The State of Communication Privacy Law in Paraguay

Katitza Rodriguez,
International Rights Director
(EFF)

Veridiana Alimonti,
Latin American Senior Policy
Analyst (EFF)

In collaboration with:

Maricarmen Sequera
(TEDIC)

Authors: Katitza Rodriguez and Veridiana Alimonti
Collaborators: Maricarmen Sequera (TEDIC)

This report builds on the *State Communications Surveillance and the Protection of Fundamental Rights in Paraguay* 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.

JUNE 2020

INTRODUCTION

This report provides condensed information on the rules for government access to communication data in criminal investigations in Paraguay. 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?

Paraguay has different regulations that cover personal data processing in a scattered fashion, with separate rules regarding collection and processing.[1] Law 1.682/2001, amended by Law 1969/02, is the main law regulating the processing of private information.[2] It focuses on rules concerning credit information systems in banking and financial institutions, and does not define key concepts, such as personal data, data processing, and data subject.[3] Paraguay's Constitution also provides for *habeas data* as a safeguard related to official or public-nature databases. Data subjects may file a *habeas data* suit to gain access to their stored personal information, know more about the processing of such information, or require updating, correction, or deletion when personal data is erroneous or illegally affect the data subject's rights.[4]

2. Is there a data protection authority?

Paraguay does not have a comprehensive data protection law, and Law 1.682/2001, which is still the main piece of legislation addressing the processing of private information, has not set an enforcement authority. As a consequence, violations of data subjects' rights provided for in this law may be addressed through a complaint to consumer protection administrative bodies[5] or can be tackled in courts. In any case, there is no *ex-ante* institutional oversight.[6] With respect to official or public-nature databases, data subjects may also resort to courts via *habeas data* to gain access to their stored personal information, know more about the processing of such information, or

[1] TEDIC, "La protección de datos personales en bases de datos públicas en Paraguay - un estudio exploratorio", 2017, p. 47. Available at: https://www.tedic.org/wp-content/uploads/2017/09/La-protección-de-Bases-de-Datos-en-Paraguay_Documento-Final.pdf (Spanish)

[2] Law n. 1682/2001 (*Ley 1682 - Que reglamenta la información de carácter privado*), http://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado (Spanish), later modified by the Law n. 1969/2014 http://www.bacn.gov.py/leyes-paraguayas/2539/ley-n-1969-modifica-amplia-y-deroga-varios-articulos-de-la-ley-n-16822001-que-reglamenta-la-informacion-de-caracter-privado (Spanish) and the Law n. 5543/2015 http://www.bacn.gov.py/leyes-paraguayas/4524/ley-n-5543-modifica-los-articulos-5-y-9-de-la-ley-n-168201-que-reglamenta-la-informacion-de-caracter-privado-modificado-por-la-ley-n-196902 (Spanish)

[3] TEDIC, "La protección de datos personales en bases de datos públicas en Paraguay - un estudio exploratorio", 2017, p. 15. Available at: https://www.tedic.org/wp-content/uploads/2017/09/La-protección-de-Bases-de-Datos-en-Paraguay_Documento-Final.pdf (Spanish). The Paraguayan Congress is currently discussing a new "data protection bill," but it remains limited to credit information. See more at http://www.senado.gov.py/index.php/noticias/noticias-comisiones/2924-debaten-proyecto-de-ley-de-proteccion-de-datos-personales-2019-04-30-19-17-59 (Spanish) and TEDIC's analysis at https://www.tedic.org/ley-de-datos-personales-no-es-una-ley-de-datos-crediticios/ (Spanish)

[4] Article 135, Paraguay's Constitution (*Constitución de la República del Paraguay*) http://www.bacn.gov.py/CONSTITUCION_ORIGINAL_FIRMADA.pdf (Spanish)

[5] Article 5 and 6, Law n. 4974/2013 (*Ley 4974 - De la Secretaría de Defensa del Consumidor y el Usuario*), http://www.bacn.gov.py/leyes-paraguayas/4772/de-la-secretaria-de-defensa-del-consumidor-y-el-usuario (Spanish).

[6] TEDIC, "La protección de datos personales en bases de datos públicas en Paraguay," supra note 3.

require the updating, correction, or deletion when personal data is erroneous or illegally affect the data subject's rights. However, when it comes to information on the data subject's financial situation, economic solvency, or compliance with commercial obligations, case law has stated that deadlines set in Law 1.682/2001[7] prevail over the use of *habeas data*.[8]

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

No. Although Law 1.682/2001 does not stipulate an explicit exception of its application for law enforcement agencies, its scope is mainly to regulate the processing of personal data in credit information systems with a view on credit protection services. In turn, law enforcement access to financial information in criminal investigations, for example, usually relies on banking secrecy exceptions established in the general law regulating financial operations.[9] Despite the lack of specific data protection rules for law enforcement agencies, *habeas data* can be used to access, update, correct, or delete personal information stored in such agencies' databases.[10]

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

Paraguay does not have a comprehensive data protection law and the norm regulating the processing of private information does not cover the transfer of personal data to third countries.

[7] Article 9, Law n. 1682/2001, http://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado (Spanish), later modified by the Law n. 1969/2014 http://www.bacn.gov.py/leyes-paraguayas/2539/ley-n-1969-modifica-amplia-y-deroga-varios-articulos-de-la-ley-n-16822001-que-reglamenta-la-informacion-de-caracter-privado (Spanish) and the Law n. 5543/2015 http://www.bacn.gov.py/leyes-paraguayas/4524/ley-n-5543-modifica-los-articulos-5-y-9-de-la-ley-n-168201-que-reglamenta-la-informacion-de-caracter-privado-modificado-por-la-ley-n-196902 (Spanish)
[8] TEDIC, "La protección de datos personales en bases de datos públicas en Paraguay," supra note 1, p. 16.
[9] Article 86, Law n. 861/1996 (*Ley 861 - Objeto de la Ley General de Bancos, Financieras y otras Entidades de Crédito*), http://www.bacn.gov.py/leyes-paraguayas/4135/ley-n-861-general-de-bancos-financieras-y-otras-entidades-de-credito (Spanish).
[10] Actually, the first *habeas data* case was filed in 1992, when a lawyer and human rights defender, Martín Alamada, asked to access his data stored during Paraguay's dictatorship. The resulting records, known as "Terror Files," were declared an intangible heritage of humanity by UNESCO. TEDIC, "La protección de datos personales en bases de datos públicas en Paraguay," supra note 1, p. 14.

COMMUNICATIONS PRIVACY LAW

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

Article 36 of the Paraguayan Constitution ensures the inviolability of private documents and communications. As such, document records (whatever their format), correspondence, writings, and communications of any kind may not be examined, reproduced, intercepted, or seized except by a judicial order for cases specifically provided for in the law, and when it is indispensable for clarifying matters within the competence of the relevant authorities. Any evidence obtained in violation of these requirements is inadmissible.[11] Similar protection regarding private communications along with related information and documents is enshrined in the Telecommunications Law.[12] According to this law, inviolability of the secrecy of telecommunications means that it's prohibited to open, remove, interfere, edit, divert, publish, use, try to ascertain, or facilitate anyone except the recipient to have knowledge of the existence or content of communications entrusted to service providers.

Interception of communication

According to the Criminal Procedure Code, only a judge can authorize telecommunications interception.[13] Article 200 refers to *communications intervention* "whatever the technical means used," which brings a broad and hazardous understanding of communications interception. The results of such interception must be provided to the judge who authorized it. The judge will communicate the results to the Public Prosecutor's Office and to the accused and their defense.

Law 1881/2002, concerning the repression of illicit trafficking of narcotics and dangerous drugs,[14] similarly requires a prior judicial order for communications interception, at the request of the prosecutor or of the National Anti-Drug Secretariat (*Secretaría Nacional Antidroga - SENAD*). The application must contain details of the types of communications to be intercepted, the technical means proposed, and the objectives of the measure. The judge may request further evidence in support of the application and the subsequent order must explicitly identify the agents responsible for executing the interception and the duration of the authorization.

[11] Article 36, Paraguay's Constitution, http://www.bacn.gov.py/CONSTITUCION_ORIGINAL_FIRMADA.pdf (Spanish)
[12] Articles 89 and 90, Law n. 642/1995 (*Ley 642 - Ley de telecomunicaciones*), http://www.bacn.gov.py/leyes-paraguayas/2452/ley-n-642-telecomunicaciones (Spanish)
[13] Article 200, Criminal Procedure Code (*Ley 1286 - Código Procesal Penal*), http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish)
[14] Articles 88 and 89, Law n. 1881/2002 (*Ley 1881 - Modifica la Ley 1340 del 22 de noviembre de 1988 "que reprime el tráfico ilícito de estupefacientes y drogas peligrosas y otros delitos afines y establece medidas de prevención y recuperación de farmacodependientes*), http://www.bacn.gov.py/leyes-paraguayas/4423/ley-n-1881-modifica-la-ley-n-1340-del-22-de-noviembre-de-1988-que-reprime-el-trafico-ilicito-de-estupefacientes-y-drogas-peligrosas-y-otros-delitos-afines-y-establece-medidas-de-prevencion-y-recuperacion-de-farmacodependientes (Spanish)

Wiretapping and audiovisual electronic recording are also part of the information collection procedures established in Law 5241/2016, which creates the National Intelligence System (*Sistema Nacional de Inteligencia - SINAI*).[15] These can be applied to organized crime and drug trafficking investigations conducted by intelligence agencies.[16] The National Intelligence Secretary is the competent authority to request judicial authorization. The judge (*juez penal de garantías*)[17] has 24 hours to issue a reasoned decision, specifying the means to be used, the person or persons targeted, and the duration of the measure, which may not exceed 90 days, extendable only once up to the same duration.[18]

Access to the content of communications and metadata

The Criminal Procedure Code requires a previous judicial order to access stored communications content.[19] The interception regime set forth by Law 1881/2002, mentioned above, also applies to accessing stored content in illegal drug trade investigations.[20] Finally, a prior judicial order is mandatory for carrying out the information collection procedures set in the National Intelligence System Law, worded broadly enough to cover different measures aimed at accessing stored content. Such procedures include: (i) the intervention of telephone, computer, radio and correspondence communications in any of their forms; (ii) the intervention of computer systems and networks; and (iii) the intervention of any other technological systems intended for the transmission, storage, or processing of communications or information.[21]

With regard to metadata, a resolution from Paraguay's telecom regulatory body (*Comisión Nacional de Telecomunicaciones - CONATEL)* requires communication service providers to retain the inbound and outbound call records of their subscribers for six

[15] Article 25, Law n. 5241/2016, http://www.bacn.gov.py/leyes-paraguayas/4620/ley-n-5241-crea-el-sistema-nacional-de-inteligencia (Spanish)
[16] Article 24, Law n. 5241/2016.
[17] This is the judge responsible for authorizing the procedures and safeguarding the compliance with rights and principles set out in national and international law during the discovery stage. See article 282, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish)
[18] Article 26, Law n. 5241/2016, http://www.bacn.gov.py/leyes-paraguayas/4620/ley-n-5241-crea-el-sistema-nacional-de-inteligencia (Spanish)
[19] Articles 198 and 200, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish) See additional restrictions in article 194.
[20] Articles 88 and 89, Law n. 1881/2002, http://www.bacn.gov.py/leyes-paraguayas/4423/ley-n-1881-modifica-la-ley-n-1340-del-22-de-noviembre-de-1988-que-reprime-el-trafico-ilicito-de-estupefacientes-y-drogas-peligrosas-y-otros-delitos-afines-y-establece-medidas-de-prevencion-y-recuperacion-de-farmacodependientes (Spanish)
[21] Article 25, Law n. 5241/2016, http://www.bacn.gov.py/leyes-paraguayas/4620/ley-n-5241-crea-el-sistema-nacional-de-inteligencia (Spanish). As mentioned above, these procedures also include wiretapping and audiovisual electronic recording.

months.[22] Despite the privacy protections provided in the Constitution[23] and the Telecommunications Law,[24] the Paraguayan Supreme Court of Justice held that public prosecutors can directly request communications metadata without a previous judicial authorization.[25] The decision relied on the provision of the Criminal Procedure Code, establishing that prosecutors may require information from any person or public or private entity and stating that the inviolability protection refers to communications content, not metadata.[26] The metadata referred to in the ruling includes subscriber data, date, time, inbound and outbound telephone numbers, and the geolocation of the calls.

Finally, the E-commerce Law stipulates data retention obligations for connection and Internet traffic data for a minimum of six months, with the specific purpose of identifying the location of the equipment used or the origin of hosted content.[27] The law doesn't mention the legal requirements for accessing this data. It states, however, that the retention of connection-related information is carried out with the sole purpose of providing an effective Internet access service.[28]

Access to subscriber data

To the best of our knowledge, there's no specific provision about law enforcement access to subscriber data. However, the Supreme Court of Justice ruling n. 674/2010[29] leads to the understanding that prosecutors can directly request subscriber data without the need of a judicial order.

Identification by IP addresses

The Paraguayan Supreme Court of Justice ruling n. 674/2010 also affects the legal regime applied to identification via IP addresses. According to the decision, the access to subscriber data and metadata doesn't require judicial authorization. Although it refers to information related to phone calls, the ruling's rationale is that constitutional protections shield communications content, not the details about such communication.

[22] Article 1, Conatel Resolution n. 1350/2002 (*Resolución 1350/2002 - Establece la obligatoriedad de detalles de llamadas por el plazo de seis meses*), http://lcweb5.loc.gov/glin/jurisdictions/Paraguay/pdfs/93922-49353.pdf (Spanish)
[23] Article 36, Paraguay's Constitution http://www.bacn.gov.py/CONSTITUCION_ORIGINAL_FIRMADA.pdf (Spanish)
[24] Articles 89 and 90, Law n. 642/1995, http://www.bacn.gov.py/leyes-paraguayas/2452/ley-n-642-telecomunicaciones (Spanish)
[25] Supreme Court of Justice, Ruling n. 674/2010 ("*RECURSO EXTRAORDINARIO DE CASACIÓN interpuesto por la Defensora Pública Sandra Rodríguez Samudio en la causa ANASTACIO MIERES BURGOS y otros s/ SECUESTRO y otros*"), https://www.csj.gov.py/jurisprudencia/ (Spanish)
[26] Article 228, Criminal Procedure Code. The ruling mentions also the article 316, which sets a duty of assistance of public authorities and public servants in providing information. http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish)
[27] Article 10, Law n. 4868/2013 (*Ley - Comércio electrónico*), http://www.bacn.gov.py/leyes-paraguayas/961/ley-n-4868-comercio-electronico (Spanish)
[28] Article 2, f, Law n. 4868/2013.
[29] Supreme Court of Justice, Ruling n. 674/2010, https://www.csj.gov.py/jurisprudencia/ (Spanish)

Location data

According to the Supreme Court of Justice's ruling N. 674/2010, location data associated with telephone calls may be directly requested by public prosecutors. On real-time tracking, Paraguay's legislation does not contain any specific explicit provision.

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

Content and metadata

According to article 36 of the Paraguayan Constitution, private documents and communications of any kind may only be examined, reproduced, intercepted, or seized with a previous judicial order for cases specifically provided for in the law, and when *it is indispensable* for clarifying matters within the competence of the relevant authorities.[30] This provision feeds into the application of the communications intervention procedure set out in the Criminal Procedure Code, Article 200 of which stipulates it is *an exceptional measure*.[31] As for the information collection procedures established in the National Intelligence System Law, the required judicial authorization shall only be granted when the information sought cannot be obtained from public sources and is strictly necessary to fulfill the goals of safeguarding peace, national security, and institutional stability; protecting the people from terrorism, organized crime, and drug trafficking; and defending the rule of democracy.[32]

With regard to metadata, retention of and access to connection and Internet traffic data under the E-Commerce Law is bound to administrative purposes, within concerns of the good provision of services online.[33] Neither the Conatel resolution n. 1350/2002 nor the Supreme Court of Justice ruling n. 674/2010,[34] both applied to facilitate access to metadata in criminal investigations, set specific standards for such access.

Subscriber data

To the best of our knowledge there is no specific legal standard to access subscriber data in Paraguayan criminal legislation.

[30] Article 36, Paraguay's Constitution (*Constitución de la República del Paraguay*) http://www.bacn.gov.py/CONSTITUCION_ORIGINAL_FIRMADA.pdf (Spanish)
[31] Article 200, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish)
[32] Article 26, Law n. 5.241/2016, http://www.bacn.gov.py/leyes-paraguayas/4620/ley-n-5241-crea-el-sistema-nacional-de-inteligencia (Spanish)
[33] Articles 2, f and 10, Law n. 4868/2013, http://www.bacn.gov.py/leyes-paraguayas/961/ley-n-4868-comercio-electronico (Spanish)
[34] Conatel Resolution n. 1350/2002, http://lcweb5.loc.gov/glin/jurisdictions/Paraguay/pdfs/93922-49353.pdf (Spanish) and Supreme Court of Justice, Ruling n. 674/2010, https://www.csj.gov.py/jurisprudencia/ (Spanish)

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

According to criminal law,[35] the competent authorities to request access to communications data are: (i) public prosecutors,[36] (ii) the National Anti-Drug Secretariat (*SENAD*),[37] and (iii) the National Intelligence Secretary.[38]

In the intelligence sector, Decree 12515/1996 provides for the creation of the Intelligence Direction under the authority of the Homeland Secretary (known as "Ministerio del Interior"), which, as one of the agencies included in SINAI, has the power to request court orders for lawful interception of communications in order to preserve national security in accordance with the procedures set out above.

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

The Criminal Procedure Code sets out that, in extreme urgent cases, public prosecutors may verbally make requests for evidence-gathering procedures to the judge, who can authorize them without the regular service of process.[39] However, the Code doesn't define the meaning of "urgency" or "urgent cases."

9. Is there any data retention mandate?

Law 2340/2016, which amends the country's Consumer Protection Law, sets a retention obligation for subscriber data (name, surname, date of birth, and ID card number) applied to telecommunication services in general.[40] The data must be retained for a minimum period of one year after the service is canceled. The E-Commerce Law requires Internet access providers and Internet applications or services that host or store users'

[35] Article 26, Law n. 5241/2016, http://www.bacn.gov.py/leyes-paraguayas/4620/ley-n-5241-crea-el-sistema-nacional-de-inteligencia (Spanish)
[36] Articles 200, 316, and 318, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish). Also, article 88, Law n. 1881/2002, http://www.bacn.gov.py/leyes-paraguayas/4423/ley-n-1881-modifica-la-ley-n-1340-del-22-de-noviembre-de-1988-que-reprime-el-trafico-ilicito-de-estupefacientes-y-drogas-peligrosas-y-otros-delitos-afines-y-establece-medidas-de-prevencion-y-recuperacion-de-farmacodependientes (Spanish)
[37] Article 88, Law n. 1881/2002.
[38] TEDIC's chart provides an outline of the communications intervention procedure considering the Criminal Procedure Code and the Law n. 1881/2002: https://necessaryandproportionate.org/country-reports/paraguay (Section V - Institutional Framework)
[39] Articles 320 and 321, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish)
[40] Article 55, Law 2340/2016 (Ley 2340 - Amplía artículos de la Ley sobre Defensa del Consumidor y del Usuario), http://www.bacn.gov.py/leyes-paraguayas/5040/amplia-la-ley-n-1334-del-27-de-octubre-de-1998-de-defensa-del-consumidor-y-del-usuario (Spanish)

content to retain connection and traffic data for six months, for electronic commerce reasons.[41] It prohibits access to such data for any other purposes. In turn, Paraguay's telecom regulator Conatel issued a resolution that compelled companies to retain phone call and text messaging data for a six-month period.[42] Interpretations of Conatel's resolution seek to apply such obligation to Internet service providers, whose services are not specifically addressed by the regulatory text.

In 2014, a bill, dubbed "Pyrawebs" (an allusion to the police espionage that was conducted during the military dictatorship), sought to force ISPs to store users' metadata for 12 months for criminal investigation purposes. After a grassroots campaign against the bill, it was rejected in the senate.[43]

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

To the best of our knowledge, Paraguay's law does not have any specific reference to or authorization regarding the use of malware. However, the broad wording of *communications intervention* in the Criminal Procedure Code, covering "any technical means," might be interpreted by law enforcement to seek the use of malware in investigations.[44] The same haziness applies to the information collection procedures set out in the National Intelligence System Law, particularly: (i) the intervention of telephone, computer, radio, and correspondence communications in any of its forms; (ii) the intervention of computer systems and networks; and (iii) the intervention of any other technological systems intended for the transmission, storage, or processing of communications or information.[45]

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, nothing in Paraguay's legislation explicitly compels companies to provide law enforcement agents direct access to their servers. To the contrary, Millicom's Transparency Report states that Paraguayan authorities require the company to provide direct access to its mobile network. Millicom explains that the procedures allow the company to view the judicial order that is required for the authorities to initiate the interception, and to be aware when interception occurs.[46] As

[41] Articles 2, f and 10, Law n. 4868/2013, http://www.bacn.gov.py/leyes-paraguayas/961/ley-n-4868-comercio-electronico (Spanish)
[42] Article 1, Conatel's Resolution n. 1350/2002, http://lcweb5.loc.gov/glin/jurisdictions/Paraguay/pdfs/93922-49353.pdf (Spanish)
[43] TEDIC, "State Communications Surveillance and the Protection of Fundamental Rights in Paraguay", March 2016, item 2.4.3. Available at: https://necessaryandproportionate.org/country-reports/paraguay#footnoteref32_lf8ajpy
[44] Article 200, Criminal Procedure Code.
[45] Article 25, 1, 2, and 4, Law n. 5241/2016, http://www.bacn.gov.py/leyes-paraguayas/4620/ley-n-5241-crea-el-sistema-nacional-de-inteligencia (Spanish)
[46] 2018 Millicom Group Law Enforcement Disclosure (LED) Report, p. 10. Available at: https://www.millicom.com/media/3674/millicom-2018-led-report.pdf

previously pointed out, the broad wording both of *communications intervention* in the Criminal Procedure Code and *information collection procedures* in the National Intelligence System Law might be interpreted to substantiate the authorities' request.[47] However, this understanding should not prevail given the vagueness of the provisions and the disproportionate nature of the measure according to international human rights standards.

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

The Criminal Procedure Code sets out that the judge and the public prosecutors may request information from any person or public or private entity. The requests must indicate the procedures, the accused's name, where the report should be delivered, the deadline, and the consequences for a breach of this "duty to inform".[48] In addition, the Code states that the Public Prosecutor's Office will carry out all the acts of the fact-finding phase that don't require a judicial order or entail jurisdictional content. Within this legal competence, prosecutors may request information from any public official or employee. All public authorities are obliged to collaborate with the investigation, according to their respective competencies, and to comply with requests for reports made in accordance with the law.[49]

[47] Article 200, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish)
[48] Article 228, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish)
[49] Article 316, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish) and Article 25, Law n. 5241/2016, http://www.bacn.gov.py/leyes-paraguayas/4620/ley-n-5241-crea-el-sistema-nacional-de-inteligencia (Spanish)

TRANSPARENCY & COMMUNICATIONS PRIVACY

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

No.

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. Paraguay's Intelligence Law states that documents and files relating to intelligence and counterintelligence activities must be kept confidential for a period of up to 20 years as determined by the country's National Intelligence System (*Sistema Nacional de Inteligencia - SINAI*). Any institutions which become aware of such documents must keep both the existence and content of such documents confidential until they are declassified.[50] This obligation cannot halt the release of statistical data, since such data do not refer to a specific case, procedure, or document, but instead to aggregate, less specific information.

15. Do telecommunication companies publish transparency reports?

- **Tigo/Millicom** publishes annual transparency reports. However, the information on data requests that the company provides is aggregated per region, and not detailed per country.
- **Personal** does not disclose transparency reports.
- **Copaco** does not disclose transparency reports.
- **Claro** does not disclose transparency reports.
- **Vox** does not disclose transparency reports.
- **Chaco Comunicaciones** does not disclose transparency reports.

[50] Articles 22 and 23, Law n. 5241/2016 (*Ley 5241 - Crea el Sistema Nacional de Inteligencia (SINAI)*), http://www.bacn.gov.py/leyes-paraguayas/4620/ley-n-5241-crea-el-sistema-nacional-de-inteligencia (Spanish)

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

The Criminal Procedure Code provides, as a general rule, that parties should be notified the day after judges issue their decisions[51] Also as a general rule, the documents, objects, and other elements of conviction incorporated into the procedure are displayed to the accused. In the case of secrecy, the judge will examine them privately, assessing what is useful to be added to the procedure.[52] This is the rule set for communications intervention established in article 200 of the Code, and for the information collection procedures in the National Intelligence System Law.[53] The latter norm stipulates strict secrecy obligations on the existence and content of the procedures until the information is declassified.[54] Those who authorize, oversee, or carry out interception and recording of oral, cable or electronic communications within drug-trafficking investigations have also a secrecy legal duty.[55] Other measures can be carried out under secrecy at the prosecutors' request, provided it is essential for the investigation to be effective.[56] The prosecutor may request this only once and for a period that may not exceed ten calendar days.

[51] Article 151, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish)
[52] Article 227, Criminal Procedure Code.
[53] Article 27, Law n. 5241/2016, http://www.bacn.gov.py/leyes-paraguayas/4620/ley-n-5241-crea-el-sistema-nacional-de-inteligencia (Spanish)
[54] Articles 22 and 23, Law n. 5241/2016.
[55] Article 91, Law n. 1881/2002, http://www.bacn.gov.py/leyes-paraguayas/4423/ley-n-1881-modifica-la-ley-n-1340-del-22-de-noviembre-de-1988-que-reprime-el-trafico-ilicito-de-estupefacientes-y-drogas-peligrosas-y-otros-delitos-afines-y-establece-medidas-de-prevencion-y-recuperacion-de-farmacodependientes (Spanish)
[56] Article 323, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal (Spanish). According to the same article, the determination of secrecy may only be invoked for the benefit of the investigation and never to the detriment of the exercise of the defense.