à ANPD', JOTA Jornalismo, 23 May 2023, https://www.jota.info/artigos/por-que-o-chatgpt-descumpre-a-lgpd-e-por-que-peticionei-a-anpd.

[106] Ashyana-Jasmine Kachra, 'Making Sense of China's AI Regulations', Holistic AI, 12 February 2024, https://www.holisticai.com/blog/china-ai-regulation; AI Watch, 'Global Regulatory Tracker - China', White & Case LLP, 13 May 2024, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china; Rogier Creemers, Graham Webster, and Helen Toner, 'Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022', *DigiChina* (blog), 10 January 2022, https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

2. APPENDIX A – BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD)

Law 13,709/2018, General Data Protection Law (LGPD) as amended by law 13,853 of 2019[1]

CHAPTER I
PRELIMINARY PROVISIONS

Article 1 This Law regulates the processing of personal data, including by digital means, by any natural person or legal entity governed by public or private law, with the aim of protecting the fundamental rights to freedom and privacy and the free development of the personality of individuals.

Single paragraph. The general rules contained in this Law are of national interest and must be observed by the Union, the States, the Federal District and the Municipalities.

Article 2 The regulation of personal data protection is grounded on:

I. respect for privacy;

II. informational self-determination;

III. freedom of expression, information, communication and opinion;

IV. inviolability of intimacy, honor and reputation;

V. economic and technological development and innovation;

VI. free enterprise, free competition and consumer protection; and

VII. human rights, free development of personality, dignity and exercise of citizenship by the individuals.

Article 3 This Law applies to any processing operation carried out by a natural person or legal entity governed by public or private law, regardless of the means, of the country in which its headquarter is located or of the country in which the data are located, provided that:

I. the processing operation be carried out in the Brazilian territory;

II. the purpose of the processing activity be the offer or supply of goods or services or the processing of data of individuals located in the Brazilian territory; or

III. the processed personal data have been collected in the Brazilian territory.

Paragraph 1 Personal data collected in the Brazilian territory are understood as those personal data whose data subject is in the Brazilian territory at the time of the collection.

Paragraph 2 The provision of item I of this article shall not apply to the processing of data set forth in item IV of the head provision of article 4 of this Law.

Article 4 This Law shall not apply to the processing of personal data:

I. made by a natural person for exclusively private and non-economic purposes;

II. made exclusively for:

[1] Unofficial translation by Luca Belli, Laila Lorenzon, Walter B. Gaspar and Luã Fergus.

a) journalistic and artistic purposes; or

b) academic purposes, in which case articles 7 and 11 of this Law shall apply;

III. made exclusively for the following purposes:

c) public security;

d) national defense;

e) safety of the Country; or

f) crime investigation and punishment activities; or

IV. originating from outside the Brazilian territory and which are not subject to communication, shared use of data with Brazilian processing agents or subject to international transfer of data with a country other than the country of origin, provided the country of origin provides a degree of personal data protection consistent with the provisions of this Law.

Paragraph 1 The processing of personal data set forth in item III shall be governed by a specific law, which shall contain proportional measures as strictly required to serve the public interest, subject to due process of law, general principles of protection and the rights of the data subjects set forth in this Law.

Paragraph 2 The processing of the data referred to in item III of the head provision of this article by a person governed by private law is prohibited, except in procedures carried out by a legal entity governed by public law, which shall be the subject matter of specific information to the supervisory authority and which shall observe the limitation imposed in paragraph 4 of this article.

Paragraph 3 The supervisory authority shall issue technical opinions or recommendations relating to the exceptions set forth in item III of the head provision of this article, and it shall request the persons in charge to provide data protection impact assessments.

Paragraph 4 In no event can all personal data of the database set forth in item III of the head provision of this article be processed by a person governed by private law, except for that which has capital entirely owned by the public power.

Article 5 For purposes of this Law, the following definitions apply:

I. personal data: information related to an identified or identifiable natural person;

II. sensitive personal data: personal data on racial or ethnic origin, religious belief, public opinion, affiliation to union or religious, philosophical or political organization, data relating to the health or sex life, genetic or biometric data, whenever related to a natural person;

III. anonymized data: data relating to a data subject who cannot be identified, considering the use of reasonable technical measures available at the time of its processing;

IV. database: structured set of personal data, established in one or several sites, in electronic or physical support;

V. data subject: natural person to whom the personal data being processed refers;

VI. controller: natural person or legal entity, governed by public or private law, in charge of making decisions about the processing of personal data;

VII. processor: natural person or legal entity, governed by public or private law, which processes personal data in the name of the controller;

VIII. data protection officer[2]: natural person appointed by the controller, who acts as a channel of communication between the controller and the data subjects and the supervisory authority, Autoridade Nacional de Proteção de Dados (ANPD);

IX. processing agents: the controller and the processor;

X. processing[3]: any operation carried out with personal data, such as those that refer to the collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, information evaluation or control, modification, communication, transfer, diffusion or extraction;

XI. anonymization: use of reasonable technical means available at the time of processing, by means of which the data loses the possibility of direct or indirect association to a natural person;

XII. consent: free, informed and unequivocal pronouncement by means of which the data subject agrees to the processing of their personal data for a specific purpose;

XIII. blocking: temporary suspension of any processing operation, by means of safekeeping of the personal data or database;

XIV. elimination: exclusion of data or of a group of data stored in a database, regardless of the procedure used;

XV. international transfer of data: transfer of personal data to a foreign country or international organism of which the country is a member;

XVI. shared use of data: communication, diffusion, international transfer, interconnection of personal data or shared processing of personal databases by public bodies and entities in the performance of their statutory duties, or between them and private entities, reciprocally, with specific authorization, for one or more processing modalities permitted by these public entities, or between private entities;

XVII. data protection impact assessment: documentation of the controller that contains a description of the personal data processing activities that could generate risks to civil liberties and to fundamental rights, as well as measures, safeguards and mechanisms to mitigate risks;

XVIII. research body: body or entity of the direct or indirect public administration

or not-for-profit legal entity governed by private law organized under the Brazilian laws, with its headquarters in Brazil, that includes basic or applied research of a historical, scientific, technological or statistical character in its institutional mission or bylaws;

XIX. supervisory authority: body of the indirect public administration in charge of supervising, implementing and inspecting compliance with this Law in all Brazilian territory.

Article 6 The personal data processing activities shall observe fairness and the following principles:

I. purpose: processing for legitimate, specific and explicit purposes informed to the data subject, without any possibility of subsequent processing inconsistently with these purposes;

II. adequacy: compatibility of the processing with the purposes informed to the data subject, in accordance with the context of the processing;

2 The literal translation of the term in Portuguese “Encarregado” would be “person in charge”. However, as the role of “Encarregado” is analogous, albeit not entirely equal, to the “Data Protection Officer”, we have decided to use the latter for the sake of facilitating comprehension.

3 This term can be understood as a translation or analogy of the term “treatment”.

III. necessity: limitation of the processing to the minimum required for the intended purposes, encompassing pertinent, proportional and non-excessive data in relation to the purposes of the data processing;

IV. free access: guarantee, to the data subjects, of facilitated and free consultation on the form and duration of the processing, as well as on all their personal data;

V. quality of data: guarantee, to the data subjects, of accuracy, clarity, relevance and that the data is up to date, according to the need and for compliance with the purpose of the processing thereof;

VI. transparency: guarantee, to the data subjects, of clear, accurate and easily accessible information on the processing and the respective processing agents, subject to business and industrial secrets;

VII. security: use of technical and administrative measures able to protect personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication or diffusion;

VIII. prevention: adoption of measures to prevent the occurrence of damage in view of the processing of personal data;

IX. non-discrimination: impossibility of processing data for discriminatory, unlawful or abusive purposes;

X. responsibility and accountability: proof, by the agent, of adoption of effective measures able to prove observance of and compliance with the personal data protection rules, and also of the effectiveness of these measures.

CHAPTER II
PROCESSING OF PERSONAL DATA

Section I

Requirements for the Processing of Personal Data

Article 7 Personal data can only be processed in the following events: I. with the data subject's consent;

II. for compliance with a statutory or regulatory obligation by the controller;

III. by the public administration, for the processing and shared use of data required for the performance of public policies set forth in laws or regulations or pursuant to contracts, agreements or similar instruments, subject to the provisions of Chapter IV of this Law;

IV. for the conduction of studies by research bodies, guaranteeing, whenever possible, the anonymization of personal data;

V. whenever necessary for the performance of agreements or preliminary procedures relating to agreements to which the data subject is a party, at the request of the data subject;

VI. for the regular exercise of rights in lawsuits, administrative or arbitration proceedings, the latter pursuant to the provisions of Law 9.307, of September 23, 1996 (Arbitration Law);

VII. for protection of the life or physical safety of the data subject or of third parties;

VIII. for the protection of health, exclusively, in a procedure performed by health professionals, health services or health authorities;

IX. whenever necessary to serve the legitimate interests of the controller or of third parties, except in the event of prevalence of fundamental rights and liberties of the data subject, which require protection of the personal data; or

X. for the protection of credit, including with respect to the provisions of the applicable law.

Paragraph 1 (Repealed)

Paragraph 2 (Repealed)

Paragraph 3 The processing of publicly accessible personal data the access to which is public shall consider the purpose, fairness and justified its publication.

Paragraph 4 The requirement of consent set forth in the head provision[4] of this article is waived for data manifestly made public by the data subject, provided the rights of the data subject and the principles set forth in this Law are observed.

Paragraph 5 The controller that has obtained the consent referred to in item I of the head provision of this article and who needs to communicate or share personal data with other controllers must obtain the specific consent of the data subject for such purpose, except where consent is waived according to this Law.

Paragraph 6 No waiver of the requirement of consent releases the processing agents from the other obligations set forth in this Law, especially observance of the general principles and of the guarantee of the rights of the data subject.

Paragraph 7 The subsequent processing of personal data referred to in Paragraph 3 and 4 of this article may be carried out for new purposes, provided that the legitimate and specific purposes for the new treatment and the preservation of the rights of the data subject are observed, as well as the grounds and principles foreseen in this Law.

Article 8 The consent set forth in item I of article 7 of this Law must be provided in writing or by other means that proves the manifestation of will of the data subject.

Paragraph 1 In case the consent is provided in writing, it shall be included in a clause separated from the other contractual clauses.

Paragraph 2 The controller has the burden to prove that the consent has been obtained in accordance with the provisions of this Law.

Paragraph 3 The processing of personal data by means of defective consent is prohibited.

Paragraph 4 Consent shall refer to defined purposes, and generic authorizations for the processing of personal data shall be null.

Paragraph 5Consent may be revoked at any time upon express pronouncement of the data subject, by a free and facilitated procedure, ratifying the processing carried out under a previous consent, as long as there is no request for elimination, pursuant to the provisions of item VI of the head provision of article 18 of this Law.

Paragraph 6 In the event of change in the information referred to in items I, II, III or V of article 9 of this Law, the controller shall inform the data subjects, specifically noting the contents of the change

4 Actually, the requirement is set forth in the item I of the Article 7.

and, whenever the consent of the data subjects is required, it may be revoked by the data subjects if they disagree with the change.

Article 9 The data subjects are entitled to facilitated access to the information on the processing of their data, which shall be clearly, adequately and visibly provided, about the following, in addition to other characteristics set forth in the regulations, for compliance with the principle of free access:

I. – specific purpose of the processing;

II. – form and duration of the processing, observing business and industrial

secrets;

III. – identification of the controller;

IV. – contact information of the controller;

V. - information about the shared use of data by the controller and its purpose; VI. – responsibilities of the agents who shall carry out the processing; and

VII. - rights of the data subject, explicitly mentioning the rights contained in article 18 of this Law.

Paragraph 1 Whenever the consent is required, it shall be deemed null in case the information provided to the data subject has misleading or abusive content or has not been previously presented in a transparent, clear and unequivocal form.

Paragraph 2 Whenever consent is required, if there are changes in the purpose for processing of personal data that are not compatible with the original consent, the controller shall previously inform the data subjects of the changes of purpose, and the data subjects may revoke the consent in case they disagree with the changes.

Paragraph 3 Whenever processing of personal data is a condition for the supply of a product or service or for the exercise of a right, the data subjects shall be emphatically informed of this fact and of the means by which they may exercise the data subjects' rights listed in article 18 of this Law.

Article 10. The legitimate interest of the controller may only be a reason for the processing of personal data for legitimate purposes, based on concrete situations, which include, without limitation:

I. – support and promotion of activities of the controller; and

II. – protection, in relation to the data subjects, of the regular exercise of their rights or provision of services that benefit them, observing their legitimate expectations and the fundamental rights and liberties, pursuant to the provisions of this Law.

Paragraph 1 Whenever processing is based on the legitimate interest of the controller, only the personal data strictly required for the desired purpose may be processed.

Paragraph 2 The controller shall adopt measures to guarantee the transparency of the processing of data based on his or her legitimate interest.

Paragraph 3 The supervisory authority may request to the controller a data protection impact assessment whenever the grounds of the processing are its legitimate interest, subject to business and industrial secrets.

Section II

Processing of Sensitive Personal Data

Article 11. Sensitive personal data can only be processed in the following circumstances:

I. whenever the data subjects or their legal representative specifically and explicitly consent to such processing, for specific purposes;

II. without the data subjects' consent, whenever they are essential for:

a) compliance with a statutory or regulatory obligation by the controller;

b) shared processing of data required for the enforcement, by the public administration, of public policies set forth in laws or regulations;

c) conducting studies by research bodies, guaranteeing, whenever possible, anonymization of sensitive personal data;

d) regular exercise of rights, including in agreements and in lawsuits, administrative or arbitration proceedings, the latter pursuant to the provisions of Law 9.307, of September 23, 1996 (Arbitration Law);

e) protection of the life or physical safety of the data subjects or of third parties;

f) health protection, exclusively, in a procedure performed by health professionals, health services or health authorities; or

g) guarantee of the prevention of fraud and of the security of data subjects, in the processes of identification and certification of record in electronic systems, observing the rights mentioned in article 9 of this Law and except in the event of prevalence of fundamental rights and liberties of the data subjects that require protection of the personal data.

Paragraph 1 The provisions of this article apply to any processing of personal data that discloses sensitive personal data and which may cause damage to the data subjects, except as otherwise provided in a specific law.

Paragraph 2 In the event of application of the provisions of letters "a" and "b" of item II of the head provision of this article by public entities, said waiver of consent shall be made public, pursuant to the provisions of item I of the head provision of article 23 of this Law.

Paragraph 3 The communication or shared use of sensitive personal data among controllers for the purpose of obtaining economic benefit may be prohibited or regulated by the supervisory authority, after consultation with the sectorial Government bodies, within the scope of their duties.

Paragraph 4 Communication or shared use between health-related personal data controllers is prohibited for the purpose of obtaining economic advantage, except in the case of the provision of health services, pharmaceutical and health care, provided paragraph 5 of this article, including ancillary diagnostic and therapy services, for the benefit of the data subjects' interests and to enable:

I. - data portability when requested by the data subject; or

II. - the financial and administrative transactions resulting from the use and provision of the services referred to in this paragraph.

Paragraph 5 The operators of private health care plans are forbidden to process health data for the practice of risk selection in hiring of any kind, as well as in hiring and excluding beneficiaries.

Article 12. Anonymized data shall not be deemed personal data for the purposes of this Law, except when the anonymization process to which they have been submitted is reversed using solely the one's own efforts, or whenever it can be reversed with reasonable efforts.

Paragraph 1 The determination of what is reasonable shall take objective factors into consideration, such as the cost and time required to reverse the anonymization process, in accordance with the available technologies, and the exclusive use of one's own means.

Paragraph 2 For the purposes of this Law, the data used in building a behavioral profile of a given natural person, if identified, may also be deemed personal data.

Paragraph 3 The supervisory authority may determine on standards and techniques used in anonymization processes and make verifications about the security thereof, after consultation with the Brazilian Personal Data Protection Board.

Article 13. In the conduction of studies on public health, research bodies may have access to personal databases, which shall be exclusively processed within those bodies and for the sole purpose of conducting studies and researches, and they must always be kept in a controlled and safe environment, according to the security practices set forth in the specific regulations, including, whenever possible, the anonymization or pseudonymization of the data, and considering the due ethical standards relating to studies and researches.

Paragraph 1 The disclosure of the results or of any excerpt of the study or of the research set forth in the head provision of this article cannot in any way reveal personal data.

Paragraph 2 The research body shall be responsible for the security of the information set forth in the head provision of this article, and transfer of the data to third parties shall not be in any way permitted.

Paragraph 3 Access to the data set forth in this article shall be regulated by the supervisory authority and by health and sanitary authorities, within the scope of their duties.

Paragraph 4 For the effects of this article, pseudonymization is the processing by means of which data loses the possibility of direct or indirect association to a natural person, except for the use of additional information separately kept by the controller in a controlled and safe environment.

Section III

Processing of Personal Data of Children and Adolescents

Article 14. The processing of personal data of children and adolescents shall be carried out to their best interest, pursuant to the provisions of this article and of the applicable law.

Paragraph 1 The processing of personal data of children shall be carried out with the specific and separate consent of at least one of the parents or the legal guardian.

Paragraph 2 In the processing of data set forth in paragraph 1 of this article, the controllers shall maintain public the information on the types of data collected, the form of use thereof and the procedures for exercise of the rights referred to in article 18 of this Law.

Paragraph 3 Personal data of children may be collected without the consent referred to in paragraph 1 of this article whenever the collection is necessary to contact the parents or the legal guardian, used a single time and without storage, or for their protection, and they cannot be transferred to third parties, under any circumstance, without the consent set forth in paragraph 1 of this article.

Paragraph 4 The controllers shall not subject the participation of the data subjects as set forth in paragraph 1 of this article in games, internet applications or other activities to the provision of personal information in addition to those strictly necessary for the activity.

Paragraph 5 The controller shall use all reasonable efforts to confirm that the consent to which paragraph 1 of this article refers was given by the person responsible for the child, considering the available technologies.

Paragraph 6 Information on the processing of data referred to in this article shall be provided in a clear, simple and accessible manner, considering the physical and motor, perceptive, sensorial, intellectual and mental characteristics of the users, with the use of audiovisual resources whenever appropriate, in order to provide the necessary information to the parents or to the legal guardian, as appropriate for the children's understanding.

Section IV

Termination of the Processing of Personal Data

Article 15. Termination of the processing of personal data shall occur in the following events:

I. – verification that the purpose was reached or that the data are no longer necessary or pertinent to attain the specific purpose sought;

II. – lapse of the processing period;

III. - communication by the data subject, including in the exercise of their right to revoke the consent as set forth in paragraph 5 of article 8 of this Law, observing public interest; or

IV. – by order of the supervisory authority, in the event of breach of the provisions of this Law.

Article 16. Personal data shall be eliminated after termination of the processing thereof, within the scope and technical limits of the activities, and conservation thereof shall be authorized for the following purposes:

I. - compliance with a statutory or regulatory obligation by the controller;

II. – studies by a research body, guaranteeing, whenever possible, the anonymization of personal data;

III. - transfer to third parties, upon compliance with the data processing requirements set forth in this Law; or

IV. – exclusive use of the controller, provided the data are anonymized, it being understood that the access thereto by third parties is prohibited.

CHAPTER III
RIGHTS OF THE DATA SUBJECT

Article 17. All natural people are ensured the ownership of their personal data and the guarantee of the fundamental rights to freedom, intimacy and privacy, pursuant to the provisions of this Law.

Article 18. The data subjects are entitled to obtain from the controller, in relation to the data of the data subjects processed by such controller, at any time and upon request:

I. - confirmation of the existence of processing; II. - access to the data;

III. – correction of incomplete, inaccurate or outdated data;

IV. - anonymization, blocking or elimination of unnecessary or excessive data or of data processed in noncompliance with the provisions of this Law;

V. - portability of data to another service or product provider upon express request, in accordance with national authority regulations, regarding commercial and industrial secrets;

VI. - elimination of the personal data processed with the consent of the data subjects, except in the events set forth in article 16 of this Law;

VII. - information of the public and private entities with which the controller carried out the shared use of data;

VIII. - information on the possibility of not providing consent and on the consequences of denial;

IX. – revocation of the consent, pursuant to the provisions of paragraph 5 of article 8 of this Law.

Paragraph 1 The data subject has the right to petition in relation to their data against the controller before the supervisory authority.

Paragraph 2 The data subjects may oppose the processing carried out based on one of the events of waiver of consent, in the event of noncompliance with the provisions of this Law.

Paragraph 3 The rights set forth in this article shall be exercised at the express request of the data subjects or of legally appointed representatives, to a processing agent.

Paragraph 4 In case it is impossible to immediately adopt the measure set forth in paragraph 3 of this article, the controller shall send to the data subjects an answer in which he or she may:

I. – communicate that he or she is not the data processing agent and inform, whenever possible, who is the agent; or

II. – inform the reasons of fact or of law that prevent immediate adoption of the measure.

Paragraph 5 The request referred to in paragraph 3 of this article shall be met free of charge to the data subjects, within the terms and in accordance with the provisions set forth in the regulations.

Paragraph 6 inform the processing agents which whom he or she has shared the use of data of the correction, elimination, anonymization or blocking of the data, for them to repeat an identical procedure, except in cases where such communication is proven impossible or involves disproportionate effort.

Paragraph 7 The portability of the personal data to which item V of the head provision of this article refers does not include data that has already been anonymized by the controller.

Paragraph 8 The right to which paragraph 1 of this article may also be exercised before the consumer defense bodies.

Article 19. Confirmation of the existence of or access to personal data shall be provided, at the request of the data subjects:

I. – immediately, in simplified form; or

II. - by means of a clear and complete statement indicating the origin of the data, the inexistence of registration, the criteria used and the purpose of the processing, observing the business and industrial secrets, provided within up to fifteen (15) days as from the date of request of the data subject.

Paragraph 1 Personal data shall be stored in a format that favors the exercise of the right to access.

Paragraph 2 The information and data may be provided, at the discretion of the data subjects:

I. - by safe electronic means appropriate for this purpose; II. - in printed form.

Paragraph 3 Whenever the processing originates from the consent of the data subjects or from an agreement, the data subjects may request full electronic copies of their personal data, observing the business and industrial secrets, pursuant to the provision of the regulations of the supervisory authority, in a format that permits the subsequent use thereof, including in other processing operations.

Paragraph 4 The supervisory authority may provide distinct provisions on the terms set forth in items I and II of the head provision of this article for the specific sectors.

Article 20. Data subjects are entitled to request a review, of decisions made only based on the automatized processing of personal data that affects their interests, including of decisions designed to define their personal, consumption and credit profile or the aspects of their personality.

Paragraph 1 The controller shall provide, upon request, clear and adequate information on the criteria and procedures used for the automatized decision, observing business and industrial secrets.

Paragraph 2 In the event of failure to offer the information set forth in paragraph 1 of this article based on business and industrial secrets, the supervisory authority may conduct an audit to confirm discriminatory aspects in the automatized processing of personal data.

Paragraph 3 (Vetoed)

Article 21. Personal data relating to the regular exercise of rights by the data subjects cannot be used against them.

Article 22. The defense of the interests and rights of the data subject may be exercised in court, individually or collectively, in the form of the provisions of the applicable law, regarding the instruments of individual and collective protection.

CHAPTER IV
PROCESSING OF PERSONAL DATA BY PUBLIC AUTHORITIES

Section I

Rules

Article 23. The processing of personal data by the legal entities governed by public law mentioned in the sole paragraph of article 1 of Law 12.527, of November 18, 2011 (Access to Information Law) shall be carried out to achieve its public purpose, in the pursuit of the public interest, for the purpose of performing the legal attributions or duties of the public service, provided:

I. – they inform the grounds on which, in accordance with their legal attributions, they process personal data, providing clear and updated information on the statutory provision, the purpose, the procedures and the practices used to perform these activities, in vehicles of easy access, preferably on their electronic websites;

II. (Vetoed)

III. - a data protection officer be appointed whenever the processing of personal data is carried out, pursuant to the provisions of article 39 of this Law; and

IV. (Vetoed)

Paragraph 1 The supervisory authority may provide on the forms of publicity of the processing operations.

Paragraph 2 The provisions of this Law do not exempt the legal entities mentioned in the head provision of this article from instituting the authorities set forth in Law 12.527, of November 18, 2011 (Access to Information Law).

Paragraph 3 The terms and procedures to exercise the data subjects' rights before the Government shall observe the provisions of specific law, especially the provisions of Law 9.507, of November 12, 1997 (*Habeas Data* Law*),* of Law

9.784, of January 29, 1999 (General Law on Administrative Proceedings), and of Law 12.527, of November 18, 2011 (Access to Information Law).

Paragraph 4 The notary office and registration services privately exercised, by delegation of the Government, shall be granted the same treatment granted to the legal entities referred to in the head provision of this article, pursuant to the provisions of this Law.

Paragraph 5 The notary office and registration bodies shall grant access to the data by electronic means to the public administration, in view of the purposes set forth in the head provision of this article.

Article 24. The state-owned companies and the government-controlled private companies that act by means of competitive bid, subject to the provisions of article 173 of the Brazilian Federal Constitution, shall be granted the same treatment granted to the legal entities governed by private law, pursuant to the provisions of this Law.

Sole paragraph. Whenever state-owned companies and government-controlled private companies are operationalizing public policies and within the scope of execution thereof, they shall be granted the same treatment granted to the Government bodies and entities, pursuant to the provisions of this Chapter.

Article 25. The data shall be kept in an interoperable and structured manner for the shared use, aiming at the execution of public policies, the provision of public services, the decentralization of public activities and the dissemination and access to information by the general public.

Article 26. The shared use of personal data by the Government shall meet specific purposes of execution of public policies and legal attribution by the public bodies and entities, subject to the principles of protection of personal data listed in article 6 of this Law.

Paragraph 1 The Government may not transfer to private entities personal data included in databases to which it has access, except:

I. – in cases of decentralized performance of public activity that requires the transfer, exclusively for this specific and determined purpose, subject to the provisions of Law 12.527, of November 18, 2011 (Access to Information Law);

II. (Vetoed)

III. – whenever the data are publicly accessible, subject to the provisions of this Law.

IV. – when there is a legal provision, or the transfer is based on contracts, conventions or similar instruments; or

V. – in the event that the transfer of data is solely intended to prevent fraud and irregularities, or to protect and safeguard the security and integrity of the data subject, provided that processing for other purposes is prohibited. VI. (Vetoed)

Paragraph 2 The contracts and agreements set forth in Paragraph 1 of this article shall be informed to the supervisory authority.

Article 27. The communication or shared use of personal data of legal entities governed by public law to legal entities governed by private law will be informed to the national supervisory authority and will depend on the consent of the data subjects, except:

I. – in the events of waiver of consent set forth in this Law;

II. – in the events of shared use of data, which shall be granted publicity pursuant to the provisions of item I of the head provision of article 23 of this Law; or

III. – in the exceptions set forth in paragraph 1 of article 26 of this Law.

Single paragraph: Information to the national authority referred to in the head of this article shall be regulated.

Article 28. (Vetoed)

Article 29. The supervisory authority may request, at any time, to the Government entities, the conduction of personal data processing operations, specific information on the scope and nature of the data and other details of the processing carried out, and it may issue a supplementary technical report to guarantee compliance with this Law.

Article 30. The supervisory authority may establish supplementary rules for the communication activities and shared use of personal data.

Section II

Responsibilities

Article 31. In the event of breach of this Law as a result of the processing of personal data by public bodies, the supervisory authority may send a communication with applicable measures to cease the violation.

Article 32. The supervisory authority may request Government agents the publication of personal data protection impact assessment and suggest the adoption of standards and good practices for the processing of personal data by the Government.

CHAPTER V
INTERNATIONAL TRANSFER OF DATA

Article 33. The international transfer of personal data is permitted solely in the following cases:

I. – to countries or international organizations that provide the appropriate level of protection of personal data provided for by this Law;

II. – where the controller provides and demonstrates guarantees of compliance with the principles, rights of the data subject and data protection regime established in this Law, in the form of:

a) specific contractual sections for a given transfer;

b) standard contractual sections;

c) global corporate rules;

d) seals, certificates and codes of conduct regularly issued;

III. – where the transfer is required for international legal cooperation between government intelligence, investigation and police bodies, in accordance with international law instruments;

IV. - where the transfer is required for life protection or physical integrity of the data subject or any third party;

V. – where the supervisory authority authorizes such transfer;

VI. – where the transfer results in a commitment undertaken under an international cooperation agreement;

VII. – where the transfer is required for enforcement of a public policy or legal attribution of the public utility, upon disclosure of the provisions of item I of the head provision of article 23 of this Law;

VIII. – where the data subject has provided specific and highlighted consent for such transfer, with previous information on the international nature of the operation, clearly distinguishing it from any other purposes; or

IX. – where required to meet the hypotheses established in items II, V and VI of article 7 of this Law.

Sole paragraph. For purposes of item I of this article, the legal entities of public law referred to in the sole paragraph of article 1 of Law 12.527 of November 18, 2011 (Access to Information Law), within the scope of their legal powers, and in charge, within the scope of their activities, may request to the supervisory authority the assessment of the level of protection to personal data granted by the international country or organization.

Article 34. The level of data protection of the foreign country or international organization mentioned in item I of the head provision of article 33 of this Law shall be assessed by the supervisory authority, which shall take into account:

I. – the general and sectorial rules of the applicable law in the country of destination or international organization;

II. – the nature of the data;

III. –compliance with the general principles of protection of personal data and rights of the data subjects established in this Law;

IV. –adoption of security measures provided for by regulations;

V. –existence of legal and institutional guarantees for compliance with personal data protection rights; and

VI. – any other specific circumstances concerning the transfer.

Article 35. The definition of the content of standard contractual sections, and the verification of specific contractual sections for a given transfer, global corporate rules, or seals, certificates and codes of conduct referred to in item II of the head provision of article 33 of this Law shall be carried out by the supervisory authority.

Paragraph 1 For verification of the provisions in the head of this article, the minimum requirements, conditions and guarantees for transfer that comply with the rights, guarantees and principles of this Law shall be taken into account.

Paragraph 2 In the analysis of contractual sections, documents or global corporate rules submitted to the supervisory authority for approval, additional information may be requested or procedures of verification of the processing operations may be carried out, as required.

Paragraph 3 The supervisory authority may designate certification organizations to carry out the provisions of the head provision of this article, which shall be subject to its inspection as defined in regulations.

Paragraph 4 The acts performed by any certification organization may be reviewed by the supervisory authority and, in case they are not in compliance with this Law, shall be revised or annulled.

Paragraph 5 Sufficient guarantees of compliance with the general principles of protection and with the data subject's rights referred to in the head provision of this article shall be also analyzed in accordance with the technical and organizational measures adopted by the processor, as provided for in paragraphs 1 and 2 of article 46 of this Law.

Article 36. Any changes in the guarantees presented as being sufficient guarantees of compliance with the general principles of protection and with the data subjects' rights referred to in item II of article 33 of this Law shall be communicated to the supervisory authority.

CHAPTER VI
PERSONAL DATA PROCESSING AGENTS

Section I

Controller and Processor

Article 37. The controller and the processor shall keep in record the personal data processing operations carried out by them, especially where they are based on a legitimate interest.

Article 38. The supervisory authority may require the controller to prepare a data protection impact assessment, including sensitive data relating to its data processing operations, as provided for by the regulations, with due regard for trade and industrial secrets.

Sole paragraph. With due regard for the provisions in the head provision of this article, the report shall contain at least a description of the types of data collected, the methodology used for collection and security measures adopted, and an analysis of the controller in relation to the measures, safeguards and risk mitigation mechanisms adopted.

Article 39. The processor shall carry out the processing in accordance with the instructions supplied by the controller, which shall determine the compliance with its own instructions and the rules on the matter.

Article 40. The supervisory authority may establish interoperability standards for purposes of portability, free access to data and security, and on the retention time of the registrations, especially in view of the need and transparency.

Section II

Data Protection Officer

Article 41. The controller shall indicate a data protection officer.

Paragraph 1 The identity and contact data of the data protection officer shall be publicly, clearly and objectively disclosed, preferably on the controllers' website.

Paragraph 2 The activities of the data protection officer consist of the following:

I. – to accept complaints and communications from data subjects, provide clarifications and take appropriate measures;

II. – to receive communications from the supervisory authority and take appropriate measures;

III. – to instruct the employees and contractors of the entity on the practices to be adopted in relation to personal data protection; and

IV. – to carry out any other duties established by the controller or in supplementary rules.

Paragraph 3 The supervisory authority may establish supplementary rules on the definition and duties of the data protection officer, including the cases in which there is no need for appointing such data protection officer, in accordance with the nature and size of the entity or the volume of data processing operations. Paragraph 4 (Vetoed)

Section III

Liability and Compensation

Article 42. Any controller or processor that, in connection with the performance of the activity of personal data processing, causes any property, moral, individual or collective damage to any third party, in violation of the personal data protection law, shall be required to indemnify it.

Paragraph 1 In order to ensure effective indemnity to the data subject:

I. – the processor shall be jointly and severally liable for any damages caused by the processing if the processor fails to comply with the obligations of the data protection law or fails to follow the lawful instructions of the controller, in which case the processor shall be equivalent to the controller, except in the events of exclusion established in article 43 of this Law;

II. – any controllers that are directly involved in the processing which resulted in damages to the data subject shall be jointly and severally liable, except in the events of exclusion established in article 43 of this Law.

Paragraph 2 The judge, in a civil proceeding, may reverse the burden of proof in favor of the data subject whenever, in the judge's opinion, the allegation is likely, the data subject is unable to produce evidences, or the production of evidence by the data subject would be exclusively burdensome for such data subject.

Paragraph 3 Actions for indemnification of collective damages as provided for in the head provision of this article, may be collectively conducted in court, with due regard for the provisions of the applicable law.

Paragraph 4 Anyone who compensates for damage to the data subject shall have a right of recourse against the other liable parties, to the extent of their participation in the harmful event.

Article 43. The processing agents shall not be held liable only if they demonstrate:

I. – that they did not carry out the personal data processing attributed to them;

II. – that, although they carried out the personal data processing attributed to them, there was no violation of the data protection law; or

III. – that the damage results from exclusive fault of the data subject or any third party.

Article 44. The personal data processing shall be irregular if it fails to comply with the law or fails to provide the security that the data subject may expect therefrom, considering the relevant circumstances, including:

I. – the way it is performed;

II. – the result and the risks that are reasonably expected from it;

III. – the personal data processing techniques available at the time it was carried out.

Sole paragraph. Any controller or processor that causes the damage by failing to take the security measures established in article 46 of this Law shall be liable for the damages arising out of the data security violation.

Article 45. The events of violation of the data subjects' right within the scope of the consumer relationships remain subject to the liability rules established in the applicable law.

CHAPTER VII
SECURITY AND BEST PRACTICES

Section I

Data Security and Confidentiality

Article 46. The processing agents shall adopt security, technical and administrative measures that are capable of protecting personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, modification, communication or any form of inappropriate or unlawful processing.

Paragraph 1 The supervisory authority may provide for the minimum technical standards to make the provisions in the head of this article applicable, considering the nature of the treated information, the specific characteristics of the processing, and the current state of technology, especially in case of sensitive personal data, as well as the principles established in the head provision of article 6 of this Law.

Paragraph 2 The measures referred to in the head of this article shall be complied with from the product or service design phase to its implementation.

Article 47. The processing agents or any other person that interferes with any of the processing phases shall be required to ensure the information security provided for by this Law in relation to personal data, including after its termination.

Article 48. The controller shall notify the supervisory authority and the data subject of the occurrence of any security incident that may result in any relevant risk or damage to the data subjects.

Paragraph 1 Such notice shall be delivered within a reasonable term, as defined by the supervisory authority, and contain at least:

I. – a description of the nature of the affected personal data;

II. – information on the data subjects involved;

III. – indication of the technical and security measures used for data protection, with due regard for trade and industrial secrets;

IV. – the risks relating to the incident;

V. – the reasons for the delay, in case the notice is not immediate; and

VI. – the measures that were or shall be adopted to reverse or mitigate the effects of the loss.

Paragraph 2 The supervisory authority shall determine the severity of the incident and, if required for safeguarding the data subjects right, may order the controller to take measures such as:

I. – broad disclosure of the fact in media outlets; and

II. – measures to reverse or mitigate the effects of the incident.

Paragraph 3 In the determination of the severity of the incident, it shall be assessed whether appropriate technical measures were adopted to make the affected personal data unintelligible, within the scope and the technical limits of its services, to third parties not authorized to access them.

Article 49. The systems used for personal data processing shall be structured in such a manner as to meet the security requirements, good practices and governance standards, and the general principles established in this Law and in any other regulatory rules.

Section II

Good Practices and Governance

Article 50. The controllers and processors, within the scope of their authority for personal data processing, individually or by means of associations, may produce good practices and governance rules that provide for organizational factors, working practices, procedures, including complaints and petitions of data subjects, security rules, technical standards, specific obligations for the different parties involved in the processing, educative actions, internal mechanisms of supervision and risk mitigation, and any other aspects relating to personal data processing.

Paragraph 1 When establishing good practices rules, the controller and the processor shall take into account, in relation to the processing and the data, the nature, scope, purpose and likelihood and severity of the risks and benefits arising out of the data subjects' data processing.

Paragraph 2 In the application of the principles indicated in items VII and VIII of the head provision of article 6 of this Law, the controller, with due regard for the structure, level and volume of its operations, and the sensitivity of the treated data and the likelihood and severity of the damages to the data subjects', may:

I. – implement a privacy governance program that shall at least:

a) demonstrate the controller's commitment to adopt internal processes and policies that ensure broad compliance with rules and good practices concerning personal data protection;

b) be applicable to any set of personal data under its control, regardless of how it was collected;

c) be adapted to the structure, level and volume of its operations, and to the sensitivity of the treated data;

d) establish appropriate policies and safeguards based on a process of systematic assessment of impacts on and risks to the privacy;

e) intend to establish a trust relationship with the data subject, by means of transparent actions that ensure mechanisms of participation of the data subject;

f) be integrated to its general governance structure and establish and apply internal and external supervision mechanisms;

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

g) have an incident response and remediation plan; and

h) be constantly updated based on information obtained from continuous monitoring and periodic assessments;

II. - demonstrate the effectiveness of its privacy governance program when appropriate, especially at the request of the supervisory authority or any other entity in charge of promoting compliance with good practices or codes of conduct, which independently promote compliance with this Law.

Paragraph 3 The good practices and governance rules shall be published and updated from time to time and may be acknowledged and disclosed by the supervisory authority.

Article 51. The supervisory authority shall encourage the adoption of technical standards for easier control by the data subjects of their personal data.

CHAPTER VIII INSPECTION

Section I

Administrative Sanctions

Article 52. The data processing agents, in connection with any infractions of the rules established in this Law, shall be subject to the following administrative penalties applicable by the supervisory authority:

I. – warning, with indication of a term for adoption of corrective measures;

II. - simple fine of up to two percent (2%) of the sales revenue of the legal entity of private law, group or conglomerate in Brazil in its last fiscal year, excluding taxes, limited, in the aggregate, to fifty million Reais (R$50,000,000.00) per infraction;

III. – daily fine, with due regard for the total limit referred to in item II;

IV. – disclosure of the infraction after it has been duly investigated and its occurrence has been confirmed;

V. – blockage of the personal data to which the infraction relates, until regularization thereof;

VI. – elimination of the personal data to which the infraction relates; VII. - (Vetoed);

VIII. - (Vetoed);

IX. - (Vetoed);

X. - partial suspension of the operation of the database to which the infringement refers for a maximum period of six (6) months, extendable for an equal period, until the controller has regularized its processing activity;

XI. - suspension of the exercise of the activity of processing personal data to which the infringement refers for a maximum period of six (6) months, extendable for the same period;

XII. partial or total ban on data processing activities.

Paragraph 1 The penalties shall be imposed after an administrative proceeding that provides the chance of broad defense, on a gradual, individual or cumulative basis, in accordance with the peculiarities of the relevant case and considering the following parameters and criteria:

I. - the severity and nature of the infractions and the personal rights affected; II. – the good faith of the infractor;

III. – the advantage obtained or intended by the infractor;

IV. – the infractor's economic condition;

V. –recidivism;

VI. – the level of damage;

VII. – cooperation by the infractor;

VIII. – repeated and demonstrated adoption of internal mechanisms and procedures that are capable of minimizing the damage, intended for secure and appropriate data processing, in accordance with the provisions in item II of paragraph 2 of article 48 of this Law;

IX. – the adoption of good practices and governance policy;

X. – the immediate adoption of corrective measures; and

XI. – the proportionality between the severity of the fault and the intensity of the penalty.

Paragraph 2The provisions of this article do not replace the application of administrative, civil or criminal sanctions defined in Law 8.078 of September 11, 1990, and in specific legislation.

Paragraph 3 The provisions of items I, IV, V, VI, X, XI and XII of the head of this article may be applied to public entities and public bodies, without prejudice to the provisions of Law 8.112, of December 11, 1990, Law 8.429, of June 2, 1992, and in Law 12.527, of November 18, 2011.

Paragraph 4 When calculating the amount of the fine referred to in item II of the head provision of this article, the supervisory authority may consider the total sales revenue of the company or group of companies, whenever it does not have the amount of the sales revenue in the business field in which the infraction occurred, as defined by the supervisory authority, or when the amount is presented in an incomplete manner and/or not demonstrated in an unequivocal and suitable manner.

Paragraph 5 The financial gains from the collection of fines imposed by the ANPD, whether posted or not in the Federal Debt Roster, will be destined to the Diffuse Rights Defense Fund dealt with in art. 13 of Law 7.347 of July 24, 1985, and Law

9.008 of March 21, 1995.

Paragraph 6 The sanctions provided for in items X, XI and XII of the head of this article shall apply:

I. only after at least one (1) of the sanctions referred to in items II, III, IV, V and VI of the head of this article have already been imposed for the same specific case; and

II. in the case of controllers subordinated to other organs and entities with sanctioning powers, after hearing these organs.

Paragraph 7 The individual leaks or unauthorized access referred to in the head of art. 46 of this Law may be subject to direct conciliation between controller and data subject and, if there is no agreement, the controller shall be subject to the application of the penalties referred to in this article.

Article 53. The supervisory authority shall define, by means of proper regulations on administrative penalties for infractions to this Law, which shall be the subject-matter of public inquiry, the methodologies that shall guide the calculation of the base amount of the penalties of fine.

Paragraph 1 The methodologies referred to in the head provision of this article shall be previously published, for information of the processing agents, and objectively present the forms and dosimetry for calculation of the base amount of fines, which shall contain a detailed justification of all elements thereof, demonstrating compliance with the criteria established in this Law.

Paragraph 2 The regulation of penalties and corresponding methodologies shall establish the circumstances and conditions for adoption of simple or daily fines.

Article 54. The amount of the penalty of daily fine applicable to infractions of this Law shall take into account the severity of the fault and the extension of the damage or loss caused and be justified by the supervisory authority.

Sole paragraph. The notice of imposition of daily fine shall contain at least a description of the obligation imposed, the reasonable term established by the body for compliance therewith, and the amount of the daily fine to be imposed for breach thereof.

CHAPTER IX
THE NATIONAL SUPERVISORY AUTHORITY ("ANPD") AND NATIONAL PERSONAL DATA AND PRIVACY PROTECTION COUNCIL

Section I

Data Protection Supervisory Authority (ANPD)

Article 55. (Vetoed)

Article 55-A. It is hereby created without any increase in expenses, The National Data Protection Authority (ANPD), a federal public administration body that is a member of the Presidency of the Republic. (Included by Law. 13.853 of 2019)

Paragraph 1 The legal nature of the ANPD is transitory and may be transformed by the Executive Power into an entity of indirect federal public administration, subject to special autarchic regime and linked to the Presidency of the Republic.

Paragraph 2 The assessment regarding the transformation provided for in paragraph 1 of this article shall occur within two (2) years from the date of entry into force of the ANPD's regimental structure.

Paragraph 3 The provision of positions and functions necessary for the establishment and performance of the ANPD is subject to express physical and financial authorization in the annual budget law and permission in the budget guidelines law.

Article 55-B. Technical and decision-making autonomy is assured to the ANPD.

Art. 55-C. The ANPD is composed of:

I. - Directing Council, highest governing body;

II. - National Council for the Protection of Personal Data and Privacy;

III. - Internal Affairs Audit;

IV. - Ombudsman;

V. - legal advisory body; and

VI. - administrative units and specialized units necessary for the application of the provisions of this Law.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Art. 55-D. The ANPD Board of Directors will be composed of 5 (five) directors, including the Chief Executive Officer.

Paragraph 1 The members of ANPD's Board of Directors will be chosen by the President of the Republic and appointed by him, after approval by the Federal

Senate, under the terms of sub-paragraph f) of item III of art. 52 of the Federal Constitution and will occupy a position on the committee of the Superior Steering and Advisory Group - DAS, at least level 5.

Paragraph 2 The members of the Board of Directors will be chosen from Brazilians who have an unblemished reputation, a superior level of education and a high level of expertise in the field of specialty of the positions to which they will be appointed.

Paragraph 3 The term of office of the members of the Board of Directors shall be four (4) years.

Paragraph 4 The terms of office of the first members of the Board of Directors chosen shall be 2 (two), 3 (three), 4 (four), 5 (five) and 6 (six) years, as set forth in the appointment.

Paragraph 5 In the event of vacancy in office during the term of office of a member of the Board of Directors, the remaining term shall be completed by the successor.

Art. 55-E. The members of the Board of Directors will only lose their positions as a result of resignation, final court conviction or penalty of dismissal arising from disciplinary administrative proceedings.

Paragraph 1 Pursuant to the head of this article, it is incumbent upon the Minister of State Chief of Staff of the Presidency of the Republic to institute disciplinary administrative proceedings, which shall be conducted by a special commission composed of stable federal public servants.

Paragraph 2 It is for the President of the Republic to determine the preventive removal, only when so recommended by the special commission referred to in paragraph 1 of this article, and to render the judgment.

Art. 55-F. The provisions of art. 6 of Law 12.813, of May 16, 2013, are applicable to the members of the Board of Directors, after the exercise of the position.

Single paragraph Infringement of the head of this article characterizes an act of administrative misconduct.

Art. 55-G. An Act of the President of the Republic shall provide for ANPD's regimental structure.

Paragraph 1 Until the date of entry into force of its regimental structure, ANPD will receive technical and administrative support from the Civil House of the Presidency of the Republic for the exercise of its activities.

Paragraph 2 The Directing Council shall provide for the internal statute of the ANPD.

Art. 55-H. Commission positions and ANPD's trust functions will be relocated from other organs and entities of the federal executive branch.

Art. 55-I. The occupants of ANPD's commission positions and trust functions shall be appointed by the Board of Directors and appointed or designated by the Chief Executive Officer.

Art. 55-J. It is up to the ANPD:

I. –to ensure the protection of personal data, in accordance with the law;

II. –to ensure the observance of commercial and industrial secrets, observing the protection of personal data and confidentiality of information when protected by law or when breach of confidentiality violates the fundaments of art. 2 of this Law;

III. –to develop guidelines for the National Policy on Personal Data Protection and Privacy;

IV. –to supervise and enforce sanctions in case of data processing carried out in breach of the law, through an administrative process that ensures due process, broad defense and the right of appeal;

V. –to consider petitions from data subjects against controllers after the data subject has substantiated a complaint to the controller that is not resolved within the time limit established in the regulation;

VI. –to promote among the population the knowledge of the norms and the public politics on protection of personal data and the security measures;

VII. –to promote and elaborate studies on national and international practices of personal data protection and privacy;

VIII. –to encourage the adoption of standards for services and products that facilitate the exercise of control of the data subjects over their personal data, which should take into account the specificities of the activities and the size of those responsible;

IX. –to promote cooperation actions with personal data protection authorities of other countries, of an international or transnational nature;

X. –to provide for the forms of advertising of personal data processing operations, respecting commercial and industrial secrets;

XI. –to request, at any time, the public authorities to carry out personal data processing operations to provide specific information on the scope, nature of the data and other details of the processing performed, with the possibility of issuing a complementary technical opinion to ensure the compliance with this law;

XII. –to prepare annual management reports on its activities;

XIII. - to edit regulations and procedures on protection of personal data and privacy, as well as on reports of impact to the protection of personal data for cases where the treatment represents high risk to the guarantee of the general principles of protection of personal data foreseen in this Law;

XIV. –to listen to treatment agents and society on matters of relevant interest and report on their activities and planning;

XV. –to collect and apply its income and publish, in the management report referred to in item XII of the head of this article, a breakdown of its income and expenses;

XVI. –to perform audits, or determine their performance, within the scope of the inspection activity dealt with in item IV and with due observance of the provisions of item II of the head of this article, on the processing of personal data by the processing agents, including the public power;

XVII. –to enter into, at any time, a commitment to treatment agents to eliminate irregularity, legal uncertainty or contentious situation in the context of administrative proceedings, in accordance with Decree-Law 4.657 of September 4, 1942;

XVIII. - edit simplified and differentiated rules, guidelines and procedures, including deadlines, so that micro and small businesses, as well as incremental or disruptive business initiatives that call themselves startups or innovation companies, can adapt to this Law;

XIX. –to ensure that the data processing of the elderly is carried out in a simple, clear, accessible and appropriate way to their understanding, pursuant to this Law and Law 10.741, of October 1, 2003 (Statute of the Elderly);

XX. –to decide, at the administrative level, on a terminative basis, on the interpretation of this Law, its powers and omitted cases;

XXI. –to report to the competent authorities the criminal offenses of which it is aware;

XXII. –to report to the internal control organs non-compliance with the provisions of this Law by federal public administration agencies and entities;

XXIII. –to articulate with public regulatory authorities to exercise their powers in specific sectors of economic and governmental activities subject to regulation; and

XXIV. –to implement simplified mechanisms, including by electronic means, for the registration of complaints about the processing of personal data in breach of this Law.

Paragraph 1 When imposing administrative constraints on the processing of personal data by private processing agents, whether limits, charges or obligations, the ANPD must comply with the requirement of minimum intervention, ensuring the grounds, principles and rights of the data subjects provided for in art. 170 of the Federal Constitution and this Law.

Paragraph 2 Regulations and standards issued by the ANPD should be preceded by public consultation and hearing, as well as regulatory impact analysis.

Paragraph 3 The ANPD and the public bodies and entities responsible for the regulation of specific sectors of economic and governmental activity shall coordinate their activities, in the corresponding spheres of activity, in order to ensure the fulfillment of their duties with the greatest efficiency and to promote the proper functioning of regulated sectors, according to specific legislation, and the processing of personal data, pursuant to this Law.

Paragraph 4 The ANPD shall maintain a permanent communication forum, including through technical cooperation, with public administration bodies and entities responsible for the regulation of specific sectors of economic and governmental activity, in order to facilitate the ANPD's regulatory, supervisory and punitive powers.

Paragraph 5 In exercising the powers referred to in the main section of this article, the competent authority shall ensure the preservation of business secrecy and confidentiality of information, in accordance with the Law.

Paragraph 6 Complaints collected in accordance with the provisions of section V of the head of this article may be analyzed in aggregate form, and any measures resulting from them may be adopted in a standardized manner.

Art. 55-K. The application of the sanctions provided for in this Law rests exclusively with the ANPD, and its powers shall prevail, regarding the protection of personal data, over the related competences of other public administration entities or bodies.

Single paragraph The ANPD will articulate its activities with other bodies and entities with sanctioning and normative competences related to the subject of personal data protection and will be the central body for the interpretation of this Law and the establishment of rules and guidelines for its implementation.

Art. 55-L. ANPD's revenues are:

I. - the allocations, set out in the general budget of the Union, special credits, additional credits, transfers and on lendings granted to it;

II. - donations, legacies, grants and other resources intended for it;

III. - the amounts determined on the sale or rental of movable and immovable property owned by it;

IV. - the amounts calculated on investments in the financial market of the revenues provided for in this article;

V. - (Vetoed);

VI. - resources arising from agreements, arrangements or contracts concluded with public or private entities, organizations or companies, national or international;

VII. - the proceeds from the sale of publications, technical material, data and information, including for public bidding purposes.

Article 56. (Vetoed) **Article 57.** (Vetoed)

Section II

National Personal Data and Privacy Protection Council

Article 58. (Vetoed)

Art. 58-A. The National Council for the Protection of Personal Data and Privacy will be composed of 23 (twenty-three) representatives, full and alternates, from the following bodies:

I. - 5 (five) from the Federal Executive Branch;

II. - 1 (one) from the Federal Senate;

III. - 1 (one) from the Chamber of Deputies;

IV. - 1 (one) from the National Council of Justice;

V. - 1 (one) from the National Council of the Public Prosecution Service;

VI. - 1 (one) from the Brazilian Internet Steering Committee;

VII. - 3 (three) from civil society entities related to the protection of personal data;

VIII. - 3 (three) from scientific, technological and innovation institutions;

IX. - 3 (three) from trade union confederations representing the economic categories of the productive sector;

X. - 2 (two) from entities representing the business sector related to the area of personal data processing; and

XI. - 2 (two) from entities representing the labor sector.

Paragraph 1 Representatives shall be appointed by act of the President of the Republic, with delegation permitted.

Paragraph 2 The representatives referred to in items I, II, III, IV, V and VI of the main section of this article and their alternates shall be appointed by the full members of the respective organs and entities of the public administration.

Paragraph 3 The representatives referred to in items VII, VIII, IX, X and XI of the head of this article and their alternates:

I. - will be indicated in the form of a regulation;

II. - may not be members of the Internet Steering Committee in Brazil;

III. - will have a term of office of 2 (two) years, with 1 (one) renewal allowed.

Paragraph 4 Participation in the National Council for the Protection of Personal Data and Privacy shall be considered as relevant, unpaid public service provision.

Art. 58-B. The National Council for the Protection of Personal Data and Privacy is responsible for:

I. - proposing strategic guidelines and providing subsidies for the elaboration of the National Policy of Personal Data Protection and Privacy and for ANPD's performance;

II. - preparing annual reports evaluating the execution of the actions of the

National Policy for the Protection of Personal Data and Privacy;

III. - suggesting actions to be performed by the ANPD;

IV. - preparing studies and holding public debates and hearings on the protection of personal data and privacy; and

V. - disseminating knowledge about the protection of personal data and privacy to the population.

Art. 59. (Vetoed).

CHAPTER X
FINAL AND TRANSITIONAL

PROVISIONS

Article 60. Law 12.965 of April 23, 2014 (Brazilian Civil Rights Framework for the Internet) shall be hereinafter in effect with the following amendments:

“Article 7 .....

X – definite exclusion of the personal data supplied to a given internet application, at its request, upon expiration of the relationship between the parties, except for the cases of mandatory storage of records provided for by this Law and by the law that provides for personal data protection; ……..” (Regulatory Rule)

“Article 16.....

II – of personal data that are excessive in relation to the purpose for which consent was given by the data subject thereof, except for the cases provided for by the Law that provides for personal data protection.” (Regulatory Rule)

Article 61. The foreign company shall be notified and summoned in relation to all procedural acts established in this Law, regardless of power of attorney or contractual or statutory provision, by means of its agent or representative or person in charge of its branch, agency, subsidiary, establishment or office installed in Brazil.

Article 62. The supervisory authority and Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), as part of its duties, shall enact specific regulations for access to data treated by the Federal Government for compliance with the provisions in paragraph 2 of article 9 of Law 9.394 of December 20, 1996 (National Education Bases and Guidelines Law), and the provisions relating to the National Higher Education Evaluation System (Sinaes) referred to by Law 10.861 of April 14, 2004.

Article 63. The supervisory authority shall establish rules for progressive adequacy of databases created by the date of effectiveness of this Law, considering the complexity of the processing operations and the nature of the data.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Article 64. The rights and principles expressed in this Law do not exclude any other rights and principles established in the Brazilian legal system concerning the matter or in the international treaties to which the Federative Republic of Brazil is a party.

Article 65. This Law comes into force:

I. On the 28th of December 2018 for articles 55-A, 55-B, 55-C, 55-D, 55-

E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A and 58-B; and

II. 24 (twenty-four) months after its publication date, as for the other articles.

Brasília, August 14, 2018.

Officially Published, August 15, 2018.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)