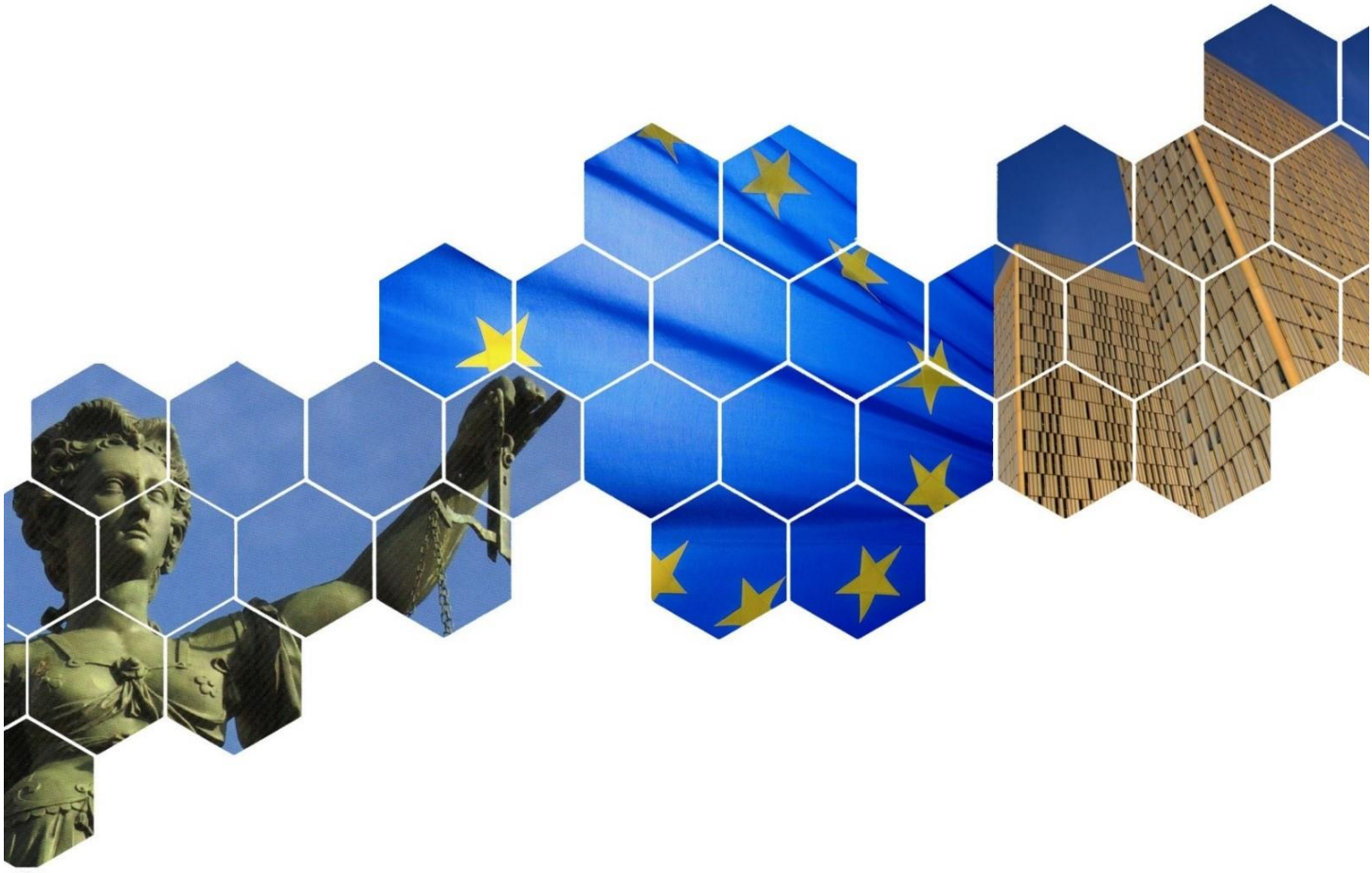
Government access to data in third countries II

Final Report

Specific Contract No. 2022-0716
Implementing the Framework Contract EDPS/2019/02



milieu
Law & Policy Consulting

KU LEUVEN

April 2023

This study has been prepared by Milieu under Contract No 2022-0716 (EDPS/2019/02) for the benefit of the EDPB.

The study has been carried out by researchers from CiTiP, KU Leuven, with the support of Milieu Consulting SRL. The authors of the study are Dr Laura Drechsler, Abdullah Elbi, Elora Fernandes, Eyup Kun, Isabela Maria Rosal, Bilgesu Sumer, and Dr Sofie Royer from CiTiP, KU Leuven.

Milieu Consulting SRL, Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: EDPB.legalstudies@milieu.be; web address: www.milieu.be.

Table of contents

EXECUTIVE SUMMARY

This report provides information on the legislation and practices in Brazil for the situation where personal data are accessed by governmental authorities for reasons of national security or law enforcement (governmental access). This study was based on a literature review via desk research (books, journal articles, databases and other online sources), also including reports of international organisations on the country in question. The legal analysis based on the literature review and the relevant legal documents was complemented by a round of interviews with carefully selected experts with the goal of gaining insights into the practice of the analysed laws. The main findings of this approach for each country are outlined in the following paragraphs.

In Brazil, the fundamental rights to privacy and to the protection of personal data are enshrined in the Constitution and can be exercised by all, including foreigners. The Brazilian General Data Protection Law (LGPD) represented a significant advance towards a more solid protection of personal data, being the result of years of multistakeholder discussions. The LGPD covers both public and private sector activities and has an extremely similar structure to the General Data Protection Regulation (GDPR). It also follows the *ex-ante* protection system and the accountability approach, sets a need for a legal basis for data processing, and establishes a minimum set of principles and data subjects' rights that must be observed in every processing of personal data. The Brazilian Data Protection Authority (ANPD), despite having started its activities only in 2020, already has a solid regulatory and personnel structure and is currently preparing for a more incisive action in concrete cases of rights' violation. Some activities of the State are, however, not in the scope of the LGPD, such as national security, public security, national defence, and criminal prosecution, which affects the level of protection provided in situations of governmental access. For such access, there are some laws and decrees in the Brazilian legal framework, as well as oversight mechanisms, which should enable *a priori* and *a posteriori* control of these activities. However, more comprehensive laws for data protection in these areas are still necessary for a full and solid protection of data subjects' rights in Brazil.

1 INTRODUCTION

1.1 OBJECTIVES AND SCOPE OF THE STUDY

According to Article 46 of the General Data Protection Regulation (GDPR)[1], data controllers and processors may transfer personal data to third countries or international organisations only if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. Whereas it is the primary responsibility of data exporters and data importers to assess that the legislation of the country of destination enables the data importer to comply with any of the appropriate safeguards, supervisory authorities (SAs) play a key role when issuing further decisions on transfers to third countries. Hence, this report provides the European Data Protection Board (EDPB) and the SAs in the EEA/EU with information on the legislation and practice in Brazil on its government's access to personal data processed by economic operators. The report contains an overview of the relevant information in order for the SAs to assess whether and to what extent legislation and practices in Brazil imply massive and/or indiscriminate access to personal data processed by economic operators.

In order to answer the research questions, the study has

- investigated the general situation of Brazil with regard to the protection of fundamental rights and freedoms, by analysing international reports and findings from public bodies (e.g. Council of Europe, UN Human Rights Council and Human Rights Committee) and renowned non-governmental bodies (e.g. Amnesty International, Human Rights Watch, Privacy International). To this end, the study also identified the country's international commitments in the field of human rights, in particular of the right to privacy and data protection;
- analysed the legislation of Brazil in order to establish the substantive and procedural conditions for government access to personal data, including law enforcement and intelligence agencies. Specific attention was paid to the authorities involved in the adoption or amendment of the related rules, and entitled to authorise the governmental access to personal information;
- investigated whether specific purposes and conditions to access personal data of foreign individuals exist;
- identified, where existing, oversight mechanisms with regard to the governmental access to personal data, and to assess the independency from the executive of the bodies empowered to perform such control; and
- focused on rights and administrative or judicial redress mechanisms that are available to data subjects (including foreign individuals).

The study is not limited to an up-to-date overview of relevant legislation and case law, but also contains information with regard to the implementation of the legislation in practice, which has mostly been collected through interviews.

1.2 LEGAL BACKGROUND

This section gives an overview of the legal framework for assessing governmental access to personal data in a third country from the perspective of EU law, where such an assessment is required in the context of international personal data transfers under the GDPR[2]. The main legal instruments considered are the EU-Charter of Fundamental Rights of the EU (EU-Charter), the European Convention of Human

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[2] Article 46 GDPR.

Rights (ECHR) and the GDPR[3].

1.2.1 DATA TRANSFERS IN THE GDPR

Personal data transfers to a third country or to an international organisation under the GDPR are only permitted if they comply with the requirements of Chapter V[4]. In principle, the GDPR allows the transfer of personal data to third countries or to international organisations based on three broad transfer tools, namely: (i) adequacy decisions; (ii) appropriate safeguards, i.e., legally binding and enforceable instruments between public authorities or bodies, binding corporate rules, standard contractual clauses, codes of conduct, or certification mechanisms[5]; and (iii) derogations[6]. With these tools, the GDPR intends to provide a high level of protection to personal data transferred to third countries and international organisations[7]. Accordingly, the third country, international organisation or the transfer instrument, in case of appropriate safeguards, should provide guarantees, safeguarding a level of protection essentially equivalent to that ensured within the Union[8]. The Court has gradually developed the criteria for essential equivalence in *Schrems I, Opinion 1/15, and Schrems II,* which are relevant for all transfer mechanisms provided in the GDPR[9].

1.2.2 INTERFERENCES WITH THE FUNDAMENTAL RIGHTS UNDER THE EU-CHARTER

Governmental access to personal data transferred from the EU to a third country or international organisation has been found by the CJEU to constitute an interference with Articles 7 (right to privacy), 8 (right to data protection), 21 (non-discrimination) and 47 EU-Charter (right to an effective remedy and fair trial). First, if communication data (content and/or meta-data) are maintained, accessed, and/or exposed by public authorities at the transfer's destination, this can constitute an interference with the fundamental right to privacy in Article 7[11]. Second, there can be an interference with Article 8, when the transfer of personal data constitutes processing of such data[10]. Third, due to "*the risk of data being processed contrary to Article 21 of the Charter*," the CJEU decided in *Opinion 1/15* that the transfer of special categories of personal data would require a precise and particularly solid justification[11]. Fourth, the lack of effective remedies in a third country or international organisation in a situation of

[3] Article 52(3) of the EU Charter states "*in so far this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.*" Therefore, the sought assessment needs to take place following the interpretation of both the CJEU and the European Court of Human Rights (ECtHR).
[4] Article 44 GDPR.
[5] Articles 46 and 47 GDPR.
[6] Article 49 GDPR.
[7] Article 44 GDPR 'to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined'.
[8] Recital 104 GDPR.
[9] Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650, paragraph 64; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 105 and 188. The *Schrems II* decision is the first to explicitly address the issue of the level of protection necessary for international data transfers under the different transfer mechanisms of the GDPR. In this case, the Court clarified the connections between the various mechanisms and ruled that they should be all afforded essentially equal levels of protection to those provided by the GDPR. See judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 92.
[10] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 124; and its paragraph 126: "*Those operations also constitute an interference with the fundamental right to the protection of personal data guaranteed in Article 8 of the EU Charter since they constitute the processing of personal data*"; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 170 and 171; and its paragraph 83: the "*[…] the operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data […]*".
[11] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 165; judgment of the Court of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 181.

governmental access can interfere with the fundamental right to an effective remedy in Article 47[12]. However, none of the mentioned fundamental rights are absolute rights, thus where necessary, they can be limited following strict conditions listed in Article 52(1) of the EU-Charter.

According to Article 52(1) of the EU-Charter, an interference with a fundamental right can be justified, if it is (i) provided by law and (ii) respects the essence of the right, meaning that the interference must not empty the right of its core elements and prevent the exercise of the right. Furthermore, the interference must (iii) genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; and finally, (iv) it must be necessary and proportionate[13].

1.2.3 LEGALITY OF GOVERNMENTAL ACCESS

According to Article 52(1) of the EU-Charter, any interference to a fundamental right of the EU Charter must be **provided for by law**. The CJEU holds that "*the legal basis which permits the interference […] must itself define the scope of the limitation on the exercise of the right concerned*"[14]. The national laws permitting the interference shall lay down clear and precise rules governing the scope and application of the limitation[15]. As dissected in its elements below, the quality of law requirement is the first step when assessing if the interference is compatible with the EU-Charter[16].

First, the law authorising the interference, e.g., the governmental access, must be "*accessible to the persons concerned and foreseeable as to its effects*"[17]. Foreseeability refers to the formulation of the law with sufficient precision to enable persons to regulate their conduct[18]. The level of such precision depends on the particular subject-matter[19]. For example, in the particular context of secret measures of surveillance, such as interception of communications, foreseeability cannot mean that individuals should be able to foresee when the authorities are likely to intercept their communications so that they can adapt their conduct accordingly[20]. However, when executed secretly, the power granted to such secret activities may risk arbitrariness[21].

In *Schrems II*, when assessing the US surveillance programme, the CJEU stated that "[…] *the legislation*

[12] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 227. Although in this case, the interference with the PNR agreement was not found to be in violation with Article 47. See further judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 186.
[13] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 124; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 82, 170-171.
[14] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 227. Although in this case, the interference with PNR agreement was not found to be in violation with Article 47. See further judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 186.
[15] Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 180.
[16] The meaning of the expression 'provided for by law' should be in line with the ECtHR case law, which is frequently cited by the CJEU: an interference shall be based on a provision of law that has certain qualities, also known as the "quality of the law" requirement (judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, EU:C:2016:970; Opinion of Advocate General Saugmandsgaard delivered on 19 July 2016, paragraph 40). The CJEU has referred to a body of ECtHR case law in *La Quadrature du Net*, paragraph 128 in this regard: "*a legal framework should be established enabling a balance to be struck between the various interests and rights to be protected"* (ECtHR, 28 October 1998, *Osman v. United Kingdom*, no. 23452/94 , paragraphs 115 and 116; ECtHR, 4 March 2004, *M.C. v. Bulgaria*, no. 39272/98, paragraph 151. See also: ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 276.
[17] ECtHR, 4 December 2015, *Zakharov v. Russia*, no. 47143/06, paragraphs 228-230; ECtHR, 16 February 2000, *Amann v. Switzerland*, no. 27798/95, paragraph 50; also see EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*, pp. 6-7.
[18] ECtHR, 16 February 2000 *Amann v. Switzerland*, no. 27798/95, , paragraph 56*;* ECtHR, 2 August 1984, *Malone v. the UK*, , no. 8691/79, paragraph 66.
[19] ECtHR, 26 April 1979, *The Sunday Times v. the UK*, no. 6538/74, paragraph 49.
[20] ECtHR, 18 May 2010, *Kennedy v. the United Kingdom*, no. 26839/05; , ECtHR, 29 June 2006, *Weber and Saravia*, no. 54934/00, paragraphs 152, 93-95.
[21] ECtHR, 2 August 1984, *Malone v. the United Kingdom*, no. 8691/79, , paragraph 67; ECtHR, 24 April 1990, *Huvig* v. *France*, no. 11105/84, paragraph 29.

in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question […]."[22]. The possibility that the surveillance programmes allow access to data (even to data in transit) without sufficiently clear and precise limits was considered a violation of the legality of the governmental access[23]. Such a law needs to have explicit, detailed provisions on surveillance procedures, providing individuals with a sufficient indication regarding the situations in which public authorities may execute surveillance measures and the conditions thereof[24]. As will be further explained below, the legality of the interference is closely related to whether the limitation is necessary and proportionate[25].

1.2.4 OBJECTIVES OF GENERAL INTEREST OR PROTECTION OF RIGHTS AND FREEDOMS OF OTHERS

Governmental access needs to be strictly necessary to comply with **an objective of general interest or to protect the rights and freedoms of others**[26]. An objective of general interest cannot be sought without considering how it must be reconciled with the fundamental rights impacted by the legislation. This is done by appropriately balancing the general interest goal against the rights in question[27]. Therefore, the objective of general interest and the necessity and proportionality of the limitation are closely associated; it is essential to define and clarify the objective of general interest aimed by the limitation in satisfactory detail, as the necessity and proportionality test will be carried out against this context[28].

In that regard, it is worth referring to the case law of the CJEU on data retention, which discusses both the retention of personal data by private operators in order to be accessed by governmental authorities, and the conditions of such access[29]. It is clear from the Court's case law that only the national security objective may justify public authorities having broad access to retained personal data in a general and indiscriminate manner (bulk access)[30]. The national security objective must be linked to a genuine and present or foreseeable serious threat[31].

[22] "*It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted* […]" judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 176.
[23] Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 180; see also judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650.
[24] ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 370.
[25] ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 334.
[26] Article 3 of the Treaty on the European Union, for instance, mentions freedom, security, and justice as general objectives. EDPB (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, p. 11. Article 23 of the GDPR states that data protection can legitimately be limited for security, defence, crime prevention, significant economic and financial interests, public health and social security, provided that the limitation respects the essence of the right to personal data protection and is necessary and proportionate. See also EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*. Relatedly, the CJEU in *Schwarz v. Stadt Bochum* found that processing personal data to prevent illegal entry to the EU pursued an objective of general interest (judgment of the Court (Fourth Chamber) of 17 October 2013, *Michael Schwarz v. Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670).
[27] Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D. v The Commissioner of the Garda Síochána and Others*, C-140/20, paragraph 52; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 130.
[28] EDPS (2017), *Necessity toolkit*, p. 4.
[29] See *Privacy International*, paragraph 73: "*the mere retention of that data by the providers of electronic communications services entails a risk of abuse and unlawful access."*
[30] Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, paragraph 31; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 166.
[31] Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D. v The Commissioner of the Garda Síochána and Others*, C-140/20, paragraph 58; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168.

Targeted access to and retention of traffic and location data are considered by the CJEU to be a serious interference, thus such targeted access must be based on objective evidence which makes it possible to target individuals whose traffic and location data are likely to reveal a direct or indirect link with serious criminal offences[32]. Objective evidence has to be non-discriminatory, e.g., a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending[33]. Moreover, on the basis of objective and non-discriminatory criteria, geographical areas characterised by a high risk of preparation for, or commission of serious criminal offences can be targeted.

An interference with fundamental rights of the EU Charter can also be justified if it is necessary to protect the rights and freedoms of others. The right to personal data protection often ambivalently interplays with other rights, such as freedom of expression and the right to receive and impart information. In such cases, courts must carry out a balancing exercise to settle the tension between the two[34].

1.2.5 NECESSITY AND PROPORTIONALITY

Fundamental rights and freedoms of the EU can be interfered with only if this is strictly necessary[35]. This translates into the requirements of necessity and proportionality[36]. Proportionality requires a balance to be struck between the importance of the public interest pursued and the seriousness of the interference with fundamental rights[37]. Pursuant to the CJEU, proportionality necessitates the presence of minimal safeguards, such as enforceable rights and effective judicial review, in order to guarantee that interferences are "limited to what is strictly necessary", as stated in *Schrems II*[38]. Apart from the cases directly related to international personal data transfers, the CJEU has developed criteria on how to handle the necessity and proportionality assessments in its case law on data retention mentioned above[39]. This case law should be considered relevant also for international personal data transfers that result in governmental access because it explains the limits to such access from the perspective of the EU-Charter[40].

The proportionality assessment extends to the access to and the use of retained data, which should also be limited to what is strictly necessary for the investigation[41]. Authorisation must be asked prior to

[32] Judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2*,C-203/15 and C-698/15, *EU:C:2016:970*, paragraph 111 and judgment of the Court (Grand Chamber) of , 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18, and C-520/18, EU:C:2020:791, paragraph 148.
[33] Judgment of the Court (Grand Chamber) of 5 April 2022, C-140/20, *G.D. v The Commissioner of the Garda Síochána and Others*, EU:C:2022:258, paragraph 78.
[34] For example, the GDPR Article 85 states that the Member States shall reconcile by law the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic, academic, artistic, and literary expression. Freedom of expression and information is ensured by Article 11 of the EU Charter, and limitations on this right must fulfil the criteria in Article 52 (1), provided above. To achieve a balance between two fundamental rights, the limitations of the right to data protection must apply only insofar as strictly necessary (judgment of the Court (Grand Chamber) of 16 December 2008, *Satakunnan and Satamedia Oy*, C-73/07, ECLI:EU:C:2008:727, paragraphs 56-62).
[35] Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 176 and Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 140-141.
[36] According to the EDPS, the necessity test requires "*a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal*" (EDPS (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit*, p. 27, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf. For other views on necessity see: Gerards, J., 'How to improve the necessity test of the European Court of Human Rights', *International Journal of Constitutional Law*, Vol. 11, No 2, April 2013, pp. 466–490, available at: https://doi.org/10.1093/icon/mot004.
[37] Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 130-131.
[38] Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 184.
[39] Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 35.
[40] EDPB (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, p. 7.
[41] Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, EU:C:2021:152, paragraph 38.

access to the data, except in the event of a justified urgency[42]. This review must be carried out either by a court or an independent administrative body whose decision is binding. Moreover, means for individuals to obtain effective judicial and administrative redress should be in place[43]. Data subjects need an effective possibility to access the retained data, obtain rectification, or erase data[44].

The ECtHR has developed minimum safeguards that the national law authorising governmental access should contain in the cases *Weber & Saravia v. Germany*,[45] *Roman Zakharov v. Russia*, and *Big Brother Watch and the Others*[46]. Such laws need to include clear provisions on:

- the nature of offences that may give rise to a limitation;
- the categories of people liable to have their communications intercepted;
- a limit on the duration of interception;
- the procedure to be followed for accessing, examining, using and storing, communicating and destroying the data obtained;
- the precautions to be taken when communicating the data to other parties and the circumstances in which intercepted data may or must be erased or destroyed; and
- the review of the authorisation procedures and arrangements supervising the implementation of the measures along with any notification mechanism and the remedies provided[47]. This last safeguard may come into play when (i) the surveillance is first ordered, (ii) while it is being carried out, or (ii) after it has been terminated[48].

1.2.6 RESPECT THE ESSENCE OF THE RIGHT

In some instances, an interference can be so extensive and invasive it empties an EU fundamental right of its essence[49]. In this regard, the CJEU considered the law allowing public authorities to access, on a general basis, the content of electronic communications as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the EU-Charter[50]. However, in *Digital Rights Ireland*, where the legislation in question did not permit generalised access to content data, the CJEU held that the limitation was not so intrusive as to impact the essence of the right[51]. *Schrems I* noted that legislation that does not provide any possibility to pursue legal remedies, e.g., access to or to rectify personal data, would be incompatible with Article 47 of the EU-Charter, ensuring the fundamental right

[42] Judgment of the CJEU (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 120; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 137-139; judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, EU:C:2021:152,, paragraphs 40,53-54,58; ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 355.
[43] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 218-227.
[44] *Ibid.* See further judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 190.
[45] ECtHR, 29 June 2006, *Weber and Saravia*, no. 54934/00, also mentioned in judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 175; judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International*, C-623/17, paragraph 65.
[46] ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 54.
[47] ECtHR, 4 December 2015, *Zakharov v. Russia*, no. 47143/06, paragraphs 228-230; ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 335.
[48] ECtHR, 25 May 2021, *Big Brother Watch*, paragraph 336.
[49] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 124, 138-141, 150; EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*, p. 6.
[50] Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14 *EU:C:2015:650*, paragraph 94.
[51] Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, EU:C:2014:238 , paragraph 39.

to effective judicial protection[52].

The essence of a right is interpreted by legal scholars in two ways. The first approach reads the notion as an absolute limit which is not subject to balancing[53]. Following the first view, where the essence of a fundamental right is violated, the interference is unlawful without a further need for testing its necessity and proportionality[54]. The second view links the essence to proportionality test as explained above[55]. In this view, essence forms one component in the proportionality test.

1.3 STUDY METHODOLOGY

For this study, a literature review via desk research (books, journal articles, databases and other online sources) was conducted as the primary step. The purpose of this review was to map the law in the books, consisting of the relevant legal instruments and relevant case law. In addition, reports of international organisations were compiled in this step. After conducting a legal analysis of the collected sources, the loopholes in the knowledge in this area of law were defined. Thereafter, focus was laid on the law in action. A customised questionnaire was composed, tackling the higher defined loopholes (see Annex 1). This country questionnaire was priorly presented to the EDPB, making it possible to distribute the questionnaire to carefully selected experts in Brazil. To have a broad perspective, the researchers of this study strived to find persons working in different legal fields (academia, non-profit sector, the Bar ...).

We have carried out the following numbers of interviews:

- four stakeholders were interviewed, including one representative of the public sector, one of academia, and two lawyers/academics. In general, the interviews did not lead to fundamental changes of the content of the already collected information, but added only precise information.

Finally, the interviews were carefully analysed and compared with the results of the desk research. Where needed, anomalies were indicated. Based on this, the end report of the in-depth analysis was drafted including the results of the interviews.

1.4 STRUCTURE OF THIS REPORT

Section 2 describes an in-depth analysis of the legislation and practice on government access to personal data in Brazil.

[52] Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650, paragraphs 64 and 95. The same conclusion regarding Article 47 was reached in *Schrems II*, where the Court stated: "*According to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter*" (judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 187).

[53] "*From a methodological perspective, the case law of the CJEU reflects the fact that court will first examine whether the measure in question respects the essence of the fundamental rights at stake and will only carry out a proportionality assessment if the answer to that first question is in the affirmative*". Lenaerts, K., 'Limits on Limitations: The Essence of Fundamental Rights in the EU', *German Law Journal*, Vol. 20, pp. 787, 779-793, Cambridge University Press, 2019. See further Brkan, M., 'The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning', *German Law Journal*, Vol. 20, pp. 864-883, Cambridge University Press, 2019.

[54] European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg, 2018, p. 44.

[55] Tridimas, T., Gentile, G., 'The essence of Rights: An Unreliable Boundary?', *German Law Journal*, vol. 20, pp. 794–816 and itsp. 804: *"In short, although the concept of essence as a legal threshold must be understood as an autonomous limit, in effect, it is impossible to determine it without engaging in a balancing process which is best carried out through a proportionality analysis."*

First subsection aims to answer the research question concerning the general situation in Brazil as regards human rights, and specifically the right to privacy and data protection. It provides an overview concerning the rule of law, respect for human rights and fundamental freedoms. The main constitutional provisions are analysed, as well as the concrete application of such provisions in the national case law. The subsection also illustrates whether and how the right to privacy exists in Brazilian legal systems. Afterwards, the general findings by international organisations on the country's human rights situation are also briefly shown.

Subsequently, the country report includes a subsection illustrating the purposes, conditions, and oversight mechanisms of the governmental access to personal data. This subsection aims to answer the research questions related to the specific legislative requirements for government access to personal data; where specific provisions on foreign individuals' personal data do not always exist in the national legal system, the report also tries to address the research questions around the applicability of the Brazilian legislation to foreigners.

A subsection is dedicated to the data subjects' rights, their conditions for applicability and the redress mechanisms available to enforce them. The subsection's goal is to answer the research questions around individual rights and existing redress mechanisms as regards the right to privacy.

Section 3 provides conclusions by answering the research questions.

The annexes included to this study entail the exact questionnaire (Annex 1), a list of all the used sources (Annex 2) and an overview of the used acronyms and abbreviations (Annex 3).

2 IN DEPTH ANALYSIS OF BRAZIL

This section aims to answer the research questions of the study. The structure of the subsections is consistent with a division into areas of interests touched upon by the research questions. The answers are integrated in the related subsections. This section studies the situation in Brazil from the perspective of the rule of law and respect for human rights and fundamental freedoms; government access to personal data; and data subject rights. Any potential upcoming changes in the legislation are also discussed. Finally, the section contains an intermediary conclusion and a grid visually presenting the research results.

2.1 RULE OF LAW, RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

2.1.1 CONTEXT

Brazil is a democratic, liberal state, governed by the rule of law. Its Constitution (1988) states that Brazil is a representative democracy and a constitutional republic with a presidential system. The country follows the civil law legal system, based on codified laws, and is established as a federal state, meaning that it has distinct levels of government (federal, state, and municipal). It is a founding member of the United Nations, and a co-sponsor of the UN Resolution n. 68/167 — on the right to privacy in the digital age[56]. It also ratified the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

The Organisation for Economic Co-operation and Development's (OECD's) Council has recently opened discussions about the accession of Brazil to it[57]. In 2021, Brazil was an observer to the CoE Convention 108 meetings[58] and in 2022, Brazil has acceded to the Convention on Cybercrime, which has entered into force on the first of March 2023[59]. Regionally, Brazil has ratified the American Convention on Human Rights.

Before the adoption of the Brazilian General Data Protection Law *(Lei Geral de Proteção de Dados Pessoais* – LGPD, in the Portuguese acronym)[60] in 2018 (*infra* section 2.1.4), data protection rules were scattered around many different legal frameworks. They were included, for instance, in the Civil Rights Framework for the Internet, also called the Internet Bill of Rights (*Marco Civil da Internet* – MCI, in the Portuguese acronym)[61], the Consumer Protection Code (*Código de Defesa do Consumidor* – CDC,

[56] Human Rights Council, A/HRC/27/3, *The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights*, available at: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.ohchr.org%2Fsites%2Fdefault%2Ffiles%2FDocuments%2FIssues%2FDigitalAge%2FA-HRC-27-37_en.doc%23%3A~%3Atext%3DIn%2520its%2520resolution%252068%252F167%2Ccommunications%2520and%2520the%2520collection%2520of&wdOrigin=BROWSELINK.

[57] OECD, *OECD takes first step in accession discussions with Argentina, Brazil, Bulgaria, Croatia, Peru and Romania*, 25 January 2022, available at: https://www.oecd.org/newsroom/oecd-takes-first-step-in-accession-discussions-with-argentina-brazil-bulgaria-croatia-peru-and-romania htm.

[58] Council of Europe, *Brazil and the Data protection Commission of Gabon to join the Committee of Convention 108 as observers*, 12 October 2018, available at: https://www.coe.int/en/web/data-protection/-/brazil-and-the-data-protection-commission-of-gabon-to-join-the-committee-of-convention-108-as-observers-.

[59] Council of Europe, *Brazil accedes to the Convention on Cybercrime and six States sign the new Protocol on e-evidence*, 30 November, 2022, available at: https://www.coe.int/en/web/cybercrime/-/brazil-accedes-to-the-convention-on-cybercrime-and-six-states-sign-the-new-protocol-on-e-evidence.

[60] *Lei nº 13.709, de 14 de Agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD)*, available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709 htm.

[61] *Lei nº 12.965, de 23 de Abril de 2014, Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*, available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965 htm.

in the Portuguese acronym)[62], the Access to Public Information Law (*Lei de Acesso à Informação* – LAI, in the Portuguese acronym)[63], the Civil Code[64], the Good Payer's Registry Law (*Lei do Cadastro Positivo*, afterwards amended by Complimentary Law N. 166/2019)[65] and Interception of Telephone Communication Law (*Lei de Interceptação Telefônica*)[66]. The patchwork of legal frameworks has received numerous criticisms, either due to the fragility of the protection of the data subject, or due to the legal uncertainty that this has caused. Actors from different sectors defended for years the need for a general data protection law, which took place in 2018 with the publication of the LGPD[67]. This first general law on data protection in Brazil involved different stakeholders during the legislative process, and considered international standards and good practices in the data protection field.

The development of the LGPD was substantially influenced by the Convention 108 of the Council of Europe (CoE), the Directive 95/46/EC and the GDPR. Among other similarities to the GDPR, it also follows the ex-ante protection system and the accountability approach, sets a need for a legal basis for data processing, and establishes a minimum set of principles and data subjects' rights that must be observed in every processing of personal data. This is a result of the heavy public engagement in the drafting of the law[68].

The LGPD provisions became applicable on different dates: (i) in 2018, the rules relating to the structure and functioning of the Brazilian Data Protection Supervisory Authority (*Autoridade Nacional de Proteção de Dados* – ANPD, in the Portuguese acronym)[69] (pending the *de facto* creation of authority through the appointment, by the President of the Republic, of its directors); (ii) in 2020, the rest of the law, except the provisions concerning sanctions; and (iii) in 2021, the sanctions provisions.

The processing of data for the purposes of criminal persecution, national defence, State security or public safety do not fall under the scope of the LGPD. The law determines that this should be addressed in a separate legislation. Still according to the LGPD, any new legislation concerning these exceptions must lay down proportionate and strictly necessary measures to meet the public interest, while considering due process, data protection principles and data subject rights in the LGPD[70].

The Brazilian Constitution[71] also contains some important provisions for the protection of personal data. It provides for the right to privacy in its Article 5º, X; the right to the secrecy of correspondence in its Article 5º, XII; and the *habeas-data* in Article 5º LXXII, a constitutional remedy that guarantees individuals the right to know whether their data are being processed by a public entity and, if necessary, the subsequent rectification. In 2022, the Constitution was amended to recognise the right to the protection of personal data as a fundamental right in the Brazilian legal order (Article 5º, LXXIX).

---

[62] *Lei nº 8.078, de 11 de Setembro de 1990, Dispõe sobre a proteção do consumidor e dá outras providências*, available at: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado htm.

[63] *Lei nº 12.527, de 18 de Novembro de 2011, Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências*, available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527 htm.

[64] *Lei nº 10.406, de 10 de Janeiro de 2002, Institui o Código Civil*, available at: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm

[65] *Lei nº 12.414, de 9 de Junho de 2011, Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito*, available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414 htm.

[66] *Lei nº 9.296, de 24 de Julho de 1996, Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal*, available at: http://www.planalto.gov.br/ccivil_03/leis/l9296 htm.

[67] Mendes, L. S., '*A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis',* Caderno Especial LGPD, São Paulo, RT, November 2019, pp. 35-56.

[68] Ministério da Justiça e Segurança Pública, *Governo lança debate público sobre regulamentação de lei e anteprojeto*, 28 January 2015, available at: https://www.gov.br/mj/pt-br/assuntos/noticias/governo-lanca-debate-publico-sobre-regulamentacao-de-lei-e-anteprojeto.

[69] Autoridade Nacional de Proteção de Dados - ANPD, https://www.gov.br/anpd/pt-br.

[70] Article 4º, paragraph 1, LGPD.

[71] *Constituição da República Federativa do Brasil de 1988*, available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao htm.

2.1.2 CONSTITUTION

The Brazilian Constitution foresees that "all persons are equal before the law, without any distinction whatsoever". Therefore, all fundamental rights which include the rights to privacy and to the protection of personal data, are guaranteed to both Brazilians and foreigners residing in the country. Since 2020, data protection is openly considered a fundamental right in Brazil, due to a ruling of the Brazilian Supreme Federal Court (*Supremo Tribunal Federal* - STF, in the Portuguese acronym)[72]. As already mentioned, this right was enshrined in the Constitution itself in 2022. The new constitutional provision also determines that it is an exclusive federal competence to organise, oversee and draft bills on the right to the protection of personal data and data processing.

A relevant consequence of the ascension of data protection to the status of an autonomous fundamental right is that any proposal to abolish the right to data protection could not even be analysed by the National Congress (Article 60 paragraph 4º Constitution). This status also highlights the dual dimension of the fundamental right to data protection: (i) the subjective dimension, which concerns the individual protection against the risks of data processing while preserving the rule of law; and (ii) the objective dimension, which concerns the legislative duty of protecting personal data[73].

Even though the Constitution only mentions the protection of foreigners residing in the country, the Migration Law (*Lei de Migração*)[74] states that every person on national territory, residing in it or not, is entitled to the protection of fundamental rights, including the right to access to information and the guarantee of confidentiality of their personal data (Article 4º XIII Migration Law). Even though most judicial decisions regarding fundamental rights of foreigners only focus on the ones with permanent residency in the country[75], they are guaranteed to all individuals.

Regarding the activities carried out by public authorities, the Brazilian Constitution states they must follow the principles of legality, impersonality, morality, publicity, and efficiency (Article 37, Constitution). It is constitutionally established that public authorities and private legal entities are liable for damages that any of their agents, acting as such, cause to third parties (Article 37 paragraph 6º, Constitution), which may include the misuse of personal data[76].

2.1.3 THE CIVIL RIGHTS FRAMEWORK FOR THE INTERNET IN BRAZIL (MCI)

The MCI is the result of a bill proposed by civil society, which was drafted through an open and collaborative effort. Although the initial drafting of the bill and online public consultations started in 2008, it was only after Snowden's revelations that the topic gained momentum in the Brazilian Congress and the bill entered into force in 2014.

[72] Supremo Tribunal Federal, ADI 6387, 2020, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165.
[73] Supremo Tribunal Federal, ADPF 695/DF, 2022, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693.
[74] *Lei nº 13.445, de 24 de Maio de 2017, Institui a Lei de Migração*, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445 htm#:~:text=Institui%20a%20Lei%20de%20Migra%C3%A7%C3%A3o.&text=Art.,pol%C3%ADticas%20p%C3%BAblicas%20para%20o%20emigrante.
[75] For example, RE 587970/SP ruled that the social assistance foreseen in the Article 203, V, Constitution benefits Brazilians by birth, naturalised Brazilians and foreigners with residency in the country (Supremo Tribunal Federal, RE 587970/SP, 2017, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2621386); or RE 1018911/RR that states that the foreigner that demonstrates their lack of financial condition do not have to pay the fees to regularize their migration situation (Supremo Tribunal Federal, RE 1018911/RR, 2021, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5115280).
[76] Autoridade Nacional de Proteção de Dados, *Tratamento de Dados Pessoais pelo Poder Público*, 2022, available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf .

The main idea of the MCI was to translate the Brazilian Constitution into the online environment[77] and it is known to be based on three main pillars: freedom of expression, net neutrality and privacy. It establishes the principles, rights, obligations, and guarantees on the internet use in Brazil. Although data protection is not the direct focus of the MCI, it is one of its principles (Article 3º, III, MCI).

A series of rights is provided for by the MCI (Article 7º, MCI), which includes the right: (i) to the inviolability of intimacy and private life; (ii) to the inviolability and secrecy of the communication flow over the internet, unless otherwise ruled by a judicial decision; (iii) to the inviolability of stored private communication, unless otherwise ruled by a judicial decision; (iv) to obtaining information about the protection of connection and registries of access to internet apps; (v) not to have one's personal data shared with third parties; (vi) to obtain information about the processing of personal data, including its purposes; and (vii) to data erasure[78].

The rights to privacy, to the protection of personal data and the inviolability and secrecy of communication must be respected when at least a part of the processing of the personal data occurs on the national territory. This includes the situations in which a company located outside Brazil offers its services to the Brazilian population or has at least one establishment in the country (Article 10, MIC). The MCI also stipulates that contractual clauses that violate the rights to privacy, freedom of expression, as well as the inviolability and secrecy of private communications are to be considered invalid (Article 8º MCI).

The MCI also sets the need to consent for data processing (Article 7, VII, MCI), which seems to have been tacitly overridden by the LGPD, although there is still no official ruling on the matter. In Brazil, the Law of Introduction to the Rules of Brazilian Law (*Lei de Introdução às Normas do Direito Brasileiro* – LINDB in the Portuguese acronym)[79], provides, in its Article 2º that a subsequent law revokes the previous one when it expressly declares it, when it is incompatible with it or when it fully regulates the object of the previous law. It is also possible to understand the LGPD as a *lex specialis* when it comes to data protection. Certainly, the MCI was not revoked as a whole, but it is possible to interpret the tacit revocation of some of its provisions, such as the one referring to consent. Sanctions and data breaches are also topics of possible antinomy[80]. The ANPD has recently published a new Regulation of Dosimetry and Application of Administrative Sanctions[81], and has focused on the provisions set by the LGPD. This can reaffirm the special character of the LGPD.

The internet service and application providers, as defined by MCI, are responsible[82] for keeping a register of internet connection and access to applications[83]. Article 10 MCI states that safeguarding and making available these logs, together with personal data and the content of personal communication

[77] Souza, C. A., Viola, M., Lemos, R., *Brazil's Internet Bill of Rights: A Closer Look, Instituto de Tecnologia e Sociedade*, 2018, available at: https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa_pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf.

[78] In the MCI, data erasure is defined in its Article 7º, X, as the permanent erasure of personal data provided by the user to a given internet application, at their request, at the end of the relationship between the parties, except for the cases of mandatory record keeping provided for in the MCI and in the LGPD.

[79] *Decreto-Lei n. 4.657, de 4 de setembro de 1942, Lei de Introdução ás Normas do Direito Brasileiro*, 1942, available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm.

[80] Parentoni, L., Lima, H., 'Proteção de Dados Pessoais no Brasil: Antinomias Internas e Aspectos Internacionais', *Direito & Internet: Sistema de Proteção de Dados Pessoais*, 2019, pp. 483-512.

[81] Autoridade Nacional de Proteção de Dados, *Resolução CD/ANPD n. 4, de 24 de fevereiro de 2023, Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas*, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf.

[82] As established by Article 13, MCI, the responsible entity for the independent system must retain the connection logs for at least one year. Nonetheless, public authorities may require, as a precautionary measure, to extend this period; after 60 days of the preventive measure, the authority must ask for a judicial authorisation to access the data. In any case, sharing the registries requires a previous judicial order.

[83] As established by Article 15, MCI, the provider of applications must retain connection logs for internet application for six months. A judicial order may establish that other companies must work to retain said logs if the information is related to a fact and time. Public authorities can also, by a provisional measure, require a longer period of retention. However, in any case, the sharing of registries depends on a judicial order.

must be done in a way to protect user's intimacy, privacy, honour and image. Article 10 paragraph 3 MCI affirms that this does not prevent access to a person's registration data such as qualification, affiliation and address. Internet service and application providers can be obliged to share access logs and other personal data to identify an individual upon a judicial order (Article 10, paragraph 1º, MCI), as discussed below.

Content of communications can also be made available pursuant to a court order (Article 10, paragraph 2º MCI). However, the MCI does not oblige internet or application service providers to keep the content of communications, as it does for the registration of internet connections and access to applications (Article 14 et seq., MCI). This led to some legal disputes, including decisions that established the suspension of applications such as [redacted] after court orders requiring the provider to make the content of encrypted communication accessible to law enforcement authorities[84].

Any interested party may apply for a court order so that logs or the content of communications be included as evidence in a civil or criminal procedure. The competent judicial authority is then responsible for guaranteeing the secrecy of information when necessary. This authority can be a judge or a member of a Court if it is still possible to produce evidence in the procedure[85]. According to Article 22, MCI, the application for a judicial order must include (i) well-founded evidence of the occurrence of the offence; (ii) reasoned justification of the usefulness of the records requested for investigation or for evidence purposes; (iii) the period to which the records refer. In addition, the judge is called to take appropriate measures to protect, *i.a.*, private life. In light of this, an intrusion to private life would need to meet the criteria of (i) proportionality; (ii) necessity; (iii) responding to a public interest and (iv) providing appropriate measures to protect the right to privacy.

The MCI does not directly address the topic of data transfers to third countries. In relation to data processed within the scope of the MCI, the LGPD would normally apply to data transfers (where this is also within the scope of the LGPD).Article 11, MCI, also reinforces that the Brazilian legislation and, specifically, the rights to privacy, to the protection of personal data, and the secrecy of private communication and records must be observed whenever at least part of the logs, data processing or communication is carried out within the national territory. The same applies to situations when the processing activities are done by an international company, as long as it offers services to the Brazilian market or when at least one member of the same economic group has an establishment in Brazil.

Although this directly regulates the activities of companies in Brazil, in a recent decision[86], the STF deemed constitutional that Brazilian authorities request information directly from those entities that are covered by the scope of Article 11, MCI, without having to use, in the specific case, the MLAT agreement with the United States of America, as will be further developed below. As justified by the STF, this model is aligned with other countries' models such as Canada, Norway, Spain and Belgium[87].

In cases where Article 10 and 11, MCI, are not observed, without prejudice to other civil, criminal or administrative sanctions, internet connection or application providers may (i) receive a warning,

[84] It is important to note that the discussion on the constitutionality of suspending [redacted] applications for law enforcement based on the MCI has reached the STF, but court proceedings have been paralysed since 2020 (see Supremo Tribunal Federal, ADI 5527, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282, and Supremo Tribunal Federal, ADPF 403, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500). So far, only two STF justices have published their votes. Both converged in the sense of ruling out the interpretation that considers possible the breaking (or weakening) encryption through a court order for accessing the content of messages with law enforcement purposes. Thus, they argue that it is not possible to impose the penalties of the MCI when they imply breaking encryption. (Vlois, R., 'Tecnoautoritarismo e o bloqueio de provedores por descumprimeinto de ordens judiciais no Brasil', *Nexo Jornal*, 26 January 2023, available at: https://pp nexojornal.com.br/opiniao/2023/Tecnoautoritarismo-e-o-blockio-de-provedores-por-descumprimento-de-ordens-judiciais-no-Brasil).

[85] In criminal cases, there is a judge involved since the investigation phase. The investigating judge will work on guarantying the fundamental rights during the course of investigation.

[86] Supremo Tribunal Federal, ADC 51, 2023, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379.

[87] Supremo Tribunal Federal, *ADC 51 – Constitucionalidade do Mecanismo Previsto no MLAT*, available at: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/briefingGabineteADC51.pdf.

indicating a deadline for adopting corrective measures; (ii) receive a fine of up to 10 % of the revenue of the economic group in Brazil; (iii) undergo temporary suspension of activities involving the acts provided for in Article 11; or (iv) be prohibited from carrying out activities involving the acts provided for in Article 11.

2.1.4 THE BRAZILIAN GENERAL DATA PROTECTION LAW

The LGPD applies to the public and private sector, if the processing of personal data takes place in the national territory[88]; if its purposes are related to the offering of services or goods to the Brazilian population; or if the data has been collected in the national territory[89]. These situations do not depend on the nationality of the data subject, meaning that foreigners will also have their rights guaranteed if their data are being processed under one of these circumstances.

As mentioned earlier, the LGPD does not apply in certain situations, such as when data is being processed for purposes of public security, national defence, State security, or investigation and repression of criminal offences (Article 4º III LGPD). These purposes listed will need to be regulated by specific law, according to the LGPD, which must provide for proportional and strictly necessary measures to serve the public interest, observing due process of law, the general principles of protection and the rights of the holder provided for in the LGPD (Article 4º, paragraph 1º LGPD). The law also establishes that private entities are prohibited to process data for these purposes, unless they work under the supervision of a public authority. In these cases, there is a specific obligation of informing the ANPD[90]. Finally, the ANPD must issue technical opinions or recommendations regarding these exceptions and request data protection impact assessments from competent authorities (Article 4º, paragraph 3º LGPD).

According to the LGPD, the processing of personal data must respect certain principles[91] and it can only take place if there is a legal basis. The relevant legal provisions can be different when it comes to special categories of data[92]. It is important to mention that it is still not clear which legal bases apply to the

[88] The LGPD defines processing as: any operation carried out with personal data, such as those referring to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, diffusion or extraction (Article 5º, X). Thus, as long as one of these steps happens in Brazilian territory, the processing must comply with the LGPD, including if the collection happened in another country and the data were then transferred to Brazil.

[89] The data collection is considered to take place in the national territory if the data subject was in Brazilian territory at the moment of the collection.

[90] Article 4, paragraph 2º, LGPD. The supervision of the public authority should be understood as the fact that the public body is responsible for the decisions of the processing, sub-contracting a private company as a processor. Also, Article 4, paragraph 4º, LGPD, establishes that in any case the full length of a database related to these purposes can be processed by a private entity, unless this company is completely composed of public capital.

[91] Article 6º, LGPD states that data processing must respect the following principles: purpose limitation; suitability for the purpose of data processing; necessity and proportionality; free access to data by the data subject; data quality; transparency; security; prevention; non-discrimination; accountability.

[92] The special categories of data include sensitive data and data of children and adolescents. Sensitive data is defined as any data about race or ethnic origin, religious beliefs, political opinion, union membership, affiliation to a religious, philosophical or political organisation. It is also considered as sensitive data regarding the health or the sexual life of an individual, or any genetic or biometric data (Article 5º, II LGPD). For processing general personal data, the legal bases that can be used are (Article 7º, LGPD): consent; legal or regulatory obligation; execution of public policies; conducting studies by research body; execution of contracts or preliminary procedures; regular exercise of rights in judicial, administrative or arbitration proceedings; protection of life or physical safety of the data subject or third party; health protection; legitimate interest; and credit protection. For processing sensitive data (Article 11, LGPD), the legal bases of legitimate interest, credit protection and execution of contracts or preliminary procedures are not allowed. However, the LGPD includes for these cases another legal basis: the prevention of fraud and security of the data subject, in the processes of identification and authentication of registration in electronic systems. For processing children's data, the LGPD is not clear if all the legal bases related to general and sensitive data apply (the ANPD is currently working on this issue after having opened a public consultation). However, Article 14, LGPD, provides specific rules on consent, stipulating that it may be given by persons aged 12 and over. It also provides specific legal bases in cases where the consent of children under 12 years old cannot be collected in its Article 14 paragraph 3º (to contact parents or the legal guardian, or for the child's protection).

public sector[93]. In 2020, the STF ruled that execution of public policies was the only possible legal basis from Article 7º (general data) and 11 (sensitive data) that could be applied to data sharing by the public administration. Based on this interpretation, the court understood that specific provisions in Chapter IV, LGPD, would provide extra legal bases for the processing of personal data by the public sector. Article 23, LGPD, for example, would allow the processing of personal data for the execution of legal competences or attributions of public services.

In an apparent different direction, a guideline published by the ANPD on data processing by the public sector establishes that any of the legal bases defined in the LGPD, either in Article 7º or 11, can be used by the public sector. When it comes to consent and legitimate interest, the examples are related to activities that have no direct corelation with public functions[94]. Beyond the legal basis of execution of public policies, the ANPD established that the fulfilment of a legal or a regulatory obligation is a relevant and applicable legal basis for data processing for public authorities.

The LGPD also establishes some data subject rights, including the right to access, rectification, portability, information, request for anonymisation, blocking or erasure of data processed in discordance with the law, and request the erasure of data processed by consent. These will be further discussed below (*infra*, section 2.4).

International data transfers are only allowed within the LGPD framework when (Article 33 LGPD):

- the third country or international organisation provides an adequate level of protection of personal data, aligned with the LGPD[95];
- there are adequate guarantees of compliance with the principles and data subject rights provided by the LGPD, in the form of
    - specific contractual clauses for a given transfer;
    - standard contractual clauses;
    - global corporate norms; or
    - regularly issued stamps, certificates or codes of conduct.
- the data transfer is necessary for international legal cooperation between public intelligence, investigative and criminal prosecutorial agencies, in accordance with the instruments of international law;
- the transfer is necessary to protect the life or physical safety of the data subject or a third party
- the ANPD has provided authorisation
- the transfer is related to an agreement undertaken through international cooperation
- the data subject has provided his/her specific and highlighted consent for the transfer, having received prior information on the international nature of the operation, clearly distinguishing it from other purposes;
- necessary for compliance with a legal or regulatory obligation by the controller;
- necessary for the performance of a contract or preliminary procedures related to a contract to which the data subject is a party, at the request of the data subject;
- necessary for the regular exercise of rights in judicial, administrative or arbitration proceedings.

[93] Wimmer, M., 'O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público', *Tratado de Proteção de Dados Pessoais*, 1. ed., Rio de Janeiro, Forense, 2021. pp. 271–288.
[94] The guideline explains that consent will not be the most appropriate legal basis for processing personal data by the Public Sector, notably when the processing is necessary for the fulfilment of legal obligations and attributions. In those cases, the body or entity exercises typical state prerogatives, which are imposed on the subject in a power imbalance relationship, in which the individual does not have effective conditions to freely express themselves (e.g., registering in a public university). Therefore, consent cannot be used, as a rule, for public activities purposes. The same applies for the legitimate interest, where the public authority must verify the proportionality of the processing (e.g., information security activities) (Autoridade Nacional de Proteção de Dados, *Tratamento de Dados Pessoais pelo Poder Público*, January 2022, available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf.
[95] The ANPD has still not issued any adequacy decisions.

Although the structure of the LGPD, when it comes to data transfers, is quite similar to the GDPR, there are important differences. According to national experts, for example, there is no hierarchy between the different possibilities for international data transfers and any of the legal grounds are valid. So far, the ANPD has not issued adequacy decisions. It is also important to note that although public intelligence, investigative and criminal prosecution activities are not within the scope of the LGPD, Article 33 foresees these activities as a legal ground for data transfers.

When a controller or data processor violates the LGPD, they are subject to redress mechanisms (*infra* section 2.3.2) and also to administrative sanctions applied by the ANPD. The possible administrative sanctions are:

- a warning, with an indication of the deadline for adopting corrective measures;
- a fine of up to 2 % of the income of the private legal entity, group or conglomerate in Brazil in its last fiscal year, excluding taxes, limited in total to R$ 50 000 000.00 (fifty million reais) for infringement;
- a daily fine, limited in total to R$ 50 000 000.00 (fifty million reais) for infringement;
- the publication of the violation after its occurrence has been duly investigated and confirmed;
- the suspension of the processing of the data related to the violation until its regularisation;
- the erasure of the personal data related to the violation.

2.1.5 THE BRAZILIAN DATA PROTECTION SUPERVISORY AUTHORITY (ANPD)

The ANPD was first envisioned as an independent body in the LGPD. However, the creation of a new agency in Brazil by the legislative power was considered unconstitutional by the president of the republic at the time, which argued that only the executive branch was competent to do so. Despite having sanctioned the LGPD, the former president vetoed the provisions related to the ANPD and issued the Provisory Measure (MP) n. 869/2018[96], creating it as a body connected to the Presidency of the Republic – thus eliminating the financial and political autonomy of the authority. The ANPD started its activities only in November 2020, after the nomination of the first directors of the authority.

In 2022, another Provisory Measure[97] modified the LGPD and turned the ANPD into a 'special nature autarchy', which means that it is autonomous and independent for its decisions and normative publications. More recently, a Presidential Decree[98] linked the ANPD to the Brazilian Ministry of Justice and Public Safety, putting an end to its direct connection with the Presidency of the Republic. The affiliation with the Ministry of Justice and Public Safety was important since the Ministry is historically linked to the protection of fundamental rights. It also does not affect the independence of the ANPD, since this is now foreseen by law. This administrative change only guarantees that the Ministry, and not the Presidency, is the public body responsible for providing administrative support to the ANPD, such

[96] Transformed into Law n. 13.853/2019 (*Lei nº 13.853, de 9 de Julho de 2019, Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências*, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853 htm).
[97] MP n. 1124/2022, transformed into the Law n. 14.460/2022 (*Lei nº 14.460, de 25 de Outubro de 2022, Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019*, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14460 htm).
[98] *Decreto nº 11.348, de 1º de Janeiro de 2023, Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública e remaneja cargos em comissão e funções de confiança*, available at: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348 htm.

as personnel and infrastructure[99]. It is important to mention that the speed of the ANPD independence procedure was due to the fact that it was also a national priority. Brazil plans ascending to the OECD and having an independent DPA was formally recommended to the Brazilian government.
The nomination of the ANPD directors is done by the president of the republic and further approved by the Federal Senate[100]. This nomination must follow specific rules, especially in relation to the expertise of the person to be nominated and their possible previous relationships with political parties, for example[101]. Other staff members of the authority are nominated via official procedures considering the hierarchy and organisation of the public entity.

Nominated directors form a regulatory body, which is responsible for deciding specific cases and developing the internal rules of the authority. The ANPD also has a consulting body, the National Council for Data Protection and Privacy (*Conselho Nacional de Proteção de Dados Pessoais e da Privacidade* – CNPD, in the Portuguese acronym). The consultancy body is composed of 23 stakeholders representing different societal sectors[102]. The CNPD is responsible for providing non-binding inputs for the National Policy on Data Protection and Privacy and for the activities performed by the ANPD. The Council should also work on the elaboration of studies and public debates about data protection and privacy and on the dissemination of these topics.

Having only been constituted at the end of 2020, the ANPD is still a new structure. According to a national expert, considering that data protection is a relatively recent topic of concern in Brazil (the first discussions on the LGPD began in 2010), the federal administration did not have adequate structures for the development of the ANPD. In recent years, the ANPD has focused many efforts on its regulatory agenda and on establishing basic guidelines for the correct understanding and application of the LGPD. This period was also important for it to structure itself internally and create the necessary formal procedures for law enforcement. Gradually the authority increased its personnel from five presidents and five permanent staff to a hundred permanent staff and twenty temporary staff.

Publishing activity reports is also one of the obligations set by the LGPD to the ANPD (Article 55-J, XII LGPD). So far, the authority has published biannual regulatory agendas and reports on the development of the planned actions to comply with said provision. The topics foreseen in the regulatory agenda for 2021-2022 were all at least initiated[103]. Considering the ongoing aspects of these activities, some topics are also fixed in the new regulatory agenda for 2023-2024 (e.g., international data transfers)[104]. Another activity that has just started is the Evaluation of Regulatory Results (*Avaliação de Resultados Regulatórios* – ARR, in the Portuguese acronym). This procedure will allow the ANPD to understand the results of the regulatory activities developed by the authority[105]. For now, two topics are

[99] Autoridade Nacional de Proteção de Dados, *ANPD e Ministério da Justiça e Segurança Pública editam portaria conjunta*, 13 February 2023, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-ministerio-da-justica-e-seguranca-publica-editam-portaria-conjunta.
[100] Article 5º, Law 9,986/00 (*Lei nº 9.986, de 18 de Julho de 2000, Dispõe sobre a gestão de recursos humanos das Agências Reguladoras e dá outras providências*, available at: http://www.planalto.gov.br/ccivil_03/leis/l9986 htm), and Article 55-D, LGPD.
[101] Article 8º-A and 8º-B, Law 9, 986/00.
[102] The ANPD received 120 names for composing the CNPD (Grossman, L. O., 'ANPD recebeu 120 indicações para Conselho Nacional de Proteção de Dados', *Convergência Digital*, 26 March 2021, available at: https://www.convergenciadigital.com.br/Seguranca/ANPD-recebeu-120-indicacoes-para-Conselho-Nacional-de-Protecao-de-Dados-56510 html?UserActiveTemplate=site).
[103] Autoridade Nacional de Proteção de Dados, *ANPD divulga balanço de acompanhamento e execução da Agenda Regulatória 2021/2022 referente ao 2º semestre de 2022*, 16 January 2023, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-, available at: balanco-semestral-de-acompanhamento-e-execucao-da-agenda-regulatoria-2021-2022.
[104] Autoridade Nacional de Proteção de Dados, *Portaria ANPD n. 35, de 4 de novembro de 2022, Agenda Regulatória para o biênio 2023-2024*, available at: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885.
[105] Autoridade Nacional de Proteção de Dados, *ANPD publica Agenda de Avaliação de Resultados Regulatórios*, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-de-avaliacao-de-resultados-regulatorios.

going through this assessment: regulation on the procedure of oversight by the ANPD, and regulation on dosimetry of sanctions[106].

2.1.6 TRANSPARENCY RULES IN THE PUBLIC SECTOR

Publicity and transparency are essential principles that guarantee the democratic control of state activities. In Brazil, the Access to Public Information Law (*Lei de Acesso à Informação* – LAI in the Portuguese acronym) applies to the executive, legislative and judicial branches and public authorities of the Federal, State, Municipal and Federal District levels, as well as to private entities that receive public funding to carry out activities in the public interest. The protection of classified and personal information should be observed by every actor to whom the LAI applies, guaranteeing the availability, authenticity, integrity, and restrictions of access to this information.

Since the LGPD entered into force, various requests of data access based on LAI have been denied often unjustifiably[107]. However, these two legal instruments are compatible and should be observed in parallel. The current understanding of the ANPD on the application of the 'compliance with a legal or regulatory obligation' legal basis should be applied in these cases. Once it is legally mandatory for an information to be made publicly available, the LGPD should not be understood as an obstacle to prevent such publication, but as a set of criteria to balance the fulfilment of different human rights[108].

Public authorities must also carry out a case-by-case analysis of the application of both laws. Recently, the ANPD issued a specific opinion in one of these cases. In February 2022, the National Institute of Educational Studies and Research Anísio Teixeira (*Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira* – INEP in the Portuguese acronym) understood that the disclosure of data contained in the publications of the National Examination of Secondary Education (*Exame Nacional do Ensino Médio* – ENEM in the Portuguese acronym) 2020 and the Basic Education School Census (Censo Escolar da Educação Básica) 2021 could risk identifying students and violate their right to data protection. The data are generally used to inform research and public education policies. The ANPD's opinion for this case was that the institute should prepare a Data Protection Impact Assessment, to assess the risks that may be caused to data subjects with the data disclosure. The report must be made public, where applicable, in order to provide transparency to the decisions and measures that will be adopted by the institute. In addition, the ANPD understood that the INEP is in a position to decide on the extent of the disclosure, and it is possible that microdata be presented in different versions for society and for research institutions, through a term of responsibility[109].

The Brazilian Office of the Controller General (*Controladoria Geral da União* – CGU in the Portuguese acronym) is the competent authority to oversee the LAI application in the federal government. Considering the necessity of clarifying the co-existence of data protection and access rules, the CGU and the ANPD recently signed a cooperation agreement[110].

---

[106] Autoridade Nacional de Proteção de Dados, *Resolução CD/ANPD n. 5, de 13 de março de 2023*, *Agenda de Avaliação de Resultado Regulatório para o período 2023-2026*, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-de-avaliacao-de-resultados-regulatorios/RESOLUON5ARR.pdf.

[107] A report published in 2022 evaluated that at least one of four LAI requests that the federal government denied because of the LGPD were not lawful (Fiquem Sabendo, INSPER, FGV, *Impactos da LGPD nos pedidos de LAI ao governo federal*, 2022, available at: https://drive.google.com/file/d/1LfYUOiNVyxC1LAL3U_fGwWSCNL7t16ap/view).

[108] Bioni, B. R., Silva, P. G. F., Martins, P. B., 'Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso', *Cadernos técnicos da CGU: coletânea de artigos da pós-graduação em ouvidoria pública*, 2022, pp. 8 –19.

[109] Autoridade Nacional de Proteção de Dados, *ANPD manifesta-se sobre divulgação de microdados do Eenem e Censo Escolar pelo INEP*, 17 Mai 2022, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-manifesta-se-sobre-divulgacao-de-microdados-do-enem-e-censo-escolar-pelo-inep.

[110] Controladoria-Geral da União, *CGU e ANPD firmam parceria para cooperação entre os órgãos*, 17 February 2023, available at: https://www.gov.br/cgu/pt-br/assuntos/noticias/2023/02/cgu-e-anpd-firmam-parceria-para-cooperacao-entre-os-orgaos.

2.1.7 CYBERSECURITY

Data security is an essential safeguard that should be considered when assessing the proportionality of processing of personal data by the state.

Currently, Brazil ranks 18th in the world on the International Telecommunications Union's Global Cybersecurity Index 2020[111], which is already a huge improvement from the 2018 edition[112], where the country ranked 70th. There are still no specific laws nor bills being discussed in Brazil that deal with cybersecurity in detail. That does not mean, however, that cybersecurity has not been on the national agenda.

In 2018, the Presidential Decree n. 9637[113] instituted the National Information Security Policy within the scope of the federal public administration, providing guidance on information security governance and providing for a waiver of public procurement procedures in cases that could compromise national security. The policy established as instruments of its application the National Information Security Strategy (E-Ciber, explained below) and national plans (which detail the implementation of strategic actions, the planning of activities and the allocation of responsibilities). The Information Security Management Committee was created, with the attribution of advising the Institutional Security Office of the Presidency of the Republic in activities related to information security. The committee is, however, composed only of representatives of the public sector.

In order to provide more clarity in relation to the cybersecurity part of the 2018 National Information Security Policy, the Presidential Decree 10.222 of 2020[114] established Brazil's National Cybersecurity Strategy (E-Ciber). It is the "first official document to provide an overview regarding Brazil's role in cybersecurity, as well as objectives and guiding principles for its development between 2020 and 2023"[115]. E-Ciber details which strategic actions should be implemented by Federal Administration bodies, according to their specific competencies. Since then, several bodies have begun to formalise their internal information security programmes, which is a great achievement for the country. However, the programmes are still superficial and incapable of guaranteeing efficient coordination between public administration, the private sector and the third sector.[116]

It is important to mention that the LGPD also provides important provisions related to cybersecurity. Article 6, VII, defines security as one of the principles that should be followed while processing personal data. Chapter VII, Section I, on Security and Data Confidentiality also requires, *i.a.*, that controllers and processors must adopt security, technical and administrative measures to prevent personal data from unauthorised access, as well as accidental or unlawful situations of destruction, loss, alteration, communication or any form of inappropriate or unlawful data processing (Article 46, LGPD). The

[111] International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI)*, 2020, available at: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.
[112] International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI)*, 2018, available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
[113] *Decreto nº 9.637, de 26 de Dezembro de 2018, Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional*, available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm#:~:text=DECRETO%20N%C2%BA%209.637%2C%20DE%2026,regulamenta%20o%20disposto%20no%20art.
[114] *Decreto nº 10.222, de 5 de fevereiro de 2020, Aprova a Estratégia Nacional de Segurança Cibernética*, Brasil, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222 htm.
[115] Hurel, L. M., *Cybersecurity in Brazil: An analysis of the National Strategy*, Igarapé Institute, 2021, available at: https://igarape.org.br/wp-content/uploads/2021/04/SP-54_Cybersecurity-in-Brazil.pdf.
[116] See Belli, L. et al, *Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil digitalmente soberano*, 2023, available at: https://cyberbrics.info/ciberseguranca-uma-visao-sistemica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/, for a detailed analysis of the current application of E-Ciber and other federal policies.

ANPD may also provide minimum technical standards for this purpose (Article 46, paragraph 1º, LGPD).

2.1.8 PUBLIC SECURITY

Brazil experiences many public security issues. For example, police brutality in Brazil is a point of attention. Although reliable figures on killings by police are hard to find, since governments often do not collect or publish them[117], the Brazilian police is known to be one of the most lethal in the world, with more than 6 100 deaths in 2021, or 17 per day on average[118]. In 2022, following a police raid that killed 23 people in a favela in Rio de Janeiro, "UN experts called on the Brazilian Government to adopt wide-ranging reforms to put an end to police violence, demilitarise all law enforcement agencies and vigorously address systemic racism and racial discrimination"[119].

Technologies are then seen by many as a way not only to bring more efficiency to the work of the security forces, but also to insert certain neutrality and remove discriminatory biases, especially racial discrimination[120]. In a recent survey carried out by the Fundação Getúlio Vargas, the most used technologies by Brazilian security forces are drones (63 %), Optical Character Recognition technologies, mainly used to identify number plates (44 %); facial recognition, (33 %), cameras attached to police uniforms (22 %) and predictive policing technologies (7 %)[121].

The LGPD does not fully apply to public security activities and clear and up-to-date rules on the use of data for this purpose do not yet exist. A future data protection law for public security and criminal prosecution will have to provide for proportionate and strictly necessary measures for fulfilling the public interest, subject to due legal process, and observe the general principles of protection and the rights of the data subject (Article 4(1) LGPD). This is further discussed in more detail in section 2.2 below.

In Brazil, the competence to deal with public security is shared between different levels of the federation and encompasses different bodies, which makes a unique analysis of the use of personal data by these institutions a complex task. According to Article 144, Constitution, public security is a duty of the State and a right and responsibility of all. It is exercised for the preservation of public order and the safety of people and property, through the following bodies: federal police, federal road police, federal railway police, civilian police, military police and military fire departments, and federal, state and district criminal police. Municipalities mainly play a role in prevention, although the expansion of the municipal guard forces has included repression tasks[122].

External control of institutions responsible for public security is carried out by different bodies, depending on the sphere of government and the type of institution. In general, they are controlled by the Public Prosecutor's Office, whether state or federal (Article 129, VII, Constitution). This constitutional provision is detailed in specific laws of each state and, within the federal scope, in the Complementary Law Nº 75/1993, which provides for the organisation, attributions and statute of the Federal Public

[117] Amnesty International, *Police Violence*, available at: https://www.amnesty.org/en/what-we-do/police-brutality/.
[118] Le Temps, *Une opération policière dans une favela de Rio fait au moins 22 morts*, 24 May 2022, available at: https ://www.letemps.ch/monde/ameriques/une-operation-policiere-une-favela-rio-22-morts.
[119] United Nations, *Brazil: UN experts decry acts of racialised police brutality*, 6 July 2022, available at: https://www.ohchr.org/en/press-releases/2022/07/brazil-un-experts-decry-acts-racialised-police-brutality.
[120] According to Amnesty International, racism in Brazil continues to drive state violence, "Mass killings by public security officials were frequent, disproportionately affecting Black people in marginalized neighbourhoods" (Amnesty International, *Amnesty International Report 2022/23: The State of the World's Human Rights*, 2023, available at: https://www.amnesty.org/en/location/americas/south-america/brazil/report-brazil/).
[121] Campos, A. C., 'Drones são adotados por 63% das forças de segurança no Brasil', *Agência Brasil*, 29 March 2023, available at: https://agenciabrasil.ebc.com.br/geral/noticia/2023-03/drones-sao-adotados-por-63-das-forcas-de-seguranca-no-brasil.
[122] Cano, I. 'Public Security Policies in Brazil: Attempts to Modernize and Democratize versus the War on Crime', *Sur*, No 5, year 3, 2006, available at: https://sur.conectas.org/en/public-security-polices-brazil/.

Prosecutor's Office[123]. This external control by the Public Prosecutor's Office takes place, for example, through the control of police occurrences and their consequences, the professionalisation of inter-institutional relations, the statistical study of the activity of the judicial police, and the training of its members[124].

Other important oversight bodies include the Judiciary, Ombudsman offices and Police Internal Affairs. The objective of the latter is to monitor and investigate the actions and/or omissions by police officers that involve a breach of the law or of the rules of conduct of the corporation[125].

2.2 GOVERNMENT ACCESS TO PERSONAL DATA

2.2.1 KEY CONSIDERATIONS

According to Brazilian case law and doctrine, no fundamental right is absolute. As a result, all fundamental rights, including data protection, can be limited depending on the circumstances. Activities of public authorities that limit the right to privacy and to the protection of personal data should always be carried out for the fulfilment of its public purpose, in pursuit of the public interest, and with the objective of executing the legal competences or fulfilling the legal attributions of the public service (Article 23 LGPD). The evaluation of public interest is essential for assessing the proportionality of the interference. The Brazilian Constitution also establishes the legality principle for all actions of the public administration, so any interference to fundamental rights should be conveyed by law (Article 37).

Moreover, Article 50, Federal Administrative Procedures Law[126], determines that every administrative act must be motivated when they deny, mitigate, or affect rights or interests of citizens. Any measure that limits the protection of personal data should be motivated, but there are no clear general rules on how this motivation should be publicised and scrutinised.

In relation to the interference with the rights to privacy and to the protection of personal data, the LGPD establishes some important safeguards, since it also applies to public authorities. Indeed, public authorities may need to access data for many different reasons, but in addition to a legal basis for data processing, this must be carried out for specific purposes, in a transparent manner, ensuring accountability and the exercise of data subjects' rights. The ANPD can also request that public entities publish their data protection impact assessments as well as adopt specific standards and good practices.

Despite the current need for compliance with the LGPD and the right to data protection being enshrined in the Brazilian Constitution, the use of surveillance technologies in the country has grown steadily since 2006. Between 2012 and 2014, various different systems were trialled in Brazil due to the mega-events held by the country. In 2018, technologies such as facial recognition began to spread in Brazil[127]. The

[123] *Lei Complementar nº 75, de 20 de maio de 1993, Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União*, available at: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp75 htm.

[124] Conselho Nacional dos Procuradores-Gerais, *Manual Nacional do Controle Externo da Atividade Policial*, 2009, available at: http://www mpsp mp.br/portal/page/portal/cao_criminal/CAOCri_ControleExtAtivPol/Manual%20Nacional%20do%20Controle%20Externo%20da%20Atividade%20Policial.pdf.

[125] Pereira, A. B. C., Cabral, S., Reis, P. R. da C., 'Accountability interna em forças policiais: explorando os fatores associados ao desempenho de uma corregedoria de polícia militar'. *Organizações & Sociedade*, 27(92), 2020, available at: https://doi.org/10.1590/1984-9270922.

[126] *Lei nº 9.784, de 29 de Janeiro de 1999, Regula o processo administrativo no âmbito da Administração Pública Federal*, available at: http://www.planalto.gov.br/ccivil_03/leis/l9784 htm#:~:text=LEI%20N%C2%BA%209.784%20%2C%20DE%2029%20DE%20JANEIRO%20DE%201999.&text=Regula%20o%20processo%20administrativo%20no%20%C3%A2mbito%20da%20Administra%C3%A7%C3%A3o%20P%C3%BAblica%20Federal.

[127] Instituto Igarapé, *Reconhecimento Facial no Brasil*, available at: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/.

peak of implementation of these technologies in 2020 was mainly due to the surveillance projects developed during the pandemic. In a recent report on the use of surveillance technologies in Brazil, it was identified that the majority of them (76.4 %) were implemented for purposes of public security, but they were also found in areas such as health, tourism and economy[128].

2.2.2 NATIONAL SYSTEM OF INTELLIGENCE

The Brazilian Intelligence System (*Sistema Brasileiro de Inteligência* – SBI in the Portuguese acronym) was established by Law n. 9,883/99[129], which created the Brazilian Agency of Intelligence (Agência Brasileira de Inteligência – ABIN in the Portuguese acronym). The law determines that only public authorities that are part of this system may produce knowledge of interest to the nation, according to the Presidential Act (Article 2º, Law n. 9,883/99)[130].

All public authorities' part of the intelligence system must comply with all constitutional provisions, including fundamental rights and freedoms, international conventions, agreements and adjustments, as well as other legislation. This should be considered during the performance of their duties, which include the processing of information needed for the executive power decision making. The processing of data must also protect the information against the access of non-authorised persons or bodies.

The acts of the Executive Power are overseen by the National Congress and the Federal Court of Accounts (*Tribunal de Contas da União* - TCU in the Portuguese acronym) (Article 49, X, Brazilian Constitution)[131] and any violation of rights can be brought to the judicial power (Article 5, XXXV, Brazilian Constitution). Thus, any issue regarding data usage may be evaluated by the legislative or judiciary powers. Any of these decisions are binding and should follow due process.

ABIN is the central body of the system, which is responsible for planning, executing, coordinating, supervising, and overseeing the intelligence activities. These activities must be carried out using confidential means and techniques. To comply with all its duties, ABIN must receive specific knowledge and data related to the defence of institutions and national interests from the different public authorities part of the SBI (Article 4, Law n. 9,883/99).

In a recent STF decision, the lawfulness of this article was questioned[132]. The ruling stated that the data that public authorities share with ABIN must abide by all formal rules, observing the strict public interest (defence of public institutions and national interest). In case of non-compliance, the activity should be declared unlawful by the judiciary. To guarantee this oversight procedure, it is essential that the purpose of each data sharing activity is defined through formal procedures. This information should be publicly available together with information on how this processing complies with the legal requirements.

Any data sharing activity must also take place on electronic systems with security and data access control, to facilitate oversight. This allows the judiciary to assess if there is a lawful public interest for the processing activities, if the competences are not overlapping (e.g., ABIN has no competence of accessing data collected by waiving of telephone communication secrecy or other data that can only be

[128] Instituto Igarapé, *Implementação de Tecnologias de Vigilância no Brasil e na América Latina*, 2022, available at: https://igarape.org.br/wp-content/uploads/2022/12/Implementacao-de-tecnologias-de-vigilancia-no-brasil-e-na-america-latina.pdf.

[129] *Lei nº 9.883, de 7 de Dezembro de 1999, Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências*, available at: https://www.planalto.gov.br/ccivil_03/leis/l9883 htm.

[130] Decree n. 4376/02 provides more detail on the organisation and functioning of the SBI (*Decreto nº 4.376, de 13 de Setembro de 2022, Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei no 9.883, de 7 de dezembro de 1999, e dá outras providências*, available at: http://www.planalto.gov.br/ccivil_03/decreto/2002/d4376 htm).

[131] The oversight activities can be developed by other bodies that collaborate with the National Congress, such as the Federal Court of Accounts (*Tribunal de Contas da União* – TCU in the Portuguese acronym).

[132] Supremo Tribunal Federal, *STF confirma limitações ao compartilhamento de dados do Sisbin*, 15 October 2021, available at: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=474835&ori=1.

accessed upon a judicial decision), and evaluate if there were any omissions, misapplications, or abuses, which may lead to the liability of agents and/or bodies[133]. In light of the general binding effect of STF decisions, data processing activities carried out by intelligence agencies should all observe this decision. Beyond the internal oversight provided by the ABIN, it is important to note that the ANPD can also carry out audits in the intelligence bodies.

The legal framework provides for an effective oversight of intelligence activities in Brazil. In recent news pieces, it was suggested that the previous federal government used an ABIN system to monitor individuals, gathering information on the location of the citizens via their cell phones. These activities are being investigated by the Federal Police, the National Congress and the TCU[redacted]

During the last years, various scandals involving the intelligence system and the federal government were reported in Brazilian news outlets, [redacted]

Contracts signed by the Executive Power are overseen by the Legislative power, especially by the TCU, Thus, the engagement between the ANPD and the TCU seems like a good initiative to guarantee data protection even in cases involving intelligence or national security activities. For instance, a procedure finalised by the TCU in 2022 evaluated the acquisition of a surveillance system to be used in open data sources. The decision allowed the intelligence entities to move on with the contract but also determined the notification of the ANPD to guarantee further oversight[137].

2.2.3 CRIMINAL PROSECUTION

As mentioned above, the LGPD does not fully apply to certain circumstances, such as when data are processed for purposes of public security, national defence, State security, or investigation and repression of criminal offences (Article 4º, III LGPD). The LGPD demands that a dedicated law be issued to deal with these situations. In relation to two of them, public security and criminal prosecution, a working group was created in 2019 by the Brazilian National Congress to prepare a bill.

The "Draft Data Protection Law for public security and criminal prosecution"[138] was presented to Congress by the commission in December 2020. However, the proposal did not move in view of the need for a parliamentarian to adopt it and take it forward in the legislative process[139]. With this situation,

[133] Supremo Tribunal Federal, ADI 6529, 2021, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837 [redacted]

[137] Tribunal de Contas da União, Processo n. 014.760/2021-5, 2022.

[138] Câmara dos Deputados do Brasil, *Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal*, 2019, available at: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf.

[139] Although the draft bill itself was not adopted by any parliamentarian, a national expert explained that several bills have emerged in recent years with a very similar structure to the working group's proposal. The most discussed bill adopts almost all the suggestions of the working group, but excludes the majority of data subjects rights (Câmara dos Deputados, PL 1515/2022, available at: https://www.camara.leg.br/propostas-legislativas/2326300).

there is still relative legal uncertainty; however, the LGPD is clear in establishing that further specific regulation for these exceptions must provide for proportional and strictly necessary measures for fulfilling the public interest, subject to due legal process, and observe the general principles of protection and the rights of the data subject (Article 4, paragraph 1º, LGPD). Thus, national experts are of the opinion that the principles of data protection must already be observed for these activities. The recent recognition of the fundamental right to the protection of personal data by the Brazilian constitution also reinforces the need for minimal safeguards for any processing of personal data in the country.

A Brazilian non-binding norm[140] also determines that the processing of personal data for the purpose of national security, public security, national defence, and criminal procedures should follow due process, the general principles of data protection and the data subjects' rights established in the LGPD. Although non-binding, this kind of interpretive statement is often used as guidance by the Brazilian judiciary.

It is important to mention that although this specific law still does not exist, there are some rules that apply to data processing for criminal prosecution in Brazil. The confidentiality of correspondence of electronic and telephone communications is considered as a fundamental right in the Brazilian legal framework. Public authorities can access these data only in exceptional cases for the purposes of criminal investigations or prosecution. Therefore, the interception of communication must always be a subsidiary and exceptional measure, that is only allowed when there are no other means to solve a specific case[141]. Furthermore, Article 2 of the Telephone Interception Law provides that the interception of telephone communications shall not be accepted in any of the following circumstances: (i) there is no reasonable evidence of authorship or participation in a criminal offence; (ii) the proof can be provided by other available means; (iii) the fact investigated constitutes a criminal offence punishable only by detention, i.e. the offence is not punishable by the more severe penalty of imprisonment[142]. In any case, the request for telephone interception must clearly describe the situation under investigation, including the identification and qualification of those investigated, unless this is manifestly impossible, which should be duly justified.

The procedural safeguards in case of an interception of communication can only be set out in federal legislation. In that regard, the Telephone Interception Law requires a judicial ruling, by motion of a court, by the court that hears a particular case, by police authorities during criminal investigations, or by the public prosecutor, during the investigation or the prosecution (Article 3º). In any case, the request for interception must clarify the necessity of the measure (Article paragraph 4º). The authorisation will lead to access the content of the communications and is valid for 15 days. This period can be extended by a new decision, once the indispensability of the measure is proven, and there is no limit on how often such a new decision can be requested (Article 5º)[143]. The law reaffirms the exceptionality of the interception, establishing the obligation for the Court to verify the proportionality of the measure (Article paragraph 2º).

Although in general a judicial ruling is necessary to have access to telecommunication data, there are some exceptions. The Brazilian Criminal Procedure Code[144], in its Article 13-A, determines that during

[140] Conselho da Justiça Federal, IX Jornada de Direito Civil, Enunciado 678, 2022, available at: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf/view. *Enunciados* are texts proposed by the public and accepted by a committee set by a Court that will provide guidance to the Judiciary.
[141] Supremo Tribunal Federal, HC 108147/PR, 2012, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.
[142] *Lei nº 9.296, de 24 de Julho de 1996, Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal,* http://www.planalto.gov.br/ccivil_03/leis/l9296 htm.
[143] Supremo Tribunal Federal, HC 133148/ES, 2017, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4932933.
[144] *Decreto-Lei nº 3.689, de 3 de Outubro de 1941, Código de Processo Penal*, available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689 htm.

the investigation of some crimes[145], members of the Public Prosecutor's Office of the police chief may request, from any government agency or private company, registration data related to victims or suspects.

Another exception is found in Article 13-B of the Brazilian Criminal Procedure Code. If necessary for the prevention and repression of crimes related to human trafficking, the member of the Public Prosecutor's Office or the police chief may request, upon judicial authorisation, the companies providing telecommunications and/or telematics services to immediately make available the appropriate technical means – such as signs, information and others – that allow locating the victim or suspects of the ongoing crime. Judicial authorisation will depend on the conditions for access provided by the Brazilian Constitution, as outlined above, and in particular on whether such access is a subsidiary and exceptional measure[146]. If there is no judicial manifestation within twelve hours, the competent authority will request the companies providing telecommunications and/or telematics services to immediately make available the appropriate technical means, with immediate communication to the judge.

As a rule, the implementation of the interception measure is an activity undertaken by the police. However, it is possible that specialised services or other public authorities get involved in the procedure to guarantee the due execution of the measure. In such cases, they will have to follow the applicable legal framework. Involving other entities will only take place to guarantee the safety and efficiency of the measure, but should always respect the need of a judicial decision[147]. The result of the interception must be sent to the competent court, which stores the data in separate files to guarantee the secrecy of the communications (Article 8º). Nonetheless, the STF ruled that when the outcome of the interception is not stored in separate files, this amounts to a mere irregularity and does not entail the nullity of the interception[148] as long as it follows the legal procedure. Not following the legal provisions and obligations leads to the complete nullity of the interception. This means that the information must be excluded of the proceedings by motion of the prosecution or the interested party (Article 9º). This information must also not be used in other procedures[149].

Also, according to the Telephone Interception Law, a judicial order can authorise the recording of a specific environment or the capture of electronic, optical, or acoustic signals by a motion of the police authority or the Public Prosecutor. According to these procedures, interception without a judicial authorisation or for the purpose of unlawful activities constitutes a crime (Article 10).

The result of the interception may be used as evidence in other procedures – even administrative ones – and in the prosecution of other crimes. For instance, if the interception leads to the discovery of another crime, the results can be used as evidence even if the crime is not related to the one being initially investigated[150]. There are limits on using the interception results for another investigation procedure when the person involved in the new crime has privileged jurisdiction and the measure was authorised

[145] The exhaustive list of rights are: kidnapping and false imprisonment (Article 148), reduction to a condition analogous to slavery (Article 149), human trafficking (Article 149-A), extortion by restricting the victim's freedom (Article 158, paragraph 3º) and extortion by kidnapping (Article 159), in the Criminal Code (*Decreto-Lei nº 2.848, de 7 de Dezembro de 1940, Código Penal*, available at: http://www.planalto.gov.br/ccivil_03/decreto-, available at: lei/del2848compilado.htm), and children trafficking (Article 239), in the Child and Adolescent Statute (*Lei nº 8.069, de 13 de Julho de 1990, Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências*, available at: http://www.planalto.gov.br/ccivil_03/leis/l8069 htm).
[146] Supremo Tribunal Federal, HC 108147/PR, 2012, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.
[147] See Supremo Tribunal Federal, HC 96986/MG, 2012, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2649995. For instance, in this case, other police bodies were involved in the interception, since there were doubts about the involvement of police officers in the crime analysed.
[148] Supremo Tribunal Federal, HC 128102/SP, 2015, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4770762.
[149] Supremo Tribunal Federal, ARE 1316369/DF, 2022, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6129951.
[150] Supremo Tribunal Federal, HC 129678/SP, 2018, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4820467.

by a non-competent judge[151]. However, in regular cases, even interceptions authorised by different Courts can lead to evidence that can be used for the investigation of other crimes[152]. The main point is having the legal procedure followed, guaranteeing the rule of law and due process.
The waiving of telephone communication secrecy can also be requested by a federal or state Parliamentary Investigation Committee (*Comissão Parlamentar de Inquérito* – CPI in the Portuguese acronym), leading to the access of telecommunication metadata, which cannot be made publicly available[153]. The CPI is a procedure used by the National Congress to exercise its oversight powers. The CPI cannot judge or punish the ones being investigated, and cannot determine the interception of communications by itself — a court order is still necessary in this case.

It is important to highlight that the STF's, as well as the Brazilian Superior Tribunal of Justice (STJ)'s case law state that the constitutional protection of telecommunication data encompasses the mere data communication flow and not the data themselves. They have ruled that accessing the content of e-mails or private conversations retained in electronic devices that were gathered as evidence by investigation authorities, for instance, is allowed and a specific judicial order is not needed. For instance, if there is a judicial decision for search and seizure, the seized electronic equipment can be accessed by the investigation bodies [154].

In terms of investigation activities, one national expert explained that in the current national legal framework, no default classification is applied to data. However, considering that some case files might contain sensitive information or classified data (e.g., bank secrecy, attorney-client information), there might be some access limitations. There are no specific rules determining that the data subjects must be informed of the processing of their personal data. If the data subject is part of the criminal procedure (e.g., as a victim, suspect, or witness), the individual will be invited to provide information for the investigation. In this case, the data subject will know that their data are being processed. However, if a person is not invited to take part in the procedure, they will most probably not know that their personal data was processed.

On the international level, Brazil has been a signatory of the Budapest Convention since 2021, which was implemented in the Brazilian Legal System through the Legislative Decree n. 37/2021[155]. Although the first protocol is already in force, a working group of national experts are still discussing how to implement the second one. The signing of the Convention was highly celebrated by government authorities and the private sector. However, the process raised many concerns in Brazilian civil society such as the approval of the Convention in a shorter period than expected and without multistakeholder discussions on the subject; the absence of a general data protection law dedicated to criminal prosecution and public security activities; and the fact that the Convention was approved during the recast discussions of the Brazilian Criminal Procedure Code, which contains dedicated provisions regulating online investigation activities, data collection and cooperation between companies and public authorities[156]. A national expert stated that it is currently not possible to assess how the convention is being internalised by public authorities. Under the current government, the central authority for the oversight of the Convention is the Department of Asset Recovery and International Cooperation

[151] Supremo Tribunal Federal, MS 34751/CE, 2018, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5172309.
[152] Superior Tribunal de Justiça, REsp 1355432-SP, 2014, available at: https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=201202488103.
[153] Supremo Tribunal Federal, MS 25940, 2018, https://portal.stf.jus.br/processos/detalhe.asp?incidente=2376827.
[154] Superior Tribunal de Justiça, RHC 75800/PR, 2016, available at: https://processo.stj.jus.br/webstj/Processo/justica/jurisprudencia.asp?valor=201602394838.
Supremo Tribunal Federal, RHC 132062/RS, 2016, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4903009.
[155] *Decreto Legislativo nº 37 de 16 de Dezembro de 2021, Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001*, available at: https://legis.senado.leg.br/norma/35289207.
[156] Santos, B. M., *Convenção de Budapeste Sobre o Cibercrime na América Latina: uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México*, Derechos Digitales, 2022, available at: https://www.derechosdigitales.org/wp-content/uploads/PT-Ciberdelincuencia-2022.pdf, p. 21.

(*Departamento de Recuperação de Ativos e Cooperação Internacional* - DRCI in the Portuguese acronym), part of the Ministry of Justice and Public Safety[157].

Another important development related to international cooperation in the criminal field is the STF ruling that took place in February 2023 on the constitutionality of the Mutual Legal Assistance Treaty (MLAT) between Brazil and the United States[158]. Although the ruling confirmed the constitutionality of Decree n. 3,810/2001, which enacted the treaty, the STF understood that national authorities can request data directly from platforms based abroad[159]. According to the treaty, data requests should be intermediated by the Ministry of Justice and Public Safety, but the Court understood that the Brazilian judiciary can use other resources to obtain information from providers, such as direct subpoenas from companies in Brazil or rogatory letters, under the terms of Article 11, MCI. The rapporteur of the case, Justice [redacted], highlighted the low effectiveness of the cases that used the procedure established in the MLAT. He determined that the STF must inform the Legislative and Executive powers of the decision so that they can take action in relation to the discussions on the Data Protection Law for public security and criminal prosecution and new bilateral or multilateral agreements. [redacted] also highlighted that the MLAT rule should be adopted in a complementary way and only when it is impossible for national authorities to directly obtain information from digital platforms.

2.2.4 DATA SHARING

The Presidential Decree n. 10,046/19 sets rules on data governance and the sharing of personal data within the federal public authorities and establishes the *Cadastro Base Cidadão* (central national identification data base) and the Central Committee of Data Governance. The Decree's rules do not apply to situations where data is shared with supervisory boards for regulated professions and with the private sector as well as to data protected by fiscal secrecy under the control of the Ministry of Economy. However, it does apply to the remaining federal public authorities.

There are three possible levels of data sharing depending on the data classification: (i) broad, involving public data (Article 11); (ii) restrict, involving classified data but that are accessible by all public authorities that should follow the Decree (Article 12); and (iii) specific, also affecting classified data, but with public authorities having limited and specific access to the information (Article 14). New data bases can only be created when the possibilities of exploring existing ones are not enough (Article 10-A).

In view of the legal nature of the decree, it cannot be interpreted as amending or derogating from the LGPD. However, since its enactment, the decree has been criticised by many actors in Brazilian Civil Society, for not aligning with the LGPD[160]. Generally speaking, the decree does not consider the need for a legal basis for access to personal data by public bodies (and not only the data sharing); does not require the need to specify the purposes for which the data will be shared and with whom (which directly

[157] Vassallo, L., Kattah, E., Medeiros, D., 'Governo Lula vai rever cooperação do MPF com outros países; medica foi central na Lava Jato', *Estadão*, available at: https://www.estadao.com.br/politica/governo-lula-vai-rever-cooperacao-do-mpf-com-outros-paises-medida-foi-central-na-lava-jato/.
[158] Supremo Tribunal Federal, ADC 51, 2023, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379.
[159] Maia, F., 'STF: MLAT é constitucional, mas acordo não é a única forma de obtenção e prova', *Jota*, 23 February 2023, available at: https://www.jota.info/stf/do-supremo/stf-mlat-e-constitucional-mas-acordo-nao-e-a-unica-forma-de-obtencao-de-prova-23022023.
[160] Associação Data Privacy Brasil de Pesquisa, *Intervenção como amicus curiae - Ação Direta de Inconstitucionalidade nº 6.649*, available at: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755538665&prcID=6079238; Laboratório de Pesquisa em Políticas Públicas e Internet (LAPIN), *Nota Técnica - Derrubada dos Decretos 10.046/2019 e 10.047/2019 - Compartilhamento de dados no âmbito da administração pública federal*, available at: https://lapin.org.br/wp-content/uploads/2020/08/NT.-2-Derrubada-dos-Decretos-10.0462019-e-10.0472019.-LAPIN.pdf.

affects the analysis of necessity and proportionality); does not provide for traceability mechanisms, such as agreements or terms of authorisation; and does not allow the exercise of data subjects' rights.[161]

In September 2022, the STF ruled on two cases that focused on the indiscriminate data sharing in the Federal Public Administration, authorised by Decree n. 10,046/2019[162]. One of them discussed the situation where data from 76 million Brazilians from the National Traffic Department (*Departamento Nacional de Trânsito* - DENATRAN, in the acronym in Portuguese) would be shared with ABIN. In this opportunity, the Court clarified that the LGPD must be applied to data sharing within the scope of the decree. Thus, there are limits to the onward sharing of personal data between public entities. Negligent and abusive acts regarding the processing of personal data by public authorities are submitted to further liability procedures.

The Court also decided that data sharing within the scope of intelligence activities must observe specific legislation and parameters established in the ruling of ADI 6529, already mentioned above, and meet the public interest. Finally, the ruling declared the unconstitutionality of Article 22 of the decree, which organised the structure of the Central Data Governance Committee. The court granted 60 days for the public administration to adjust the composition of the committee, providing it with a plural and independent composition, in addition to creating rules for the accountability of infringing agents. This was complied with by Decree n. 11,266/2022.

2.2.5 OVERSIGHT MECHANISMS

The ANPD is the central body responsible for providing guidance on the interpretation and oversight of data protection rules (Article 55-K, sole paragraph and Article 55-J, XX, LGPD). The authority also holds the exclusive competence of applying administrative sanctions in such cases (Article 55-K, LGPD). Sanctions foreseen by the LGPD include powers to ensure compliance with data protection rules (e.g., binding orders of erasure of data basis, publishing the infraction) and pecuniary fines, as explained above.

The ANPD is also competent to request information regarding the processing of data by a public body, which may include audits over the processing of personal data held by it[163]. Even though the ANPD has limited oversight powers in the activities out of the scope of the law, the authority can request information to public bodies involved in such tasks, including data protection impact assessments. The ANPD can also publish opinions and recommendations for guaranteeing best practices of data protection for all kinds of data processing activities.

The oversight of activities out of the scope of the LGPD also involve the judicial supervision foreseen for surveillance activities such as interception of communications. As mentioned before, other bodies are also engaged in control activities, especially the TCU and the CGU.

The Brazilian system also allows the ANPD to apply sanctions to public bodies within the scope of LGPD, except for fines that can only be applied to private entities[164]. As a rule, for oversight purposes, the public body should be considered as the controller or processor, not a specific civil servant. However,

[161] Mendes, L. M., Gasiola, G. G., 'Inconstitucionalidade do Decreto 10.046: limites do compartilhamento de dados', *Conjur,* 14 September 2022, available at: https://www.conjur.com.br/2022-set-14/schertel-gasiola-compartilhamento-dados-setor-publico; Mendes, L. S., 'Laura Schertel Mendes: Democracia, poder informacional e vigilância', *OGlobo,* 13 August 2022, available at: https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml.

[162] Supremo Tribunal Federal, ADI 6649, 2022, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238, and Supremo Tribunal Federal, ADPF 695/DF, 2022, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693.

[163] Article 55-J, XVI, LGPD.

[164] Article 52, paragraph 3º, LGPD.

sanctioning the individual who works in the public administration is possible[165], if their behaviour falls under one of the provisions that would allow for this (e.g., selling data sets or modifying data) [166].

Taking into account that the ANPD is still relatively new, only recently did it announce that it will begin the sanctioning process and that it already has eight ongoing cases that could result in the application of penalties[167]. As explained by a national expert, a number of high-profile cases have also been examined since the start of its activities. For example, in a case involving data sharing between two companies providing chat applications [redacted], the ANPD worked together with the National Consumer Secretariat (*Secretaria Nacional do Consumidor* – SENACON in the Portuguese acronym), the Administrative Council for Economic Defense (*Conselho Administrativo de Defesa Econômica* – CADE in the Portuguese acronym) and with the Federal Public Prosecutor's Office (*Ministério Público Federal* – MPF in the Portuguese acronym). [redacted] Another example is the opinion given by the ANPD in the INEP case mentioned above. In recent years the ANPD also signed some important technical cooperation agreements such as with SENACON, CADE and the Superior Electoral Court (*Tribunal Superior Eleitoral* – TSE in the Portuguese acronym) to joint efforts to promote the proper application of the LGPD. Finally, the authority has also worked on a number of requests for advice and guidance issued by public authorities and private entities.

As mentioned throughout the analysis, apart from the ANPD, several other public bodies have competences that are also important to make sure that the public sector complies with the rights to privacy and to the protection of personal data, such as the Prosecutor's Office and the Judiciary. The CGU, for example is the competent authority to oversee the LAI application in the federal government. In the draft bill for the law for public security and criminal prosecution, CGU is also foreseen as the competent authority to oversee the application of the law. In relation to the Budapest Convention, a department within the Ministry of Justice and Public Safety is considered the central authority.

As for intelligence activities, internal control by the executive branch is carried out not only by the hierarchy of each agency, such as the ABIN, but also by the executive ministry to which it is part of. The external control is made by the judiciary and the legislative powers. The judiciary has a prior role, for example, by authorising actions such as telephone interception and breach of telephone communication secrecy. *A posteriori*, it will adjudicate lawsuits from citizens against the intelligence services and those initiated by the Public Ministry. The latter also has its role as a supervisor of the law and instance of external control of the police. Finally, the legislative power has the primary role of supervising the intelligence activities, both directly, through the Joint Commission for Control of Intelligence Activities of the National Congress (*Comissão Mista de Controle das Atividades de Inteligência do Congresso Nacional* – CCAI in the Portuguese ~~acronym), and through bodies tha~~t report to the Parliament, such as the TCU[169].

[165] Article 28, Decreto Lei 4657/42.

[166] Autoridade Nacional de Proteção de Dados, *Tratamento de Dados Pessoais pelo Poder Público*, 2022, available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf.

[167] Souza, N. 'ANPD mira em punições para garantir cumprimento da lei de dados', *Jota*, 6 February 2023, available at: https://www.jota.info/coberturas-especiais/protecao-de-dados/anpd-mira-em-punicoes-para-garantir-cumprimento-da-lei-de-dados-06022023.

[redacted]

Beyond the joint statement, the ANPD also issued technical opinions on the matter. (Autoridade Nacional de Proteção de Dados, *Nota Técnica n. 02/2021/CGTP/ANPD*, 2021, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NotaTecnicaANPDWhatsapp_ocr.pdf; Autoridade Nacional de Proteção de Dados, *Nota Técnica n. 19/2021/CGF/ANPD*, 2021, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTcnica19.2021.CGF.ANPD.pdf; Autoridade Nacional de Proteção de Dados, *Nota Técnica n. 49/2022/CGF/ANPD*, 2022, available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf).

[169] Gonçalves, J. B., 'Quem vigia os vigilantes? O controle da atividade de inteligencia no Brasil e o papel do Poder Legislativo', *Revista de Informação Legislativa, Brasília*, a. 47, n. 187, 2010, available at: https://www12.senado.leg.br/ril/edicoes/47/187/ril_v47_n187_p125.pdf.

2.3 DATA SUBJECT RIGHTS

2.3.1 AVAILABLE RIGHTS AND THEIR SCOPE OF APPLICATION

The LGPD defines a minimum set of rights that should be respected by organisations processing personal data. Data subjects[170] have the right to (i) receive a confirmation that the data is being processed; (ii) access their data; (iii) rectify incomplete, inaccurate or outdated data; (iv) anonymisation, blocking or erasure of excessive data or within the scope of unlawful data processing; (v) data portability[171], as long as it observes trade secrets; (vi) erasure of data processed under the consent of the data subject; (vii) obtain information about public and private entities with which the controller carried out shared use of data; (viii) obtain information about the possibility of not providing consent to a specific data processing and the consequences thereof; (ix) withdraw their consent; and (x) request the review of decisions based solely on automated means[172].

In order to exercise their rights, the data subject or their representative must contact the data controller and this request should have no costs for the data subject. After the data subject's request, the controller must immediately answer the request. However, if this is not possible, the data controller must communicate that it does not process data from the data subject and indicate, whenever possible, the correct controller; or indicate the factual or legal reasons that prevent the immediate fulfilment of the request. From this point onwards, there are no specific rules on how long a controller may take to answer such requests, except in the case of the right to access, which demands that the controller provides a simplified version of the information immediately or a complete declaration in up to 15 days. For other requests, further guidelines from the ANPD are required. While the regulation is not published, controllers must respond to data subjects immediately (Article, paragraph 3º, LGPD).

Only in cases of omission by the controller or when the information provided raises questions about the legitimacy of the processing, has the data subject the right to bring the matter to the ANPD (Article 18 paragraph 1º; Article 55-J, V, LGPD) or consumer protection authorities (Article 18, paragraph 8º, LGPD), if this applies.

Prior to the LGPD, the CPC already contained provisions related to the protection of data sets and consumers' registration. It states that the consumer has the right to access their information, as well as the right to know where they were collected. The consumer also has the right to update any unprecise data, guaranteeing the data quality. All kinds of registers and data sets must be transparent, and the establishment of these sets must be notified to the consumer, when the processing was not requested by them. The CPC intended to address the issues related to a developing market in Brazil, the services of credit protection.

As explained by a national expert, there is a legal and ongoing debate on the extent to which the data subject rights apply to activities that are not in the scope of the LGPD. This is part of the discussion in the National Congress about a specific legislation to regulate these activities in more detail, as mentioned above. National experts also stated that data subjects will not be notified about the data processing in law enforcement activities, unless they become a part of the procedure (*e.g.*, provide a testimony, being prosecuted). In relation to data processing by public authorities more broadly, national experts also highlighted that it is still not clear if the right to erasure applies to their activities, since public authorities must comply with legal obligations related to keeping information in public files for historical purposes or even to be used as evidence in court.

[170] Article 18 and 20, LGPD.
[171] The ANPD must develop further guidelines on the matter (Article 18, V, LGPD).
[172] The LGPD does not provide for the right to have automated decisions reviewed by a human.

2.3.2 REDRESS MECHANISMS

2.3.2.1 RIGHT TO COMPENSATION AND LIABILITY

Article 42, LGPD, states that a controller or processor who causes material or non-material damages, be it individual or collective, while processing data in violation of LGPD is obliged to repair it. Data subjects can claim compensation collectively when the violation has affected multiple data subjects. Article 52, paragraph 7º, LGPD, also mentions the possibility that, in cases of data breaches or non-authorised access to data, this violation may be subject of direct conciliation between the controller and the data subject, and, if there is no agreement, penalties may also be applied by the ANPD. The ANPD guidelines also suggest that, in cases of data breaches or fraud, the police authority should be notified[173].

In relation to the liability of the controller or processor, it is important to mention that there is an ongoing doctrinal discussion on whether strict liability (no need to prove intent or fault) or a subject liability (proof of intent or fault is needed) applies to incidents involving personal data. Similar to what is seen in the GDPR, case-law will establish the liability system that should be applied. This doubt only applies to the situations outside the scope of the consumer protection code, since it explicitly adopts strict liability.

In a recent controversial decision, the STJ decided that, despite being an undesirable failure in the processing of personal information, a data breach cannot, by itself, cause non-material damages. Thus, in any claim for compensation, it is necessary for the data subject to prove the actual damage caused by the data breach[174].

As regards harm related to national security activities and law enforcement, the judiciary is responsible for dealing with both individual and collective claims. The Brazilian judiciary is competent to judge an action when the defendant, regardless of their nationality, is domiciled in Brazil; when the obligation has to be fulfilled in Brazil; or the basis for the procedure is a fact that occurred or an act performed in Brazil (Article 21, Civil Procedure Code)[175].

2.3.2.2 HABEAS DATA

Habeas Data is a fundamental right and constitutional remedy that guarantees the right of access to personal data held by public authorities or by public data sets. It is a summary, civil and free of charge procedure, that demands the participation of a lawyer in the procedure, and that can be used to: (i) guarantee the access of data being processed in registers or in data sets maintained by public authorities or public data sets; or (ii) rectify data, when this is not done within a confidential procedure (Article 5, LXXII and LXXVII, Constitution).
Any natural or legal person can be a holder of the legal claim, if the data is related to that person, regardless of their nationality. The only exception to this rule is the case of a surviving partner. The remedy can only be used after there is an omission or a refusal of the public authority (or the owner of the public data set) to access or correct the data[176]. Thus, this redress mechanism requires that the data

[173] Autoridade Nacional de Proteção de Dados, *Petição de Titular*, 2022, available at: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contra-controlador-de-dados.
[174] Superior Tribunal de Justiça, *Titular de dados vazados deve comprovar dano efetivo ao buscar indenização, decide Segunda Turma*, 2023, available at: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/17032023-Titular-de-dados-vazados-deve-comprovar-dano-efetivo-ao-buscar-indenizacao--decide-Segunda-Turma.aspx.
[175] *Lei nº 13.105, de 16 de março de* 2015, *Código de Processo Civil*, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm.
[176] The *Habeas Data* cannot be used if the administrative authority has not refused access to the information (Superior Tribunal de Justiça, Súmula 2, 1990, available at: https://scon.stj.jus.br/SCON/SearchBRS?b=SUMU&livre=@NUM=2).

subject is aware of the data processing, what may not always be the case for purposes of law enforcement, national security or intelligence activities.

2.4 FUTURE LEGISLATION

Work on the development of laws to fill the gaps left by the LGPD is already underway. As explained above, there are already discussions in the National Congress related to a specific law focused on data processing in public security and criminal prosecution activities.

Another national expert described that the legislative power in Brazil is active at the moment, and there are several proposed bills on different topics within the digital rights' realm. Bills regulating social media platforms and content moderation are also rising in Brazil. Currently, there are various cases focused on content moderation within the TSE and the STF. Recently, the Ministry of Justice and Public Safety stated that, alongside the Communications Secretariat (*Secretaria de Comunicação* – SECOM in the Portuguese acronym), a bill on the regulation of social media platforms is being developed[177].

Finally, taking into account the ANPD's regulatory agenda, several topics will start to be addressed in the near future. This comes after the development of the internal regulatory framework needed to guarantee the start of sanctioning activities by the authority.

2.5 OVERVIEW OF RELEVANT LEGISLATION

Public authority activity	Laws applied	Oversight	Redress mechanisms
Intelligence purposes	Law n. 9883/99 Constitution	Legislative bodies	N/A
Law enforcement purposes	Telephone Interception Law Criminal Procedures Code	Judiciary	Judiciary
General rules of data access	LGPD Constitution Habeas Data Law Decree n. 10.046/19	ANPD Judiciary Constitutional control	ANPD Judiciary

[177] Índio do Brasil, C., 'Dino: governo prepara PL para regulamentação das redes sociais', *Agência Brasil*, 13 March 2023, available at: https://agenciabrasil.ebc.com.br/politica/noticia/2023-03/dino-governo-prepara-pl-para-regulamentacao-das-redes-sociais?utm_source=meio&utm_medium=email.

3 CONCLUSION

This study has assessed the relevant legal frameworks and practices around governmental access for Brazil. The paragraphs below summarise the main findings of the report.

Brazil has a fairly new legal data protection framework. Recent years' achievements include the approval of a general law, the creation of the ANPD, the enshrinement of data protection as a fundamental right in the Brazilian Constitution, ascending to the Budapest Convention, and the development of a data protection culture through jurisprudence, doctrine and guidance documents. The LGPD presents a structured system to guarantee the rights to privacy and to the protection of personal data, with a very similar approach to the GDPR.

While the LGPD presents a solid and extensive data protection framework, comprehensive rules on national security, public security, national defence, and criminal procedure need to be developed.Criminal procedures do have to comply with a fragmented, but robust, legal framework. Consequently, the majority of surveillance measures are overseen and controlled by judicial authorities (e.g., the need for a judicial order for the interception of telecommunications or adjudicating a lawsuit). Data processing for national security and national defence, on the other hand, has less rigid legal limits, with the judiciary and the legislature as their main oversight bodies. As seen, the LGPD determines that its principles and data subject rights must be included in the specific legislation to be developed, in addition to providing for proportional and strictly necessary measures to serve the public interest, subject to due process of law. National experts are of the opinion that these provisions already apply to activities outside of the scope of the LGPD. However, a specific law providing details of the application of the right to data protection in these cases is crucial to protect data subjects and provide legal certainty. Furthermore, it is still to be seen how the ANPD will deal with these exceptions, in view of its specific competence in these cases to issue technical opinions and recommendations, as well as to request reports on the impact on the protection of personal data.

ANNEX 1 – QUESTIONNAIRE

Brazil

General questions

1. How are necessity and proportionality evaluated when public authorities have access to personal data? Are there any legal obligations on this matter (e.g., need for publishing the assessment)? In recent years, there has been news regarding the monitoring of public employees by Brazilian public authorities. Has this issue been addressed? How?

2. Are there any cases/situations where a judicial decision is not needed for a government body to have access to personal data for investigation purposes or national security?

3. According to the Constitution, fundamental rights are guaranteed to foreigners living in Brazil. Do foreigners, including EU citizens, who live outside of Brazil also have their rights guaranteed?

4. Are there legally binding safeguards for the processing of personal data for intelligence and law enforcement purposes?

5. Brazil has been working on different initiatives to guarantee the digitalisation of identities and develop smart cities. Are safeguards being discussed in these projects? Who is participating in these discussions?

6. Are there any proposed bills or paradigmatic court decisions regarding the use of malware for lawful surveillance practices?

7. Some sensitive topics (e.g., government access for intelligence purposes) depend on presidential acts. Does this model bring a lot of legal uncertainty to the system? What has been the main understanding regarding the exceptions of data usage for intelligence purposes?

8. Are there any bills to address cybersecurity minimum grounds that should be followed in the country? Did the adoption of the Budapest Convention make any significant changes in the Brazilian regulatory framework? Does this new regulatory framework avoid the usage of unsafe surveillance technologies by the government?

9. How is personal data protected in the processing for criminal persecution, national defence and security or public safety, considering the existing legal gap (e.g., the fact that the Brazilian Data Protection law does not apply to these cases)?

10. What are the existing rules on data sharing from one Brazilian public authority to another (onward sharing)? How do data subject rights apply in these situations?

11. What are the existing rules regarding data transfers from Brazil to other (third) countries, especially when the personal data was collected or accessed by a Brazilian public authority?

Data subject rights

12. Considering the secrecy of the police investigation, how and when is the data subject informed about the collection of his/her personal data for crime investigation or national

security purposes?

13. What oversight is there for the access of personal data by regulatory agencies (*agências reguladoras*, i.e., ANATEL)? Are there any redress mechanisms for the data subject to guarantee her/his data subject rights?

Case law

14. Were the last decisions of the Superior Court of Justice and Supreme Court of Justice enough to guarantee the respect of data protection principles in activities out of the scope of the Brazilian Data Protection Law (e.g., public, and national security)?

15. How are the regulatory framework and national practices adapting to the recent court decisions regarding the use of facial technology in public spaces?

Remedies and redress mechanisms

16. The Brazilian Data Protection Supervisory Authority just turned independent. How do you evaluate the work of the SA until now? Did the administrative change make any significant difference in its work?

17. Is it possible to consider that the Brazilian SA has focused more on normative work following its regulatory agenda than in evaluating specific cases? What is your opinion on this choice?

ANNEX 2 – SOURCES OF INFORMATION

General Part

Case law

CJEU

Judgment of the Court (Grand Chamber) of 20 September 2022, C-339/20 VD and C-397/20 SR, ECLI:EU:C:2022:703.

Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D v The Commissioner of the Garda Síochána, and Others*, C-140/20, ECLI:EU:C:2022:258.

Judgment of the Court (Tenth Chamber) of 21 October 2021, *the Spetsializiran nakazatelen sad*, C-350/21, ECLI:EU:C:2021:874.

Judgment of the Court (Eighth Chamber) of 2 September 2021, *Telekom Deutschland GmbH v Bundesrepublik Deutschland*, C-794/19.

Judgment of the Court (Grand Chamber) of 22 June 2021, *Ordre des barreaux francophones et germanophone and others*, C-512/18, ECLI:EU:C:2021:505.

Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, ECLI:EU:C:2021:152.

Judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790.

Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18, ECLI:EU:C:2020:791.

Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, ECLI:EU:C:2020:559.

Judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, ECLI:EU:C:2016:970.

Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14 ECLI:EU:C:2015:650.

Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238.

Judgment of the Court (Fourth Chamber) of 17 October 2013, *Michael Schwarz v. Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670.

Judgment of the Court (Grand Chamber), 26 February 2013, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2013:107.

Judgment of the Court (Grand Chamber) of 16 December 2008, *Satakunnan and Satamedia Oy*, C-73/07, ECLI:EU:C:2008:727.

Judgment of the Court of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596.

Judgment of the Court (Grand Chamber) of 20 September 2022, *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH.SpaceNet*, C-793/19, ECLI:EU:C:2022:702.

ECtHR

Judgement of 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, nos. 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013.

Judgement of 4 December 2015, *Zakharov v. Russia*, no. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306.

Judgement of 18 May 2010, *Kennedy v. the United Kingdom*, no. 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905.

Judgement of 2 December 2008, *K.U. v. Finland*, no. 2872/02, ECLI:CE:ECHR:2008:1202JUD000287202.

Judgement of 29 June 2006, *Weber and Saravia*, no. 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400.

Judgement of 4 March 2004, *M.C. v. Bulgaria*, no. 39272/98, ECLI:CE:ECHR:2003:1204JUD003927298.
Judgement of 4 May 2000, *Rotaru v Romania*, no. 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195.
Judgement of 16 February 2000, *Amann v. Switzerland*, no. 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895.
Judgement of 28 October 1998, *Osman v. United Kingdom*, no. 23452/94, ECLI:CE:ECHR:1998:1028JUD002345294.
Judgement of 24 April 1990, *Huvig v. France*, no. 11105/84.
Judgement of 26 March 1987, *Leanderv. Sweden*, no. 9248/81, ECLI:CE:ECHR:1987:0326JUD000924881.
Judgement of 2 August 1984, *Malone v. the UK*, no. 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179.
Judgement of 26 April 1979, *The Sunday Times v. the UK*, no. 6538/74, ECLI:CE:ECHR:1979:0426JUD000653874.

Opinions

Opinion of the Court (Grand Chamber) of 26 July 2017, Opinion 1/15 on the EU-Canada PNR Agreement, ECLI:EU:C:2017:592.

Other sources

European Data Protection Board (2023), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Version 2.0.
European Data Protection Board (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*.
European Data Protection Board (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*.
European Data Protection Supervisor (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit*.
European Data Protection Supervisor (2021), *Case Law Digest: Transfers of personal data to third countries*.
European Data Protection Supervisor (2019), *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*.
European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg, 2018.
Gerards, J., 'How to improve the necessity test of the European Court of Human Rights', *International Journal of Constitutional Law*, Vol. 11, No 2, April 2013, pp. 466–490.
Lenaerts, K., 'Limits on Limitations: The Essence of Fundamental Rights in the EU', *German Law Journal*, Vol. 20, pp. 779-793, Cambridge University Press, 2019.
Brkan, M., 'The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning', *German Law Journal*, Vol. 20, pp. 864-883, Cambridge University Press, 2019.
Tridimas, T., Gentile, G., 'The essence of Rights: An Unreliable Boundary?', *German Law Journal*, Vol. 20, pp. 794–816, Cambridge University Press, 2019.
Tracol, X., 'Ministerio fiscal: Access of public authorities to personal data retained by providers of electronic communications services', *European Data Protection Law Review*, Vol. 5, No 1, pp. 127-135.

Brazil

Case law

Superior Tribunal de Justiça, REsp 1355432-SP, 2014, available at: https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=201202488103.

Superior Tribunal de Justiça, RHC 75800/PR, 2016, available at: https://processo.stj.jus.br/webstj/Processo/justica/jurisprudencia.asp?valor=201602394838.

Superior Tribunal de Justiça, Súmula 2, 1990, available at: https://scon.stj.jus.br/SCON/SearchBRS?b=SUMU&livre=@NUM=2.

Supremo Tribunal Federal, ADC 51, 2023, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379.

Supremo Tribunal Federal, ADI 5527, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282.

Supremo Tribunal Federal, ADI 6387, 2020, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165.

Supremo Tribunal Federal, ADI 6529, 2021, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837.

Supremo Tribunal Federal, ADI 6649, 2022, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238.

Supremo Tribunal Federal, ADPF 403, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500.

Supremo Tribunal Federal, ADPF 695/DF, 2022, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693.

Supremo Tribunal Federal, ARE 1316369/DF, 2022, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6129951.

Supremo Tribunal Federal, HC 96986/MG, 2012, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2649995.

Supremo Tribunal Federal, HC 108147/PR, 2012, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.

Supremo Tribunal Federal, HC 128102/SP, 2015, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4770762.

Supremo Tribunal Federal, HC 133148/ES, 2017, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4932933.

Supremo Tribunal Federal, HC 129678/SP, 2018, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4820467.

Supremo Tribunal Federal, MS 25940, 2018, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2376827.

Supremo Tribunal Federal, MS 34751/CE, 2018, available at https://portal.stf.jus.br/processos/detalhe.asp?incidente=5172309.

Supremo Tribunal Federal, RE 587970/SP, 2017, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2621386.

Supremo Tribunal Federal, RE 1018911/RR, 2021, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5115280.

Supremo Tribunal Federal, RHC 132062/RS, 2016, available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4903009.

Tribunal de Contas da União, Processo n. 014.760/2021-5, 2022.

Legislation

Constituição da República Federativa do Brasil de 1988, available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

Decreto-Lei nº 2.848, de 7 de Dezembro de 1940, Código Penal, available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

Decreto-Lei nº 3.689, de 3 de Outubro de 1941, Código de Processo Penal, available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

Decreto-Lei n. 4.657, de 4 de setembro de 1942, Lei de Introdução às Normas do Direito Brasileiro, 1942, available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm.

Decreto Legislativo nº 37 de 16 de Dezembro de 2021, Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001, available at: https://legis.senado.leg.br/norma/35289207.

Decreto nº 4.376, de 13 de Setembro de 2022, Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei no 9.883, de 7 de dezembro de 1999, e dá outras providências, available at: http://www.planalto.gov.br/ccivil_03/decreto/2002/d4376.htm.

Decreto nº 9.637, de 26 de Dezembro de 2018, Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional, available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm#:~:text=DECRETO%20N%C2%BA%209.637%2C%20DE%2026,regulamenta%20o%20disposto%20no%20art.

Decreto nº 10.222, de 5 de fevereiro de 2020, Aprova a Estratégia Nacional de Segurança Cibernética, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

Decreto nº 11.348, de 1º de Janeiro de 2023, Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública e remaneja cargos em comissão e funções de confiança, available at: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm.

Lei Complementar nº 75, de 20 de maio de 1993, Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União, available at: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp75.htm.

Lei nº 8.069, de 13 de Julho de 1990, Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências, available at: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm.

Lei nº 8.078, de 11 de Setembro de 1990, Dispõe sobre a proteção do consumidor e dá outras providências, available at: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

Lei nº 9.296, de 24 de Julho de 1996, Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal, available at: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

Lei nº 9.784, de 29 de Janeiro de 1999, Regula o processo administrativo no âmbito da Administração Pública Federal, available at: http://www.planalto.gov.br/ccivil_03/leis/l9784.htm#:~:text=LEI%20N%C2%BA%209.784%20%2C%20DE%2029%20DE%20JANEIRO%20DE%201999.&text=Regula%20o%20processo%20administrativo%20no%20%C3%A2mbito%20da%20Administra%C3%A7%C3%A3o%20P%C3%BAblica%20Federal.

Lei nº 9.883, de 7 de Dezembro de 1999, Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências, available at: https://www.planalto.gov.br/ccivil_03/leis/l9883.htm.

Lei nº 9.986, de 18 de Julho de 2000, Dispõe sobre a gestão de recursos humanos das Agências Reguladoras e dá outras providências, available at: http://www.planalto.gov.br/ccivil_03/leis/l9986.htm.

Lei nº 10.406, de 10 de Janeiro de 2002, Institui o Código Civil, available at: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm.

Lei nº 12.414, de 9 de Junho de 2011, Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.

Lei nº 12.527, de 18 de Novembro de 2011, Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e

dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências, available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

Lei nº 12.965, de 23 de Abril de 2014, Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Lei nº 13.105, de 16 de março de 2015, Código de Processo Civil, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm.

Lei nº 13.445, de 24 de Maio de 2017, Institui a Lei de Migração, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445.htm#:~:text=Institui%20a%20Lei%20de%20Migra%C3%A7%C3%A3o.&text=Art.,pol%C3%ADticas%20p%C3%BAblicas%20para%20o%20emigrante.

Lei nº 13.709, de 14 de Agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Lei nº 13.853, de 9 de Julho de 2019, Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm.

Lei nº 14.460, de 25 de Outubro de 2022, Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14460.htm.

Other sources

Amnesty International (2023), *Amnesty International Report 2022/23: The State of the World's Human Rights*, available at: https://www.amnesty.org/en/location/americas/south-america/brazil/report-brazil/.

Amnesty International, *Police Violence*, available at: https://www.amnesty.org/en/what-we-do/police-brutality/.

[redacted]

Associação Data Privacy Brasil de Pesquisa, *Intervenção como amicus curiae - Ação Direta de Inconstitucionalidade nº 6.649*, https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755538665&prcID=6079238.

Autoridade Nacional de Proteção de Dados - ANPD, available at: https://www.gov.br/anpd/pt-br.

Autoridade Nacional de Proteção de Dados, *ANPD divulga balanço de acompanhamento e execução da Agenda Regulatória 2021/2022 referente ao 2º semestre de 2022*, 16 January 2023, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-balanco-semestral-de-acompanhamento-e-execucao-da-agenda-regulatoria-2021-2022.

Autoridade Nacional de Proteção de Dados, *ANPD e Ministério da Justiça e Segurança Pública editam portaria conjunta*, 13 February 2023, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-ministerio-da-justica-e-seguranca-publica-editam-portaria-conjunta.

Autoridade Nacional de Proteção de Dados, *ANPD manifesta-se sobre divulgação de microdados do Eenem e Censo Escolar pelo INEP*, 17 Mai 2022, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-manifesta-se-sobre-divulgacao-de-microdados-do-enem-e-censo-escolar-pelo-inep.

Autoridade Nacional de Proteção de Dados, *ANPD publica Agenda de Avaliação de Resultados Regulatórios*, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-de-avaliacao-de-resultados-regulatorios.

Autoridade Nacional de Proteção de Dados (2021), *Nota Técnica n. 02/2021/CGTP/ANPD*, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NotaTecnicaANPDWhatsapp_ocr.pdf.

Autoridade Nacional de Proteção de Dados (2021), *Nota Técnica n. 19/2021/CGF/ANPD*, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTcnica19.2021.CGF.ANPD.pdf.

Autoridade Nacional de Proteção de Dados (2022), *Nota Técnica n. 49/2022/CGF/ANPD*, available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf.

Autoridade Nacional de Proteção de Dados (2022), *Petição de Titular*, available at: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contra-controlador-de-dados.

Autoridade Nacional de Proteção de Dados, *Portaria ANPD n. 35, de 4 de novembro de 2022, Agenda Regulatória para o biênio 2023-2024*, available at: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885.

Autoridade Nacional de Proteção de Dados, *Resolução CD/ANPD n. 4, de 24 de fevereiro de 2023, Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas*, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf.

Autoridade Nacional de Proteção de Dados, *Resolução CD/ANPD n. 5, de 13 de março de 2023, Agenda de Avaliação de Resultado Regulatório para o período 2023-2026*, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-de-avaliacao-de-resultados-regulatorios/RESOLUON5ARR.pdf.

Autoridade Nacional de Proteção de Dados (2022), *Tratamento de Dados Pessoais pelo Poder Público*, available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf.

Belli, L. et al (2023), *Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil digitalmente soberano*, available at: https://cyberbrics.info/ciberseguranca-uma-visao-sistemica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/.

Bioni, B. R., Silva, P. G. F., Martins, P. B., 'Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso', *Cadernos técnicos da CGU: coletânea de artigos da pós-graduação em ouvidoria pública*, 2022, pp. 8 –19.

Câmara dos Deputados do Brasil, *Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal*, 2019, available at: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf.

Câmara dos Deputados, PL 1515/2022, available at: https://www.camara.leg.br/propostas-legislativas/2326300.

Campos, A. C., 'Drones são adotados por 63% das forças de segurança no Brasil', *Agência Brasil*, 29 March 2023, available at: https://agenciabrasil.ebc.com.br/geral/noticia/2023-03/drones-sao-adotados-por-63-das-forcas-de-seguranca-no-brasil.

Cano, I., 'Public Security Policies in Brazil: Attempts to Modernize and Democratize versus the War on Crime', *Sur*, Number 5, Year 3 , 2006, available at: https://sur.conectas.org/en/public-security-polices-brazil/.

[redacted]

Conselho da Justiça Federal, *IX Jornada de Direito Civil, Enunciado 678*, 2022, available at: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf/view.

Conselho Nacional dos Procuradores-Gerais, *Manual Nacional do Controle Externo da Atividade Policial*, 2009, available at: http://www.mpsp.mp.br/portal/page/portal/cao_criminal/CAOCri_ControleExtAtivPol/Manual%20Nacional%20do%20Controle%20Externo%20da%20Atividade%20Policial.pdf.

Controladoria-Geral da União, *CGU e ANPD firmam parceria para cooperação entre os órgãos*, 17 February 2023, available at: https://www.gov.br/cgu/pt-br/assuntos/noticias/2023/02/cgu-e-anpd-firmam-parceria-para-cooperacao-entre-os-orgaos.

Council of Europe, *Brazil and the Data protection Commission of Gabon to join the Committee of Convention 108 as observers*, 12 October 2018, available at: https://www.coe.int/en/web/data-protection/-/brazil-and-the-data-protection-commission-of-gabon-to-join-the-committee-of-convention-108-as-observers-.

Council of Europe, *Brazil accedes to the Convention on Cybercrime and six States sign the new Protocol on e-evidence*, 30 November, 2022, available at: https://www.coe.int/en/web/cybercrime/-/brazil-accedes-to-the-convention-on-cybercrime-and-six-states-sign-the-new-protocol-on-e-evidence.

[redacted]

Fiquem Sabendo, INSPER, FGV, *Impactos da LGPD nos pedidos de LAI ao governo federal*, 2022, available: at https://drive.google.com/file/d/1LfYUOiNVyxC1LAL3U_fGwWSCNL7t16ap/view.

Gonçalves, J. B., 'Quem vigia os vigilantes? O controle da atividade de inteligencia no Brasil e o papel do Poder Legislativo', *Revista de Informação Legislativa*, Brasília, Vol 47, No 187, 2010, available at: https://www12.senado.leg.br/ril/edicoes/47/187/ril_v47_n187_p125.pdf.

Grossman, L. O., 'ANPD recebeu 120 indicações para Conselho Nacional de Proteção de Dados', *Convergência Digital*, 26 March 2021, available at: https://www.convergenciadigital.com.br/Seguranca/ANPD-recebeu-120-indicacoes-para-Conselho-Nacional-de-Protecao-de-Dados-56510.html?UserActiveTemplate=site.

Human Rights Council, A/HRC/27/3, *The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights*, available at https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.ohchr.org%2Fsites%2Fdefault%2Ffiles%2FDocuments%2FIssues%2FDigitalAge%2FA-HRC-27-37_en.doc%23%3A~%3Atext%3DIn%2520its%2520resolution%252068%252F167%2Ccommunications%2520and%2520the%2520collection%2520of&wdOrigin=BROWSELINK.

Hurel, L. M., 'Cybersecurity in Brazil: An analysis of the National Strategy', *Igarapé Institute*, 2021, available at: https://igarape.org.br/wp-content/uploads/2021/04/SP-54_Cybersecurity-in-Brazil.pdf.

Hurel, L. M., Lobato, L. C., 'A Strategy for Cybersecurity Governance in Brazil', *Igarapé Institute*, 2019, available at: https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf.

Índio do Brasil, C., 'Dino: governo prepara PL para regulamentação das redes sociais', *Agência Brasil*, 13 March 2023, available at: https://agenciabrasil.ebc.com.br/politica/noticia/2023-03/dino-governo-prepara-pl-para-regulamentacao-das-redes-sociais?utm_source=meio&utm_medium=email.

Instituto Igarapé, *Documents - Portal Brasileiro da Cibersegurança*, available at: https://ciberseguranca.igarape.org.br/en/category/documents/.

Instituto Igarapé, *Implementação de Tecnologias de Vigilância no Brasil e na América Latina*, 2022, available at: https://igarape.org.br/wp-content/uploads/2022/12/Implementacao-de-tecnologias-de-vigilancia-no-brasil-e-na-america-latina.pdf.

Instituto Igarapé, *Reconhecimento Facial no Brasil*, available at https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/.

Instituto Igarapé, 'The Brazilian Cybersecurity Ecosystem', *Portal Brasileiro de Cibersegurança*, available at: https://ciberseguranca.igarape.org.br/en/ecosystem/.

International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI)*, 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

International Telecommunication Union (ITU), *Global Cybersecurity Index (CGI)*, 2020, available at available at: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

Laboratório de Pesquisa em Políticas Públicas e Internet (LAPIN), *Nota Técnica - Derrubada dos Decretos 10.046/2019 e 10.047/2019 - Compartilhamento de dados no âmbito da administração*

pública federal, https://lapin.org.br/wp-content/uploads/2020/08/NT.-2-Derrubada-dos-Decretos-10.0462019-e-10.0472019.-LAPIN.pdf.
Maia, F., 'STF: MLAT é constitucional, mas acordo não é a única forma de obtenção e prova', *Jota*, 23 February 2023, available at: https://www.jota.info/stf/do-supremo/stf-mlat-e-constitucional-mas-acordo-nao-e-a-unica-forma-de-obtencao-de-prova-23022023.
Mendes, L. S., 'A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis', *Caderno Especial LGPD*, São Paulo, RT, November 2019, pp. 35-56.
Mendes, L. S., 'Democracia, poder informacional e vigilância', *OGlobo*, 13 August 2022, available at: https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml.
Mendes, L. M., Gasiola, G. G., 'Inconstitucionalidade do Decreto 10.046: limites do compartilhamento de dados', *Conjur*, 14 September 2022, available at: https://www.conjur.com.br/2022-set-14/schertel-gasiola-compartilhamento-dados-setor-publico.
Ministério da Defesa, *Estratégia Nacional de Defesa*, 2008, available at: http://livroaberto.ibict.br/bitstream/1/605/2/Estrategia-Nacional-de-Defesa.pdf.
Ministério da Justiça e Segurança Pública, *Governo lança debate público sobre regulamentação de lei e anteprojeto*, 28 January 2015, available at: https://www.gov.br/mj/pt-br/assuntos/noticias/governo-lanca-debate-publico-sobre-regulamentacao-de-lei-e-anteprojeto.
Nunes, P., Silva, M. R., Oliveira, S. R. de, 'A Rio of cameras with selective eyes: the use of facial recognition by the Rio de Janeiro state police', *O Panóptico*, 2022, available at: https://opanoptico.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b_english.pdf.
OECD, *OECD takes first step in accession discussions with Argentina, Brazil, Bulgaria, Croatia, Peru and Romania*, 25 January 2022, available at: https://www.oecd.org/newsroom/oecd-takes-first-step-in-accession-discussions-with-argentina-brazil-bulgaria-croatia-peru-and-romania.htm.
Parentoni, L., Lima, H. 'Proteção de Dados Pessoais no Brasil: Antinomias Internas e Aspectos Internacionais', *Direito & Internet: Sistema de Proteção de Dados Pessoais*, 2019, pp. 483-512.
Pereira, A. B. C., Cabral, S., Reis, P. R. da C., 'Accountability interna em forças policiais: explorando os fatores associados ao desempenho de uma corregedoria de polícia militar', *Organizações & Sociedade*, 27(92), 2020, available at: https://doi.org/10.1590/1984-9270922.
Petrocilo, C., Lacerda, L., Seto, G., 'Prefeitura revê, mas não desiste de programa de reconhecimento facial em SP', *Folha de São Paulo*, 2 December 2022, available at: https://www1.folha.uol.com.br/cotidiano/2022/12/suspenso-apos-criticas-projeto-de-reconhecimento-facial-sera-mantido-diz-nunes.shtml.
Presidência da República, *Estratégia de Segurança da Informação e Comunicações (SIC) e de Segurança Cibernética da Administração Pública Federal (APF)*, 2013, available at: https://www.gov.br/gsi/pt-br/assuntos/noticias/2015/estrategia-de-seguranca-da-informacao-e-comunicacoes-sic-e-de-seguranca-cibernetica-da-administracao-publica-federal-apf.
Presidência da República, *Livro Verde Segurança Cibernética no Brasil*, 2010, available at https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf.
[redacted]
Rebello, A., 'O mecenas', *The Intercept*, 5 April 2023, available at https://www.intercept.com.br/2023/04/05/delegado-waldir-torrou-r-30-milhoes-em-reconhecimento-facial-para-cidades-que-sequer-tem-saneamento-em-goias/.
[redacted]
Santos, B. M., 'Convenção de Budapeste Sobre o Cibercrime na América Latina: uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México', *Derechos Digitales*, 2022, available at https://www.derechosdigitales.org/wp-content/uploads/PT-Ciberdelincuencia-2022.pdf.

Souza, C. A., Viola, M., Lemos, R., 'Brazil's Internet Bill of Rights: A Closer Look', *Instituto de Tecnologia e Sociedade*, 2018, available at https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa__pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf'

Souza, N., 'ANPD mira em punições para garantir cumprimento da lei de dados', *Jota*, 6 February 2023, available at https://www.jota.info/coberturas-especiais/protecao-de-dados/anpd-mira-em-punicoes-para-garantir-cumprimento-da-lei-de-dados-06022023,

Superior Tribunal de Justiça, *Titular de dados vazados deve comprovar dano efetivo ao buscar indenização, decide Segunda Turma*, 2023, available at https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/17032023-Titular-de-dados-vazados-deve-comprovar-dano-efetivo-ao-buscar-indenizacao--decide-Segunda-Turma.aspx.

Supremo Tribunal Federal, *STF confirma limitações ao compartilhamento de dados do Sisbin*, 15 October 2021, available at https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=474835&ori=1.

Le Temps, *Une opération policière dans une favela de Rio fait au moins 22 morts*, 24 May 2022, available at https://www.letemps.ch/monde/ameriques/une-operation-policiere-une-favela-rio-22-morts.

Tire meu Rosto da Sua Mira (2022), *Open Letter to Ban the Use of Digital Facial Recognition Technologies in public Security*, available at https://tiremeurostodasuamira.org.br/en/open-letter/.

United Nations, *Brazil: UN experts decry acts of racialised police brutality*, 6 July 2022, available at: https://www.ohchr.org/en/press-releases/2022/07/brazil-un-experts-decry-acts-racialised-police-brutality.

Vassallo, L., Kattah, E., Medeiros, D., 'Governo Lula vai rever cooperação do MPF com outros países; medica foi central na Lava Jato', *Estadão*, available at https://www.estadao.com.br/politica/governo-lula-vai-rever-cooperacao-do-mpf-com-outros-paises-medida-foi-central-na-lava-jato/.

Vlois, R., 'Tecnoautoritarismo e o bloqueio de provedores por descumprimeinto de ordens judiciais no Brasil', *Nexo Jornal*, 26 January 2023, available at https://pp.nexojornal.com.br/opiniao/2023/Tecnoautoritarismo-e-o-blockio-de-provedores-por-descumprimento-de-ordens-judiciais-no-Brasil.

Wimmer, M., 'O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público', *Tratado de Proteção de Dados Pessoais*, 1. ed., Rio de Janeiro, Forense, 2021. pp. 271–288.

ANNEX 3 – ACRONYMS AND ABBREVIATIONS

General

Acronyms and Abbreviations	Meaning
CJEU	Court of Justice of the European Union
CoE	Council of Europe
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
Convention 108+	Convention 108+ on protection of individuals with regard to the Processing of Personal Data
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EU	European Union
EU-Charter	Charter of Fundamental Rights of the European Union
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
HRC	United Nations Human Rights Council
HRW	Human Rights Watch
ICCPR	International Covenant on Civil and Political Rights
OECD	Organisation for Economic Co-operation and Development
SA(s)	Supervisory authority(-ies)
UDHR	Universal Declaration of Human Rights
UN	United Nations

Brazil

Acronyms and Abbreviations	Meaning
ABIN	Brazilian Agency of Intelligence (*Agência Brasileira de Inteligência)*
ANPD	Brazilian Data Protection Supervisory Authority (*Autoridade Nacional de Proteção de Dados*)
ARR	Regulatory Results Assessment (*Avaliação de Resultados Regulatórios*)
CADE	Administrative Council of Economic Defense – Brazilian Antitrust Body (*Conselho Administrativo de Defesa Econômica*)
CCAI	Joint Commission for Control of Intelligence Activities of the National Congress (*Comissão Mista de Controle das Atividades de Inteligência do Congresso Nacional*
CGU	Office of the Comptroller General (*Controladoria Geral da União*)
CPI	Parliamentary Investigation Committee *(Comissão Parlamentar de Inquérito*)
CDC	Consumer Protection Code (*Código de Defesa do Consumidor)*
CNPD	National Council for Data Protection and Privacy (*Conselho Nacional de Proteção de Dados Pessoais e da Privacidade*)
DENATRAN	National Traffic Department (*Departamento Nacional de Trânsito*)

DRCI	Department of Asset Recovery and International Cooperation (*Departamento de Recuperação de Ativos e Cooperação Internacional)*
ENEM	National Examination of Secondary Education (*Exame Nacional do Ensino Médio)*
INEP	National Institute of Educational Studies and Research Anísio Teixeira (*Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira)*
LAI	Access to Public Information Law (*Lei de Acesso à Informação*)
LGPD	Brazilian Data Protection Law (*Lei Geral de Proteção de Dados*)
LINDB	Law of Introduction to the Rules of Brazilian Law (*Lei de Introdução às Normas do Direito Brasileiro*)
MCI	Civil Rights Framework for the Internet in Brazil (*Marco Civil da Internet*)
MLAT	Mutual Legal Assistance Treaty
MPF	Federal Public Prosecutor's Office (*Ministério Público Federal*)
OECD	Organisation for Economic Co-operation and Development
SBI	Brazilian Intelligence System (*Sistema Brasileiro de Inteligência*)
SECOM	Communications Secretariat (*Secretaria de Comunicação*)
SENACON	National Consumer Secretariat (*Secretaria Nacional do Consumidor*)
STF	Supreme Federal Court (*Supremo Tribunal Federal*)
STJ	Superior Court of Justice (*Superior Tribunal de Justiça*)
TCU	Federal Court of Accounts (*Tribunal de Conats da União*)
TSE	Superior Electoral Court (*Tribunal Superior Eleitoral*)