The State of Communication Privacy Law in Argentina

Katitza Rodriguez,
International Rights Director
(EFF)

Veridiana Alimonti,
Latin American Senior Policy
Analyst (EFF)

In collaboration with:

Leandro Ucciferri (ADC)

Authors: Katitza Rodriguez and Veridiana Alimonti
Collaborators: Leandro Ucciferri (Asociación por los Derechos Civiles - ADC)

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

Yes, Argentina has a comprehensive data protection framework, Law 25.326/2000.[1]

2. Is there a data protection authority?

Yes, since 2017, the Access to Public Information Agency (*Agencia de Acceso a la Información Pública*) has been the new data protection oversight authority and has replaced the ex-National Data Protection Directorate (*Dirección Nacional de Protección de Datos Personales*).[2] The agency resides under the Chief of the Cabinet of Ministers,[3] and its director will serve five years in office with the possibility of being re-elected for a single time.[4]

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

As for data protection rules applicable to law enforcement agencies, Article 23 of the Data Protection Law stipulates which cases are subject to the law, and outlines some fundamental principles:[5]

- Personal data subject to the law are those stored for administrative purposes and permanently registered in an armed and security forces, police, or intelligence agencies database; as well as those personal background databases that have been handed over to the administrative or judicial authorities upon legal request.
- The processing of personal data for purposes of national defense or public security by the armed forces, law enforcement, and intelligence agencies, without the consent of those affected, must be limited to those categories of data that are necessary for the strict fulfillment of national defense, public security, or combat crimes. The database, in such cases, must be specific and established for that purpose, and must be classified by categories, according to their degree of reliability.
- Personal data registered for police purposes must be deleted when they are no longer necessary for the investigation.

[1] Data Protection Law - Law 25.326/2000 (*Ley 25.236 - Protección de los Datos Personales*).
http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm (Spanish).
[2] Article 19, Law 27.275/2016.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/texact.htm (Spanish).
[3] Article 19, Law 27.275/2016 (*Ley 27.275 - Derecho de Acceso a la Información Pública*).
http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/texact.htm (Spanish)
[4] Article 20, Law 27.275/2016.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/texact.htm (Spanish).
[5] Article 23, Law 25.236/2000.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm (Spanish).

Regarding the collection and processing of personal data held by the State, Article 8 of the Access to Public Information Act establishes some exceptions where data can not be obtain through access to information law:[6]

- Information expressly classified as reserved, confidential, or secret, for reasons of defense or foreign policy;
- Information that contains personal data and can not be secured through dissociation procedures, unless the processing of the data complies with the Data Protection Law's lawfulness principle;
- Information obtained in investigations considered confidential and disclosure of which could frustrate the success of an investigation.

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

Argentina has been considered a country that provides an adequate level of data protection according to EU standards.[7] The Argentinian Data Protection Law prohibits the transfer of personal data to any country or international organization that does not provide adequate levels of protection. This prohibition does not apply when the data subject has expressly consented to the transfer.[8]

Article 12.2 also stipulates cases in which this prohibition does not apply, such as international judicial collaboration; upon-agreed international treaties regarding transfer of personal data in which Argentina is a party; and international cooperation between intelligence agencies against organized crime, terrorism, and drug trafficking.

Finally, Law 24.767, in force since 1997, is the legal basis for international legal cooperation in criminal matters in Argentina. It establishes the rules of procedure applicable to all requests for international judicial assistance and extradition received by the country. In cases in which there is no treaty linking Argentina with the requesting State, Law 24.767 describes the procedure to grant assistance.[9]

[6] Article 8, Law 27.275/2016.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/texact.htm (Spanish)

[7] Article 45 of the EU General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-45-gdpr/
[8] Article 12, Law 25.326/2000.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm (Spanish).
[9] Law 24.767, http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=41442 (Spanish). More information here: http://www.cooperacion-penal.gov.ar/introduccion (Spanish)

COMMUNICATIONS PRIVACY LAW

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

Interception of communication

The interception of communications is conducted by an agency currently under the authority of the Supreme Court. The Department of Capturing of Communications of the Judiciary (*DCCPJ*, in Spanish) is the specialized agency in charge of intercepting all communications, upon a judicial request in criminal investigations.[10] This is in line with Law 19.798, which states that the interception of communications only proceeds at the request of a competent judge.

Those who work in telecommunication services must maintain the confidentiality of communications, an obligation which is extended to "any person" who learns about their content.[11] The Supreme Court has also held, in the Halabi case, that the law must meet the following criteria to justify intrusion into the private lives of individuals:[12]

- when the law determines the "cases" and "justifications" for which the content of such correspondence needs to be known;
- when the law supports the existence of a substantial or essential aim of the State;
- when such restriction is compatible with the pursued legitimate purpose;
- when the means of achieving it do not exceed what is strictly necessary.[13]

On December 24, 2015, President Macri moved the body responsible for carrying out the interception of communications from the Public Ministry to the Supreme Court. Decree 256/2015[14] states that the power to intercept communications should lie in authority "that is not part of the criminal investigation." The Decree task Argentina's Supreme Court to regulate the functioning of this body, which was done by Acordada 2/2016.[15] Both the decree and the acordada raised criticism among the country's civil society groups.[16]

---

[10] Article 150, Criminal Prosecution Code, Decree 118/2019, Annex I.
[11] Law 19.798/1972 (*Ley 19.798/1972 - Ley Nacional de Telecomunicaciones*), Articles 18-21. http://servicios.infoleg.gob.ar/infolegInternet/anexos/30000-34999/31922/texact.htm (Spanish). Law 19.798/1972 was repealed by the Law 27.078/2014 (*Argentina Digital)*, currently in force, with regard to conflicting articles; However, the process for communications interception remains under the old-1972 law and law 27.126 the new intelligence law. Law 27.126 transfers who conducts the interception (first the Ministerio Publico Fiscal, and now the Supreme Court). This law needs to be read jointly with the Criminal Procedure Code that sets the requirements on how those interceptions are authorized. The need for a prior judicial order is reasserted in article 5 of Law 27.078. http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm (Spanish).
[12] Halabi Case http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-halabi-ernesto-pen-ley-25783-dto-1563-04-amparo-ley-16986-fa09000006-2009-02-24/123456789-600-0009-0ots-eupmocsollaf (Spanish)
[13] Halabi Case, recital 25.
[14] Decree 256/2015 (http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257346/norma.htm) (Spanish)
[15] Supreme Court, Acordada 2/2016 (https://www.csjn.gov.ar/documentos/descargar/?ID=96793) (Spanish).
[16] The Association for Civil Rights (*ADC*) pointed out the discussion around the constitutionality of the decree as well as risks unfolded from vague and ambiguous provisions of the acordada, which could, for example,

Access to subscriber data

Access to subscriber information is not specifically protected by the Constitutional guarantee, which bars access to "private papers." Prosecutors can make a simple request to obtain subscriber data. There is neither law nor jurisprudence about this.

Access to the content of communications

Access to the content of communications is treated like an interception of communication. Judges are authorized to request interception in the course of the criminal investigations they conduct. The judge may order, upon the request of one of the parties, the interception and seizure of postal or telegraphic correspondence or any other object sent by or to the accused. Such intervention is exceptional and can only be carried out for a maximum period of 30 days, and may be renewed, stating the reasons that justify the extension based on the nature and circumstances of the investigated event. The request must indicate the duration that deemed necessary according to the circumstances of the case. The judge controls the legality and proportionality of the request and issues a substantiated decision. Companies that provide communications services must facilitate the immediate accomplishment of this surveillance task. Otherwise, they may also be held criminally liable. The interception must stop if the reasons used to authorize it is no longer valid, or once the period given has elapsed, or the aim achieved.[17]

In criminal investigations, the rules sanctioned through the former Code (Law 27.063) are still valid, since the implementation of the new Code is still in early stages. Only a few provinces have actually replaced it completely.

And for search and seizures: Article 18 of the Constitution regulates search and seizure. The Code of Criminal Procedure provision applies to the search of domiciles only. In Argentina, the concept of "search and seizure" does not apply directly to telecommunications or their metadata, location data, or content. However, Article 233-235 of the Code of Criminal Procedure allows for the interception of communications (see wiretapping) and for the seizure of personal belongings. Hence, the police can seize computers and phones, and their content can be searched and copied.

Access to metadata

There is no specific regulation on metadata but the Supreme Court in the Halabi decision has considered it at the same level as the private papers protected by Article 18 of the

lead to the understanding that prosecutors would have the ability to directly ask the body responsible for conducting interceptions to initiate such a procedure without a prior specific court order.

[17] Article 150, Criminal Procedural Code.

National Constitution.[18] Therefore, the same rules apply for *metadata* as for the actual contents of personal communications.

Location data

The rules for metadata apply to location data. The Halabi doctrine explained below applies to metadata including location data.

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

According to Article 150 of the Criminal Prosecution Code, the interception of communications may take place whenever it is useful for the verification of the offense. Although paragraph 2 states it is an exceptional measure, the provision doesn't stipulate further standards.[19] Similarly, the framework applied to intelligence activities sets out that the intelligence authority shall request the appropriate judicial authorization "when, in the development of intelligence or counterintelligence activities, it is necessary to carry out interceptions or captures of private communications of any kind.[20] Nevertheless, in the Halabi case, the Supreme Court stated that case law referring to the inviolability of correspondence should apply to the context of interception of communications. The inviolability of correspondence should be authorized when:

- there is a law determining the "cases" and "justifications" for which the content of such correspondence needs to be known;
- the basis of the law is the existence of a substantial or essential aim of the State;
- such restriction is compatible with the pursued legitimate aim; and
- the means to achieve it does not exceed what is strictly necessary.[21]

Article 10 of the Data Protection Law sets out the duty of secrecy for the processing of personal data. That duty may be relieved by judicial order and for reasons related to public safety, national defense, or public health.[22]

---

[18] The case is *Halabi* (Supreme Court of Argentina, decision of February 24, 2009). Article 18 of the National Constitution states the following:
"No inhabitant of the Nation may be punished without previous trial based on a law enacted before the act that gives rise to the process, nor tried by special committees, nor removed from the judges appointed by law before the act for which he is tried. Nobody may be compelled to testify against himself, nor be arrested except by virtue of a written warrant issued by a competent authority. The defense by trial of persons and rights may not be violated. *The domicile may not be violated, as well as the written correspondence and private papers; and a law shall determine in which cases and for what reasons their search and occupation shall be allowed. Death penalty for political causes, any kind of tortures and whipping, are forever abolished. The prisons of the Nation shall be healthy and clean, for the security and not for the punishment of the prisoners confined therein; and any measure taken with the pretext of precaution which may lead to mortify them beyond the demands of security, shall render liable the judge who authorizes it."
[19] Criminal Procedural Code, art. 150
https://www.argentina.gob.ar/normativa/nacional/decreto-118-2019-319681/texto (Spanish)
[20] Articles 18 and 19 of the Law 25.520/2001.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm (Spanish)
[21] Halabi case, recital 25.
http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-halabi-ernesto-pen-ley-25783-dto-1563-04-amparo-ley-16986-fa09000006-2009-02-24/123456789-600-0009-0ots-eupmocsollaf (Spanish).
[22]Article 10, Law 25.326/2000
http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm (Spanish).

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

The authorities with the legal capacity to request judicial authorization to carry out communications interception are:

- Fiscal Public Prosecutor (*Ministerio Público Fiscal*) in criminal investigations;[23]
- Federal Intelligence Agency, through its General Director.[24]

The Comisión Nacional de Comunicaciones can also access retained data related to the regulation of quality of telecommunications service.[25]

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

Argentina's new Criminal Prosecution Code has not explicitly reproduced the emergency exception provided in the old code, which allowed the Fiscal Public Prosecutor to directly order the intervention of a communication and request its associated data when there is a duly justified danger in delaying. The Prosecutor could immediately notify the judge, who then has 24 hours to validate the order.[26] In ADC's opinion, the new code is more restrictive. Article 142, paragraph e, states that the Public Prosecutor, and not the judge, can order the interception of communication or access to the associated data[27] in cases where the victim of an illegal deprivation of liberty finds himself and his life or physical integrity in imminent danger.[28] For all other cases, ADC states that prior judicial authorization is still necessary.

9. Is there any data retention mandate?

There is no specific general data retention obligation for traffic data in Argentina. Argentina's controversial data retention law was passed as an amendment to the National Telecommunications Law (*Artículo 45 ter*, *Ley Nacional de Telecomunicaciones*, *Ley 19.798*). This law and its secondary regulation compel all telecommunications companies and Internet service providers to possess the necessary resources to "capture and divert communications, to monitor them remotely upon the request of the Judicial Branch or the Public Ministry," and to keep such data for 10 years.[29] In May 2009, the

[23] Article 150 and 152, Criminal Procedural Code, https://www.argentina.gob.ar/normativa/nacional/decreto-118-2019-319681/texto (Spanish).
[24] Article 5 bis, 15 bis, and 18, Law 25.520/2001. http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm (Spanish).
[25] Resolución Nº 5/2013 http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/216915/norma.htm
[26] Article 236, Law 23.984/1991 - old Criminal Procedural Code. http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/383/texact.htm (Spanish).
[27] Article 150, Criminal Procedural Code states that the interception of communication shall proceed in an analogous way to a search. Article 142 paragraph e) authorized a search without a prior warrant. http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm (Spanish).
[28] ADC, Reflections on the creation of the DDC (*Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones*), February 2016, https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-de-comunicaciones/ (Spanish).
[29] Decree 357/2005 suspended the application of Decree 1563.

Argentinean Supreme Court, in the Halabi case, declared unconstitutional Article 45 ter of Law 19.798. The court annulled the data retention legislation due to lack of precision in its wording, and the court called the law a "drastic interference with the private sphere of the individual."

However, a couple of regulations imposed a narrower data retention obligation:

- Law 25.891 on Mobile Communications Services creates a national public registry of mobile users where users' personal, and domiciliary data should be registered. The law mandates mobile telecommunications companies to send "all the information on their users" to such registry.[30]
- Quality of Telecommunications Services Regulation: Article 6 of the country's Regulations on the Quality of Telecommunications Services requires providers to keep the data collected by their systems electronically for at least three years for quality assurance purposes.[31] Also, it stipulates that the enforcement authority (ENACOM) may request access to such data partially or in full.

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

There are currently no laws that explicitly authorize the use of malware, but there have been at least two instances of legislative debate to include such provisions in criminal procedure codes, both at the national level and in the City of Buenos Aires. In both cases, the chapters that incorporated these provisions were dropped during the legislative debate.[32]

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

There is no law that obliges companies to provide this kind of access.

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

Article 150 of the Criminal Procedure Code, concerning interception, stipulates that communication service providers must enable the measure to be immediately carried out, subject to criminal liability in case of noncompliance.[33] A general obligation for

[30] Law 25.891/2004 (*Ley 25.891 - Servicios de comunicaciones móviles*)
http://servicios.infoleg.gob.ar/infolegInternet/anexos/95000-99999/95221/norma.htm (Spanish)
[31] Resolution 580/2018, Annex I, Article 6 (*Resolución 580/2018, Anexo I - Reglamento de calidad de los servicios de tecnologías de la información y las comunicaciones*)
https://www.enacom.gob.ar/multimedia/normativas/2018/res580MM.pdf (Spanish)
[32] ADC, Spy Reform: Comments on the regulation of new surveillance techniques in the new reformed project (*Reforma Espia: Comentarios a la regulacion de nuevas tecncas de viglancia en el proyecto de reforma)*, April 2018, https://adcdigital.org.ar/portfolio/reforma-espia-nuevas-tecnicas-de-vigilancia-para-la-investigacion-penal/ (Spanish)
[33] Article 150 (6), Criminal Procedure Code,
https://www.argentina.gob.ar/normativa/nacional/decreto-118-2019-319681/texto (Spanish).

Internet Service Providers' to render information to the competent authorities is set by Law 27.078/2014.[34] In addition, the law establishes the penalties the telecommunications enforcement authority (ENACOM) may apply to companies for not complying with the law and the service's license obligations.[35]

[34] Article 62, g, Law 27.078/2014, http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm (Spanish).
[35] Article 67, Law 27.078/2014.

TRANSPARENCY & COMMUNICATIONS PRIVACY

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

The Argentinian State does not publish transparency reports.[36] However, in 2015, the Department of Interception and Capture of Communications (*Departamento de Interceptación y Captación de las Comunicaciones - DICOM*) published a transparency report detailing the number of interception requests regarding different types of investigated crimes.[37] In 2015, the Public Prosecutor's Office, supervised the Office of Communications Capturing (*Oficina de Captación de Comunicaciones - OCC*). Now, the OCC is under the jurisdiction of the Supreme Court. The OCC is the only organization with the legal authority to carry out the interception of communications in Argentina.

In 2018, INFOBAE published a story reporting the leaked number of interceptions and other statistical information. The story reported about 5,000 phone lines intervened, of which 90 were real-time interception of communications.[38]

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.

15. Do telecommunication companies publish transparency reports?

- Cablevision hasn't published any transparency reports.
- Telefónica - Movistar publishes yearly transparency reports
- Telecom hasn't published any transparency reports.
- Telecentro hasn't published any transparency reports.

[36] Abstract from Argentina Country Report. Verónica Ferrari and Daniela Schnidrig, Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina, EFF, August 2016. https://necessaryandproportionate.org/country-reports/argentina#footnoteref90_3pq1noe
[37] Procuración General, The Department of Interception of Communications presented its management report (*El Departamento de Interceptación y Captación de las Comunicaciones presentó su informe de gestión*), https://www.fiscales.gob.ar/procuracion-general/el-departamento-de-interceptacion-y-captacion-de-las-comunicaciones-presento-su-informe-de-gestion/ (Spanish).
[38] *See Los números de las escuchas que se hacen en el país,* https://www.infobae.com/politica/2018/04/10/los-numeros-de-las-escuchas-que-se-hacen-en-el-pais/ (Spanish).

- DIRECTV publishes yearly transparency reports, but with very little data regarding most of the Latin American countries.
- IPLAN hasn't published any transparency reports.

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

Argentinian criminal law does not include an obligation nor a prohibition to notify the individual, not even when the interception is over. The subject of the investigation may learn about the evidence used in a criminal proceeding. However, an individual may never learn about the evidence if it was irrelevant to an investigation and dismissed by the prosecutor or the judge.