The State of Communication Privacy Law in Brazil

Katitza Rodriguez,
International Rights Director
(EFF)

Veridiana Alimonti,
Latin American Senior Policy
Analyst (EFF)

In collaboration with:

Nathalie Fragoso
(InternetLab)

Authors: Katitza Rodriguez and Veridiana Alimonti
Collaborators: Nathalie Fragoso (InternetLab)

This report builds on the *State Surveillance of Communications in Brazil and the Protection of Fundamental Rights* report, published in 2016.

EFF's Associate Director of Research, Gennie Gebhart edited this report. EFF's Engineering and Design Project Manager, Kim Carlson, along with EFF's Art Director, Hugh D' Andrade and EFF's Education & Design Lead, Soraya Okuda designed and formatted this report. EFF's engineers, Syd Young, Artemis Schatzkin, and Will Greenberg developed the revamped version of the Necessary & Proportionate website.

EFF would like to thank Luiza Rehder do Amaral, EFF Tecs-USP Fellow (2019) for her research and contributions to this report.

A publication of the Electronic Frontier Foundation, 2020.
"The State of Communication Privacy Law in Brazil" is released under a Creative Commons Attribution 4.0 International License (CC BY 4.0).

AUGUST 2020

INTRODUCTION

This report provides condensed information on the rules for government access to communication data in criminal investigations in Brazil. It offers brief and straightforward answers on a set of relevant questions regarding when and under which conditions law enforcement authorities can gain access to users' communications data in criminal investigations as well as an overview of transparency obligations and practices.

This FAQ is intended for non-lawyers who want some general information about the legal framework for government access to data, but is not legal or technical advice.

The legal questions raised by this FAQ can be complex and the legal risks in any case will depend on the particular facts and on legal doctrines not necessarily mentioned here. This FAQ is meant to familiarize you with some of the principles involved, so that you can have a more effective discussion if and when you engage an attorney to help you with your particular circumstance.

DATA PROTECTION OVERVIEW

1. Is there a data protection law?

Brazil's data protection law[1] was adopted in 2018. The provisions regarding the oversight authority entered into force in December 2018. The remainder part comes into effect in September 2020, except for the penalties section that was postponed to August 2021.[2]

2. Is there a data protection authority?

The law creates the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados - ANPD)*. Although the provisions creating it came into effect in December 2018, the government introduced a decree implementing its structure one year and a half later. The decree, however, will only have legal force when the President of the Board is officially appointed and approved by the Senate.[3]

The legal framework that creates the ANPD does not properly fulfil independence requirements. Although the law ensures technical and decision-making autonomy as well as stipulating fixed-term mandates for its Board of Directors, the authority is part of the administrative structure of the Presidency.[4] The legal status of the authority as part of the Presidency is transitory and the Executive Branch is entitled to change the authority's organizational framework to one that best meets independence requirements by December 2020 without the need for a legislative reform, even though such changes are not mandatory.[5]

The law also creates a multi-stakeholder National Council for the Protection of Personal Data and Privacy (*Conselho Nacional de Proteção de Dados Pessoais e da Privacidade*).[6] Some of the Council's responsibilities are to propose strategic guidelines and provide inputs for drafting a "National Policy for the Protection of Personal Data and Privacy" and for the authority's activities; to issue annual reports evaluating how the National Policy actions have been executed; to suggest actions for the authority to implement; and to prepare studies and hold public debates and hearings on the protection of personal data and privacy.[7]

---

[1] Data Protection Law -- Law 13.709/2018 (*Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)*) http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (Portuguese)

[2] Article 65, I-A, Law 13.709/2018. The date set for the legal force of the remaining part of the law was August 2020. Brazil's President Bolsonaro tried to postpone it to May 2021 through an executive act that has an immediate effect but demands Congress approval to remain valid. The Brazilian Senate stopped the deferral when approving the President's act without the extension provision. Read more at: https://www12.senado.leg.br/assessoria-de-imprensa/notas/nota-de-esclarecimento-vigencia-da-lgpd (Portuguese)

[3] Article 6, Decree 10.474/2020, https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226 (Portuguese)

[4] See Articles 55-A, 55-B, 55-D, and 55-F, Law 13.709/2018

[5] Article 55-A, paragraphs 1 and 2, Law 13.709/2018.

[6] Article 58-A, Law 13.709/2018.

[7] Article 58-B, Law 13.709/2018.

3. Does the data protection law apply to law enforcement activities?

The processing of personal data *solely* for the purposes of public safety, national defense, state security or investigations, and prosecution of criminal offenses is out of the scope of Law 13.709/2018's overall regime. The law sets out that specific legislation has to be approved to regulate the processing of personal data in such cases.[8] This legislation must provide for measures that are proportionate and strictly necessary to meet the public interest, in accordance with due process, data protection principles, and data subjects' rights. Nonetheless, art. 4, paragraphs 2 to 4 of the Law 13.709/2018 are applicable to law enforcement activities once the data protection law enters in force. Paragraphs 2 and 4 limits the processing of personal data within such activities by private parties. Paragraph 3 stipulates the national data protection authority has the duty to request data protection impact assessments for the processing of personal data for law enforcement purposes and may also issue technical opinions and recommendations.

4. What are the criteria, if any, for the transfer of personal data to third countries under their data protection law?

Chapter V of the Data Protection Law sets forth the criteria for the transfer of personal data to third countries. According to Article 33, the transfer is allowed:

- to countries or international organizations that provide an appropriate degree of protection of personal data relative to the level of protection ensured by the Brazilian law;
- when, in a specific transfer, the controller demonstrates that it complies with the data protection principles, data subjects' rights and the data protection regime set forth by Brazilian law, which can be done through specific or standard contractual clauses or by complying with global corporate standards or other regularly issued certificates and codes of conduct;
- when the transfer is necessary for international legal cooperation between law enforcement and intelligence agencies, in accordance with international law;
- when the transfer is necessary to protect the life or physical safety of the data subject or a third party;

[8] Article 4, paragraph 1, Law 13.709/2018. Despite this exception, there are rules already in place regarding personal data and criminal identification that, for example, require justified reasons for the collection of sensitive data. As part of this framework, see Law n.12.037/2009 (>http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12037.htm<), art. 90 of the Law 7.210/1984 (>http://www.planalto.gov.br/ccivil_03/leis/l7210.htm<), the Decree 7.950/2013 (>http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7950.htm<), and the Resolution of the Steering Committee of the Database of Genetic Profiles n. 9/2018 (>http://www.lex.com.br/legis_27640537_RESOLUCAO_N_9_DE_13_DE_ABRIL_DE_2018.aspx<) .

- with the data subject's specific and explicit consent, based on prior information about the international nature of the operation, clearly distinguishing it from other data processing purposes; or
- when the transfer is authorized by the national authority, an outcome of an international cooperation agreement, or necessary for the implementation of public policies or if it derives from a legal attribution for the provision of public services; if it is necessary for the controller to comply with a legal or regulatory obligation; for the execution of a contract or its preliminary procedures at the request of the data subject; or for the regular exercise of rights in judicial, administrative, or arbitral proceedings.

The national authority must take into account the following elements when assessing the adequate level of privacy protection of a third country or international organization: the legislation in force, either general norms or specific sectoral rules, in the country or international body to whom the data is being transferred; the nature of the data; the compliance with data protection principles and data subjects' rights set forth in Brazilian data protection law; the adoption of security measures provided for in specific regulation; proper judicial and institutional guarantees for the protection of personal data; and other specific circumstances relating to the transfer.[9] Also, the national authority must be informed of any changes in the standards mentioned in the item above.[10]

The national authority, or certification bodies assigned and supervised by the authority, [11] are to draft the standard contractual clauses mentioned above, and verify the specific contractual clauses in a given transfer, the controllers' global corporate standards, or their certificates and codes of conduct.[12]

[9] Article 34, Law 13.709/2018.
[10] Article 36, Law 13.709/2018.
[11] Article 35, paragraph 3, Law 13.709/2018.
[12] Article 35, Law 13.709/2018.

COMMUNICATIONS PRIVACY LAW

5. What's the legal authorization needed to access communications data?

Interception of communication

Brazil's Federal Constitution requires a court order to lift the confidentiality of telephone communications.[13] The Criminal Procedure Code, amended by Law 13.964/2019, sets that interception measures must be authorized by a "*juiz das garantias*," responsible for ensuring the respect of individual rights and legal safeguards during police investigations and anticipated discovery. The same judge cannot function in the criminal prosecution.[14] However, this separation between the judge who functions in the criminal prosecution and the one who authorizes investigative measures is currently suspended due to a decision of a Supreme Court Justice.[15]

The law regulating the interception of telephone communications, of any nature,[16] also refers to the interception of the flow of communications in computer and telematic systems.[17] It reasserts the need for a previous judicial order, following the request of the prosecutor or the police authority.[18] Such a request must demonstrate that the interception is necessary for the criminal investigation and indicate the means to be employed.[19] Further, the fact under investigation must be clearly described, including the identification of the person affected, unless this is justified as manifestly impossible.

[13] Article, 5, XII, Brazilian Federal Constitution (*Constituição de República Federativa do Brasil de 1988*) http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (Portuguese)
[14] Articles 3-A to 3-F, Criminal Procedure Code (*Decreto-Lei 3.689/1941 - Código de Processo Penal*) http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm (Portuguese), amended by Article 3, Law 13.964/2019 (*Lei 13.964/2019 - Aperfeiçoa a legislação penal e processual penal*). http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm (Portuguese). According to Article 3-B, XI, the "*juiz das garantias*" is the competent judge for all the other measures described in question 1.3.a requiring a judicial order.
[15] The Justice that set this suspension for an indefinite period, until the Court decides on the merit of constitutional challenges against the amendment, considered that the Judiciary should have proposed the law, as it affects the functioning of the justice system in the country. He has also justified that the law passed without proper budgetary provision for the implementation of an "additional judge" per legal prosecution. See https://g1.globo.com/politica/noticia/2020/01/22/fux-suspende-juiz-de-garantias-por-tempo-indeterminado.ghtml (Portuguese).
[16] Article 1, Law 9.296/1996 - "Telephone Interception Law" (*Lei 9.296/1996 - Lei de Interceptação Telefônica)* http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm (Portuguese)
[17] Article 1, sole paragraph, Law 9.296/1996. Controversies about the interpretation of the constitutional provision protecting the secrecy of communications on whether it allowed the interception of online data led this paragraph to be challenged in the Supreme Court. However, the lawsuit was dismissed on procedural grounds. Currently, Article 7 of the Law 12.965/2014 (*Marco Civil da Internet*) explicitly mentions the interception of the flow of communications over the Internet, by a judicial order, and following the requirements of the Telephone Interception Law. See InternetLab, "State Surveillance of Communications in Brazil and the Protection of Fundamental Rights", item 1.5 at: https://necessaryandproportionate.org/country-reports/brazil#footnoteref28_8k9208g
[18] Article 3, Law 9.296/1996 http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm
[19] Article 4, Law 9.296/1996.

[20] The judge must issue a reasoned decision, indicating how the measure will be conducted. The interception may not exceed fifteen days and is renewable for equal periods provided proof of the indispensability of the evidence.[21] Procedures, recordings, and transcripts are secret and documented in separate court records. The defense has access to it once the accusation is formalized. However, even before that, the Brazilian Supreme Court ensures the defense's right to have access to evidence already documented within an investigative procedure when it concerns the exercise of the right of defense.[22]

Access to the content of communications and metadata

Law 12.965/2014, known as "Brazil's Civil Rights Framework for the Internet" (*Marco Civil da Internet*), requires prior judicial authorization to access metadata and communications content.[23] Authorities can also access stored content of seized devices, provided that the search and seizure procedure was authorized by a judge. There is no need for a new and specific court order according to a Brazilian Supreme Court precedent.[24]

Access to retained traffic data

Regarding telephone communications, Law 12.850/2013 requires fixed and mobile phone providers to retain call records of the origin and destination of national and international calls for a period of five years, and make such records available to the Chief of the Civil Police[25] and prosecutors.[26] The provision does not mention the need of a previous judicial order, and the case law on that point is still contentious.[27] The law also states that the Chief of the Civil Police and prosecutors can access subscriber data without a judge's authorization.[28] The scope of Law 12.850 is limited to investigations of crimes related to terrorist or criminal organizations as well as criminal offenses provided for in international treaties when their commitment has begun in Brazil and

[20] Article 2, sole paragraph, Law 9.296/1996.
[21] Article 5, Law 9.296/1996.
[22] Brazilian Supreme Court, "Binding Precedent" n. 14 (*Supremo Tribunal Federal, Súmula Vinculante n. 14*) http://www.stf.jus.br/portal/jurisprudencia/menuSumario.asp?sumula=1230 (Portuguese)
[23] Article 7, III, Art. 10, para. 1 and 2, Law 12.965/2014 (*Lei 12. 965/2014 - Marco Civil da Internet*) http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (Portuguese)
[24] See STF, RE 418.416/SC, http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790. See also precedent of Superior Court of Justice (STJ), HC 372.762-MG, https://stj.jusbrasil.com.br/jurisprudencia/511208828/habeas-corpus-hc-372762-mg-2016-0254030-1?ref=juris-tabs
[25] The civil police is assigned to carry out the duties of judicial police and to investigate criminal offenses, except military ones. The Chief (*delegado de polícia*) is responsible for leading the investigations. In the case of federal crimes, such attributions pertain to the federal police. Article 144, para 1 and 4, Brazilian Federal Constitution, http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (Portuguese)
[26] Article 17, Law 12.850/2013 (*Lei 12.850/2013 - Lei de Organizações Criminosas*) http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm (Portuguese)
[27] The disclosure of communications data without a prior judicial order has been challenged in the country's Supreme Court by the National Association of Mobile Operators (*Associação Nacional das Operadoras Celulares - ACEL*)) through the ADI 5063/DF. The suit is still awaiting trial. See more at http://www.stf.jus.br/portal/peticaoInicial/verPeticaoInicial.asp?base=ADIN&s1=5063&processo=5063 (Portuguese)
[28] Article 15, Law 12.850/2013. The constitutional challenge presented in ADI 5063/DF also targets this provision.

the result has or should have occurred abroad, or vice versa.[29] Resolutions of the Brazilian National Telecommunications Agency (*Agência Nacional de Telecomunicações - Anatel*) also contain provisions of communications data retention (see question 1.3.d), but they do not specify the requirements for law enforcement access.

For online communications, Articles 13 and 15 of Brazil's Civil Rights Framework set forth the requirements for mandatory retention of connection logs and access to Internet application logs. Both can be accessed by prosecutors and police or administrative authorities with prior judicial authorization.[30] "Connection log" is defined as the set of information regarding the start and end date and time of an Internet connection, its duration, and the IP address used by the terminal for sending and receiving data packets.[31] "Access to Internet application log" is defined as the set of information regarding the date and time of use of a particular internet application from a given IP address.[32]

Access to subscriber data

For subscriber data, Brazil's Civil Rights Framework provides an exception to its general rule requiring a prior judicial order for having access to communication-related data. Where authorized by other laws, "competent administrative authorities" are allowed to directly require subscriber data.[33] Laws 12.850/2013[34] and 9.613/98[35] grant this authorization to prosecutors and police officers (usually the Chief of the Civil Police - *delegado de polícia*) within the context of money laundering and criminal organization investigations.[36] The Criminal Procedure Code does the same for crimes it specifies, such as human trafficking, kidnapping, organ trafficking, and sexual exploitation.[37] Despite these explicit, specific legal provisions on certain and specified crimes, there are cases where police authorities claim the power to directly access subscriber data during the investigation of other crimes based on an alleged general authorization in the law that regulates the criminal investigation conducted by the Chief of the Civil Police.[38] Such

[29] Art. 1, Law 12.850/2013 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm (Portuguese)
[30] Article 10, para 1, Art. 13, para 5, and Art. 15, para 3, Law. 12.965/2014 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (Portuguese)
[31] Article 5, VI, Law 12.965/2014 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (Portuguese)
[32] Article 5, VIII, Law. 12.965/2014 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (Portuguese)
[33] Article 10, para 3, Law. 12.965/2014 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (Portuguese)
[34] Article 15, Law 12.850/2013 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm (Portuguese)
[35] Article 17-B, Law 9.613/1998 (*Lei 9.613/1998 - Lei de Lavagem de Dinheiro*) http://www.planalto.gov.br/ccivil_03/leis/l9613.htm (Portuguese)
[36] Although the provisions are set in two specific laws, one targeting criminal organizations (Law 12.850) and the other money laundering activities (Law 9.613), their broad wording can lead to a wider, and improper, application. See comment in question 1.3.d - *mandatory data retention*.
[37] Article 13-A, Criminal Procedure Code http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm (Portuguese)
[38] Article 2, para 2, Law 12.830/2013 (*Lei 12.830/2013 - Dispõe sobre a investigação criminal conduzida pelo delegado de polícia*), http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12830.htm (Portuguese)

interpretation is currently under constitutional challenge in the country's Supreme Court.[39]
Subscriber data is defined in legislation as the person's first name, last name, marital status, occupation, parents' names, and address.[40] Direct requests must be specific regarding targeted individuals and desired information; collective requests that are generic or non-specific are prohibited.[41]

Identification by IP addresses

Subscriber data associated with an IP address may be directly accessed by prosecutors and police officers in cases authorized by law (see access to subscriber data). Otherwise, a judicial order is required.

Location data

The need of a previous warrant to access location data is an ongoing legal debate. The Criminal Procedure Code sets that, for the prevention and repression of human trafficking crimes, prosecutors and police authorities may request a judicial order to require telecommunication companies to immediately provide the technical means enabling the location of victims or suspects of an ongoing crime.[42] If the judge does not decide within 12 hours, the Code allows authorities to directly demand telecommunication companies to provide the data, immediately notifying the judge about the measure.[43] This exemption to a prior judicial order is currently under constitutional challenge regarding the privacy protections set in Article 5, X and XII of the Brazilian Constitution.[44] As for the access to past location data (not in real time), court decisions have ruled that a prior judicial order is not required.[45] However, this is a controversial interpretation considering the privacy and data protection safeguards established in Brazil's constitutional and legal frameworks, since interferences with fundamental rights should be clearly specified in law.[46]

---

[39] The constitutional challenge is the ADI 5059/DF. See more at http://www.stf.jus.br/portal/peticaoInicial/verPeticaoInicial.asp?base=ADIN&s1=5059&processo=5059 (Portuguese)
[40] Article 11, para 2, Decree 8771/2016 http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm (Portuguese)
[41] Article 11, para 3, Decree 8771/2016 http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm (Portuguese)
[42] Article 13-B, Criminal Procedure Code, http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm (Portuguese)
[43] Article 13-B, para. 4, Criminal Procedure Code. Paragraph 2 sets out that location must be provided by the mobile company for a period of up to 30 days, renewable once. For longer than that, a specific court order is required. The National Association of Mobile Operators (*Associação Nacional das Operadoras Celulares - ACEL*) has challenged this provision in the Brazil's Supreme Court claiming it could be misinterpreted to mean that a prior judicial order would be required only for longer periods requests.
[44] Article 5, X and XII, Brazilian Federal Constitution http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (Portuguese). The constitutional challenge is the ADI 5642/DF. See more at http://www.stf.jus.br/portal/peticaoInicial/verPeticaoInicial.asp?base=ADIN&s1=5642&processo=5642 (Portuguese)
[45] Superior Court of Justice (STJ), HC 247.331-RS, https://www.jusbrasil.com.br/diarios/documentos/137159649/habeas-corpus-n-247331-rs-do-stj (Portuguese)
[46] *See* more about this debate at the discussion during the 3rd International Congress "Fundamental Rights and Criminal Procedure in the Digital Age," held by InternetLab, https://www.youtube.com/watch?v=fuHf4tCUD54 (Portuguese)

Monitoring of the spectrum

The Criminal Organizations Law and the Telephone Interception Law allow the environmental capture of electromagnetic signals.[47] The procedure must be previously authorized by a judge, at the request of a public prosecutor or the police.[48]

6. What's the factual basis to access communications data?

The Criminal Procedure Code commands courts to abide by principles of adequacy, necessity, and proportionality when ordering evidence gathering.[49] The same goes for rulings on motions that seek injunctive remedies on submission of evidence.[50]

Content and metadata

The interception of communications is allowed when, cumulatively, there are reasonable indications of authorship or participation in a criminal offense, the fact investigated constitutes a criminal offense punished with confinement, and the proof cannot be produced by other available means.[51] The request should indicate the means to be adopted[52] and clearly describe the situation under investigation, including the indication and qualification of who is investigated, unless manifestly impossible and duly justified. The judge must issue a reasoned decision within 24 hours, indicating how the measure will be executed.[53]

As for the physical access to the device and the device's content, the Criminal Procedure Code authorizes searches and seizures without judicial authorization on the grounds of suspicion that someone conceals "objects necessary for proof of the offense or defense of the defendant" and "letters, open or not, intended for the accused or in his possession, when there is suspicion that knowledge of the contents may be useful in elucidating the fact."[54] However, the Brazilian Superior Court of Justice (STJ) has ruled it is unlawful to access the content on the devices seized without a previous judicial order.

[47] Article 3, II, Law 12.850/2013, http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12850.htm (Portuguese) and Article 8-A, Law 9.296/1996, amended by Article 7, Law 13.964/2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm.
[48] Article 8-A, Law 9.296/1996.
[49] Article 156, Criminal Procedure Code, http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm (Portuguese)
[50] Criminal Procedure Code, article 282.
[51] Article 2, Law 9.296/1996, http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm (Portuguese)
[52] Article 4, Law 9.296/1996
[53] Article 4, para. 2 and Article 5, Law 9.296/1996
[54] Article 240, para 1, *d* and *f*, and para. 2, Criminal Procedure Code, http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm (Portuguese)

[55] According to the Brazilian Supreme Court (STF), a warrant for search and seizure is sufficient to allow access to data stored in computers.[56]

Brazil's Civil Rights Framework stipulates the standard for accessing connection and access to Internet application logs. The request should contain: (i) evidence-based indications that the unlawful act occurred; (ii) reasoned justification that the logs are useful for investigative or evidential purposes; and (iii) the logs' period of time.[57]

Subscriber data

Direct requests for subscriber data must be specific regarding targeted individuals and desired information; collective requests that are generic or non-specific are prohibited.[58] The competent administrative authorities should indicate their explicit legal footing for direct access and the justification for the request.[59] As already mentioned, the competent authorities are the Chief of the Civil Police and public prosecutors. The investigation must be related to the scope of the authorizing laws in order to fulfill the legal footing requirement (see Question 1.3.a - *Access to Subscriber Data*).

Monitoring of the spectrum

The legal standard applied to the environmental capture of electromagnetic signals is also set by the Telephone Interception Law.[60] In this case, the judge can authorize the measure when the evidence cannot be produced by other available means and there are reasonable indications of authorship or participation in criminal offenses whose maximum penalties are longer than four years or in related criminal offenses. The police or prosecutor request has to detail where the procedure will take place and the way the device should be set up.[61] The measure cannot exceed 15 days, and is renewable by judicial decision for equal periods if the investigation involves permanent, habitual, or continued criminal activity and the indispensability of the evidence is ascertained.

7. Which authorities have the legal capacity to request access to communications data?

In the context of a criminal investigation, the following authorities have the capacity to request access to communications data: (i) the Chief of the Civil Police (*delegado de*

[55] Superior Court of Justice (STJ), RHC 51.531-RO, https://stj.jusbrasil.com.br/jurisprudencia/340165638/recurso-ordinario-em-habeas-corpus-rhc-51531-ro-2014-0232367-7/inteiro-teor-340165652 (Portuguese)
[56] See Internet Lab, "Vigilância sobre as Comunicações no Brasil", 2017, p. 12. http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf (Portuguese)
[57] Article 22, Law 12.965/2014, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
[58] Article 11, para 3, Decree 8.771/2016 http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm (Portuguese)
[59] Article 11, Decree 8.771/2016
[60] Article 8-A, Law 9.296/1996, amended by Article 7, Law 13.964/2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm.
[61] Article 8-A, Law 9.296/1996, amended by Article 7, Law 13.964/2019.

polícia);[62] (ii) public prosecutors; and (iii) judges,[63] who can request the data either *ex officio* or following an initiative by the police or prosecutor.

Parliamentary Committees of Inquiry, temporarily formed within the Legislative Power to ascertain a given fact, hold "investigative powers of the judicial authorities."[64] They may order breach of confidentiality of stored data without judicial intervention[65] as well as subscriber data and the identification of devices (including IMSI or IMEI).

8. Does the country have provisions about access to data in cases of emergency?

The Criminal Procedure Code allows the judge to order *ex officio*[66] or following the parties' request the production of urgent and relevant evidence before the criminal prosecution is initiated, according to necessary, adequate, and proportionate standards.[67] Precedent set by the Superior Court of Justice states that the mere course of time is not enough to justify such anticipation.[68] Although there is no legal definition of "urgency" or "urgent evidence," relevant elements may be derived from case law, such as the impossibility of gathering the evidence in the procedural phase, reasonable indications that the evidence may perish, or its relevance and indispensability for the sentence. The Code also deems "urgent" situations involving human trafficking, since it allows the Chief of the Civil Police and prosecutors to directly access geolocation data when the judge does not decide within 12 hours of the request.[69] Finally, the Telephone Interception Law states that "exceptionally" the judge may allow the interception request to be formulated verbally, provided that the interception legal requirements are met.[70] However, the law does not establish what "exceptionally" means.

[62] Article 2, para. 2, Law 12.830/2013 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12830.htm (Portuguese)
[63] Article 156, Criminal Procedure Code http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm (Portuguese). See also, Article 3, Law 9.296/1996, http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm (Portuguese). The currently suspended amendment in the Criminal Procedure Code creating the *juiz das garantias* also tacitly withdraws the judge's initiative for anticipated discovery. See art. 3, Law 13.964/2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm#art3 (Portuguese)
[64] Article 58, para. 3, Brazilian Federal Constitution, http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (Portuguese)
[65] *See* Internet Lab, "Vigilância sobre as Comunicações no Brasil", 2017, p. 9. http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf (Portuguese)
[66] The currently suspended amendment in the Criminal Procedure Code creating the *juiz das garantias* also tacitly withdraws the judge's initiative for anticipated discovery. See art. 3, Law 13.964/2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm#art3 (Portuguese)
[67] Article 156, I, Criminal Procedure Code, http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm (Portuguese)
[68] Superior Court of Justice (STJ), Precedent n. 455 (Súmula 455), https://scon.stj.jus.br/SCON/sumulas/doc.jsp?livre=@num=%27455%27 (Portuguese)
[69] Article 13-B, para 4, Criminal Procedure Code, http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm (Portuguese)
[70] Article 4, para 1, Law 9296/1996, http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm (Portuguese)

9. Is there any data retention mandate?

Brazil is the only country in Latin America that has developed different data retention rules depending on the kind of service: fixed line, mobile phones, or Internet services.

Fixed Line and Mobile Phone Services

The Fixed Telephone Service Regulation states that telecommunications companies must retain data related to the provision of services, including call logs, for a minimum of five years.[71] The article does not specifically describe the type of data that should be retained, who can access it, or for what purposes.

Similarly, the Regulation on Personal Mobile Service[72] requires telecommunications providers to retain "at the disposal of Anatel and other parties, tax documents (*documentos de natureza fiscal*) that contain data on incoming and outgoing calls, dates, time, duration and price, as well as account information of subscribers [...]" for a minimum of five years.[73] Both resolutions establish data retention obligations even for services providing flat-rate plans, where a call's duration or the number dialed does not affect the amount a user pays. It is thus reasonable to suppose that Anatel's data retention regulations are used for purposes that go well beyond those associated with its service provision responsibilities.

The Criminal Organizations Law also requires fixed and mobile phone providers to retain call records (*registros de identificação*) of the origin and destination of national and international calls for a period of five years, and make such records available to the Chief of the Civil Police and public prosecutors.[74] The provision does not specify the type of data that should be logged, the limitations on access and usage conditions, or the data security rules that should apply. This provision also states that the Chief of the Civil Police and the public prosecutor can access a defendant's account information without a judicial order.[75]

[71] Article 22, Anatel's Resolution 426/2005 (*Resolução 426/2005 - Aprova o Regulamento do Serviço Telefônico Fixo Comutado – STFC*) https://www.anatel.gov.br/legislacao/resolucoes/2005/7-resolucao-426 (Portuguese)
[72] Anatel's Resolution 477/2007 (*Resolução 477/2007 - Aprova o Regulamento do Serviço Móvel Pessoal – SMP*) https://www.anatel.gov.br/legislacao/resolucoes/2007/9-resolucao-477 (Portuguese)
[73] The rationale of the five-year data-retention obligation for telephone services, and justification of billing auditing and oversight by Anatel, are outlined in Article 10, XXII of Resolução no. 477/07. However, Resolution no. 477/07 and Resolution 426/05 establish data retention obligations for fixed and mobile telephone service providers have long allowed for the convenience of keeping such records for the state's investigatory and prosecution purposes.
[74] Article 17, Law 12.850/2013 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm (Portuguese)
[75] The constitutionality of this provision is being challenged through an Ação Direta de Inconstitucionalidade procedure, ADI 5063/DF, and is awaiting trial.

Internet Providers

Anatel's Resolution 614/13[76], which sets out the regulation of multimedia communication services, requires Internet service providers to retain subscriber records and account data for one year.

Brazil's Civil Rights Framework for the Internet requires operators of an "autonomous system" who provide Internet access to retain connection logs for one year.[77] Here, "autonomous system" is a technical term that refers to those who administer specific IP address blocks and the corresponding autonomous system for routing purposes. This implies that the obligation to retain applies only to the largest ISPs and not to each entity that provides Internet access to end users, such as a school, library, café, or small local ISP that doesn't administer its own IP address blocks.

"Connection log" is defined as the set of information regarding the start and end date and time of an Internet connection, its duration, and the IP address used by the terminal for sending and receiving data packets. A current controversial issue is whether this obligation entails the retention of the logic gate used in the connection when the IP address is shared among different users. Case law has not reached a convergent position so far and digital rights experts defend the narrow interpretation of the retention obligation.[78] The law also requires commercial operators of Internet applications to retain access logs to their own applications for a period of six months.[79] Non-commercial operators of such applications may also be ordered by a court or public authority to retain such logs.

In June 2019, the Superior Court of Justice (STJ) ruled[80] that Internet Service Providers have the obligation to retain subscriber data associated with IP addresses for five years according to the statute of limitation period established in the Brazilian Civil Code.[81]

10. Are there any rules that authorize the use of malware?

There are currently no laws that explicitly authorize the use of malware.

---

[76] Article 53 and 54, Anatel's Resolution 614/2013, (*Resolução 614/2013 - Aprova o Regulamento do Serviço de Comunicação Multimídia - SCM*) https://www.anatel.gov.br/legislacao/resolucoes/2013/465-resolucao-614 (Portuguese)
[77] Article 13, Law 12.965/2014, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (Portuguese)
[78] See Internet Lab, "O Marco Civil da Internet e o dilema da 'porta lógica" https://www.jota.info/opiniao-e-analise/artigos/o-marco-civil-da-internet-e-o-dilema-da-porta-logica-22082019 (Portuguese)
[79] Article 15, Law 12.965/2014. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (Portuguese). "Access to Internet application log" is defined as the set of information regarding the date and time of use of a particular internet application from a given IP address.
[80] Superior Court of Justice (STJ), REsp n. 1.785.092-SP, https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1821044&num_registro=201502935292&data=20190509&formato=PDF (Portuguese)
[81] Article 1.194, Brazilian Civil Code *(Lei 10.406/2002 - Institui o Código Civil)* http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm (Portuguese)

However, there are indications that law enforcement agents have relied on the Telephone Interception Law to request judicial order for using malicious software in criminal investigations.[82] Such alleged legal footing is at odds with a 2018 decision of the Superior Court of Justice ruling that the telephone interception procedure could not authorize the police to access WhatsApp messages by covertly mirroring them on the app's web version.[83] According to the court, relevant disparities between the measures disallow this analogous application, such as the fact that the mirroring grants access to past, present, and future messages, while a regular interception procedure can only cover a limited time span; or that police officers could send or delete messages, which is not possible in a regular interception procedure. The use of malicious software would enable features equivalent to those contested in the decision.

Similar actions might also rely on the provisions of "virtual infiltration" in the Laws 8.069/1990[84] and 12.850/2013,[85] which is again unclear and objectionable. There is no precise legal definition of "virtual infiltration" capable of authorizing such an invasive measure. In addition, the regular meaning of "infiltration" refers to the action of undercover agents who obtain information by gaining criminals' trust. In general terms, virtual infiltration must be previously ordered by a judge when there are indications that a crime referred to in the authorizing laws has been committed and evidence cannot be produced by other available means. The request must demonstrate the need for the measure and indicate the scope of the police officers' tasks, the names or surnames of the persons investigated and, where possible, the logs allowing the identification of these persons. [86]

11. Is there any law that compels companies to provide direct access to their internal servers for law enforcement purposes?

To the best of our knowledge, there is no legal provision authorizing this kind of access in criminal investigations.

[82] The Brazilian Federal Police has already stated, in response to a request for access to information, that the Law 9296/1996 represents the legal ground for using malicious software in criminal investigations. See the piece at https://www.vice.com/pt_br/article/qkzdzq/mercado-milionario-de-compra-e-venda-de-bugs-aumenta-inseguranca-na-internethttps://www.vice.com/pt_br/article/qkzdzq/mercado-milionario-de-compra-e-venda-de-bugs-aumenta-inseguranca-na-internet (Portuguese).
[83] Superior Court of Justice (STF), RHC 99.735-SC. The ruling rationale can be found at https://ww2.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=@cod=%270640%27 (Portuguese)
[84] Articles 190-A to 190-E, Law 8.069/1990 (*Lei 8.069/1990 - Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências*) http://www.planalto.gov.br/ccivil_03/leis/l8069.htm (Portuguese)
[85] Article 10-A, Law 12.850/2013, amended by Article 14, Law 13.964/2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm (Portuguese)
[86] The Law 12.850/2013 applies to investigations of crimes related to terrorist or criminal organizations as well as criminal offenses provided for in international treaties when their commitment has begun in Brazil and the result has or should have occurred abroad, or vice versa. The Law 8.069/1990 authorizes the use of virtual infiltration only for the investigation of crimes against child and adolescent sexual dignity.

12. Does the law compel companies to assist law enforcement agencies in their investigations?

The police authority may require specialized services and specialist technicians to telephone companies for conducting interception measures.[87] Telephone companies also have the legal duty to assist law enforcement authorities to access geolocation data in human trafficking cases[88] and make call records available for investigations.[89] Private companies and public bodies, as laid out in specific law, have the duty to provide subscriber data to law enforcement authorities.[90] Art. 21 of the Law 12.850/2013, related to criminal organization investigations, sets a prison sentence of six months to two years for anyone who refuses or omits subscriber data, records, documents, and information requested by the judge, prosecutor or the Chief of the Civil Police.

[87] Article 7, Law 9296/1996, http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm (Portuguese)
[88] Article 13-B, *caput* and para. 4, Criminal Procedure Code, http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm (Portuguese)
[89] Article 17, Law 12.850/2013, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm (Portuguese)
[90] Article 13-A, Criminal Procedure Code, http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm; Article 15, Law 12.850/2013, http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12850.htm (Portuguese); and Article 17-B, Law 9613/1998, http://www.planalto.gov.br/ccivil_03/leis/l9613.htm (Portuguese)

TRANSPARENCY & COMMUNICATIONS PRIVACY

13. Does the State report on the number of requests to access communications data?

Brazil's National Council of Justice (*Conselho Nacional de Justiça*)[91] publishes a public database with statistical data on communications interception procedures authorized by courts.[92] The system breaks the data down per year, month, and court in the following categories: number of started and ongoing requests, number of started and ongoing criminal procedures, number of monitored phones, number of monitored VOIP communications, and number of monitored electronic addresses. The first two categories are split into telephone and electronic interception. Other state agencies do not publish similar information—to the best of our knowledge, not even on the number of requests for Internet users' subscriber data, which is mandatory for federal administration bodies.[93]

14. Is there any legal limitation that prohibits companies from publishing transparency reports?

To the best of our knowledge, no normative framework prohibits companies from publishing statistical data on the number of data requests made by the state in criminal or national security matters. On the contrary, Decree 8.771/2016 establishes that the highest authority of each federal public administration agency shall publish, on its website, yearly statistical reports about their requests for access to Internet users' subscriber data[94] (i.e. name, first name, marital status, occupation, parents' names, and address).[95] The statistical reports should include: the number of requests; the list of ISPs and Internet applications from which data has been requested; the number of requests

[91] The National Council of Justice (CNJ) is a public institution that aims to improve the work of the Brazilian legal system, especially with regard to the control and administrative and procedural transparency. See more at https://www.cnj.jus.br/sobre-o-cnj/quem-somos-e-visitas/
[92] National System of Telephone Interception Control (*Sistema Nacional de Controle de Interceptações Telefônicas*) https://www.cnj.jus.br/sistemas-9/sistema-nacional-de-controle-de-interceptacoes-telefonicas/ (Portuguese).
[93] Article 12, Decree 8.771/2016. A study conducted by InternetLab in 2018 highlights that many federal administration bodies are not, or state not being, aware of the obligation set by the Decree. See more at: http://www.internetlab.org.br/pt/privacidade-e-vigilancia/marco-civil-da-internet-e-transparencia-resultados-de-pedidos-de-acesso-informacao-sobre-quebras-de-sigilo-de-dados-cadastrais/ (Portuguese)
[94] Article 12, Decree 8.771/2016, which regulates the Law 12.965/2014, known as the Brazilian Civil Rights Framework for the Internet (*Marco Civil da Internet*) http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm (Portuguese)
[95] Article 11, paragraph 2, Decree 8.771/2016.

granted and rejected by ISPs and Internet applications; and the number of users affected.[96]

15. Do telecommunication companies publish transparency reports?

- **Claro/NET** does not disclose transparency reports.
- **Oi** does not disclose transparency reports.
- **TIM** does not disclose transparency reports.
- **Vivo/Telefónica** provides annual transparency reports.
- **Algar** does not disclose transparency reports.
- **Nextel** does not disclose transparency reports.
- **SKY/AT&T** publishes regular transparency reports, but with few data regarding their operations outside the US.

16. Can companies notify users about States' data requests?

There is no legal obligation that compels either the State or companies to notify targets of surveillance prior to carrying it out. The secrecy requirement is previously set in the Telephone Interception Law.[97] In other relevant statutes, the law gives a general authorization for the judge to determine it or not.[98] Companies are not prevented from notifying when secrecy is not legally or judicially set. Even in those cases, there is no prohibition for subsequent notification. Finally, it is worth mentioning that the Brazilian Supreme Court ensures the accused's defense a broad right to have access to evidence already documented within an investigative procedure when it concerns the exercise of his/her right of defense.[99]

[96] Article 12, Decree 8.771/2016.
[97] Article 8, Law 9.296/1996, http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm (Portuguese)
[98] Article 23, Law 12.850/2013, http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12850.htm (Portuguese) and Article 23, Law 12.965/2014, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (Portuguese).
[99] Brazilian Supreme Court, "Binding Precedent" n. 14 (*Supremo Tribunal Federal, Súmula Vinculante n. 14*) http://www.stf.jus.br/portal/jurisprudencia/menuSumario.asp?sumula=1230 (Portuguese). See also Article 23, Law 12.850/2013, http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12850.htm (Portuguese)