The State of Communication Privacy Law in Colombia

Katitza Rodriguez,
International Rights Director
(EFF)

Veridiana Alimonti,
Latin American Senior Policy
Analyst (EFF)

In collaboration with:

Juan Diego Castañeda
(Fundación Karisma)

Authors: Katitza Rodriguez and Veridiana Alimonti
Collaborators: Juan Diego Castañeda (Fundación Karisma)

This report builds on the *State Communications Surveillance and the Protection of Fundamental Rights in Colombia* 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 Colombia" is released under a Creative Commons Attribution 4.0 International License (CC BY 4.0).

JUNE 2020

INTRODUCTION

This report provides condensed information on the rules for government access to communication data in criminal investigations in Colombia. 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. Colombia has adopted Law 1581 of 2012, also known as the General Data Protection Law (GDPL). It covers the protection of personal data by the public and private sector.[1] Data protection is a fundamental right in Colombia. This law is regulated by Decree 1377 of 2013.[2]

Colombia has another sectoral data protection law, Law 1266 of 2008, also known as the Financial Habeas Data, which sets out the data protection rules for financial and commercial personal data purposes.[3]

2. Is there a data protection authority?

Yes. The GDPL assigns the Superintendence of Industry and Commerce (SIC) as the Colombian Data Protection Authority. The SIC is not an independent agency since it's under the Executive branch, and the Ministry of Industry, Trade, and Tourism of Colombia. The SIC can issue sanctions.

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

Colombian data protection law applies to the personal data held by the public sector. However, the law also exempts databases whose purpose is national security, defense, prevention, detection, and monitoring and control of money laundering and terrorist financing, as well as intelligence and counterintelligence activities.

The Colombian Constitutional Court has stated that these exceptions are not excluded from the application of the data protection law but exempted from some of its provisions by virtue of their interests. Those exempted cases must be regulated by special and complementary statutory laws, which must be subject to the requirements of the proportionality principle. The Constitutional Court argued that special laws that deal with exempted areas must pursue a constitutional purpose, provide suitable means to achieve that goal, and establish a regulation that for the purpose pursued does not unreasonably sacrifice other constitutional rights, particularly the right to habeas data. In addition, compliance with guarantees and the limitation of habeas data within the limits of proportionality must be supervised and controlled by an independent body, whether common or sectoral.[4] Being said that, Karisma Foundation has stated that while data protection law principles apply, "there is no independent regulator to control and

[1] Law 1581 of 2012, and reviewed by the Colombian Constitutional Court Decision C-748 of 2011, http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html (Spanish)
[2] Decree 1377 of 2013, https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf (Spanish)
[3] Law 1266 of 2008, and reviewed by Colombian Constitutional Court Decision C-1011 of 2018.
[4] Constitutional Court Decision, October 6, 2011, http://www.secretariasenado.gov.co/senado/basedoc/c-748_1911.html#inicio (Spanish)

protect personal data held by or for intelligence purposes. As a result, the existing seven agencies with intelligence functions are not accountable to the data protection regulator of public agencies."[5]

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

Colombia has adopted its own "adequacy" standards different from the EU standards. Article 26 of the RNBD prohibits the transfer of personal data to any country that fails to provide an adequate level of data protection comparable to Colombian standards. The Colombian Superintendence of Industry and Commerce (SIC) set the Colombian standards of "adequacy," and they are considered a lower standard than the GDPR.[6]

Circular Externa 08 of 2017 has determined which countries comply with their own Colombian "adequacy" standards, which among others, include six criteria of accountability. Those countries are the 28 European Union countries as well as the ones that the European Union has established adequate,[7] plus the ones chosen by Colombia but not by the EU: Costa Rica, México and Perú. The U.S. is deemed to be adequate both in Colombia and the European Union.

That being said, the European Commission has not established that Colombia provides a comparable level of personal data protection to that in the European Union.[8]

[5] Dejusticia, Fundación Karisma and Privacy International, *Stakeholder Report Universal Periodic Review 30th Session - Colombia*, September 2017, https://privacyinternational.org/sites/default/files/2018-03/UPR_The%20Right%20to%20Privacy%20in%20Colombia_2017.pdf (Spanish)

[6] Nelson Remolina-Angarita, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010).

[7] "Those countries are: Alemania, Andorra, Argentina, Austria, Bélgica, Bulgaria, Canadá, Chipre, Costa Rica, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, España, Estados Unidos de América, Finlandia, Francia, Grecia, Guernsey, Hungría, Irlanda, Islandia, Isla de Man, Islas Faroe, Italia, Japón, Jersey, Letonia, Lituania, Luxemburgo, Malta, México, Noruega, Nueva Zelanda, Países Bajos, Perú, Polonia, Portugal, Reino Unido, República Checa, República de Corea, Rumania, Serbia, Suecia, Suiza, Uruguay, https://docs.google.com/spreadsheets/d/1IMz6_Cr6zhkObCkanBV-_2Gn3pdiGZpnbsCj5_EWFec/edit#gid=0 (Spanish)

[8] European Commission, How the EU determines if a non-EU country has an adequate level of data protection, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents (Spanish).

COMMUNICATIONS PRIVACY LAW

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

Interception of communication and metadata

The Constitutional Court has stated that, as a general rule in the Colombian legal system, a judge's authorization is necessary if there is interference with a fundamental right of the investigated or accused.[9] However, as an exception to the general rule, when the Office of the Attorney General is given the power to interfere with an individual's rights for the purpose of collecting information relevant to a criminal investigation, these actions are subject to subsequent judicial review, and not prior authorization.[10] This means in practice that the prosecutor proceeds with the interception and then asks the judge to approve if the intercepted material can be used as evidence, but after the interception has already been carried out.

This exception for subsequent judicial review applies only in the cases of searches, house visits, seizures, and interceptions of communications.[11] The exception must be strictly interpreted so that the safeguard of a prior judicial authorization is not superfluously bypassed. Under this rule, for example, the Constitutional Court has held that practices like selectively searching a database for an accused person's confidential information requires prior judicial authorization.[12] A 2011 administrative regulation has defined interception very broadly to include not only the content of communication, but also the related metadata. It defines interception as the acquisition, display, capture, or copy of content or part of the content of a communication, including traffic data, by wire, electronic, optical, magnetic, or other forms."[13] Therefore, an interception order is needed for both types of data.

Article 235 of the Criminal Procedural Code defines the process for an interception order. It states that the prosecutor may order, only for evidentiary purposes, the interception

[9] Pedro Pablo Camargo's complaint of unconstitutionality against the second paragraph of Article 2, the third paragraph of Article 3 and the first section of Article 5 of Legislative Act N°.03 of 2002, "which reforms the National Constitution", sentence C-1092, Constitutional Court, November 19, 2003, http://www.corteconstitucional.gov.co/relatoria/2003/C-1092-03.htm (Spanish)

[10] The Criminal Procedure Code establishes the cases and the procedures in which the Office of the Attorney General may use this power. It indicates that the interception of communications (i) may take place to search for material elements of evidence transmitted through any type of communication that are important to the criminal investigation, (ii) must be justified in writing, (iii) must not be conducted on the communications of the accused and his or her defense lawyer, (iv) must have a maximum validity of three months, and (v) must be subjected to judicial control within 36 hours.

[11] Alejandro Decastro González's complaint of partial unconstitutionality against Articles 14, 244, and 246 of Act 906 of 2004 "Which draws up the Criminal Procedure Code," sentence C-336, Constitutional Court, May 9, 2007, http://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm (Spanish)

[12] Alejandro Decastro González's complaint of partial unconstitutionality against Articles 14, 244, and 246 of Act 906 of 2004 "Which draws up the Criminal Procedure Code," sentence C-336, Constitutional Court, May 9, 2007, http://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm (Spanish)

[13] The Colombian Communications Regulation Commission Resolution 3067 of 2011, https://www.crcom.gov.co/recursos_user/Normatividad/Normas_Actualizadas/Res_3067_Act_4807_15.pdf (Spanish)

of telephone, radiotelephone, and similar communications that use the electromagnetic spectrum, whose information is of interest for the purposes of the investigation. The Prosecutor must send such interception orders to the telecom network and service providers.[14] The interception of the defendant's communications is forbidden. The interception order will have a maximum validity of three months, but it may be extended if, in the opinion of the prosecutor, the justification that authorizes the order remains valid.[15]

Location data and other identifiers

Location data can also be accessed with an interception order as per article 235 explained above. Article 5 of Decree 1704 of 2012 authorizes telecom, network, and service providers to provide data about communications, including location. Such data includes geographic coordinates, signal potency, and "other information" that helps to determine the geographic location of the terminal, equipment, or devices. Content and Internet application providers are excluded from this provision. The real-time location-tracking provisions in Article 4 are unclear about the type of data that should be turned over in real time to the General Prosecutor's Office. According to this article, the data should be "the specific information contained in the companies' databases, such as sectors, geographic coordinates, and signal potency, among others."

Subscriber data

Colombian law does not require a judicial authorization before disclosing users' subscriber data for criminal investigations. According to Article 4 of Decree 1704 of 2012, as part of an interception order, the telecom network and service providers are obliged to disclose subscriber's data (identity, billing address, type of connection) to the Prosecutor and other competent authorities immediately upon request. The 2016 ruling of the Colombian Council of State declares nulled the term "or other competent authorities" of article 4, clarifying that subscriber's information can only be requested by the Prosecutor (Attorney General's Office).[16]

Stored data

Article 236 of the Criminal Procedural Code states that the prosecutor can order the seizure of the computers, servers, floppy disks, and/or media storage that the accused may have used while browsing the internet or using other technology that produce equivalent effects, if the prosecutor has reasonably well-founded reasons to infer that the accused has been transmitting useful information for the investigation. The seized equipment must be returned immediately. The standards applicable are analogous to those for search and seizures.[17]

---

[14] The Colombian Communications Regulation Commission Resolution 3067 of 2011, https://www.crcom.gov.co/recursos_user/Normatividad/Normas_Actualizadas/Res_3067_Act_4807_15.pdf (Spanish)
[15] Article 235 of the Criminal Procedural Code.
[16] Sala de lo Contenciosos Administrativo, Decree 1704 de 2012, Ferney Camacho vs Ministerio de Justicia, February 2016, http://www.suin-juriscol.gov.co/clp/contenidos.dll/ConsejoEstado/30033603?fn=document-frame.htm$f=templates$3.0 (Spanish)
[17] Articles 236 and 237 of the Criminal Procedure Code.

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

Colombian criminal procedure law establishes that communications can only be intercepted for the sole purpose of collecting evidence for a criminal investigation regardless of the potential crimes being investigated.[18] There is no other legal standard, such as probable cause or reasonable suspicion, on record. According to Article 250 of the Constitution, the Office of the Attorney General must take possession of the evidence in the framework of a criminal investigation. It specifies that when a measure interferes with a fundamental right, the appropriate authorization must be obtained from the judge responsible for the control of guarantees in order to validate the evidence gathered by the interception procedure.

The case law of the Constitutional Court states that intelligence activities must be clearly and specifically established by law, which must explain in detail the proceedings to conduct them, the officials who may authorize them, and the motivations underlying the authorization; pursue constitutionally legitimate aims, like the protection of constitutional democracy, national security and national defense; be necessary, i.e. be strictly required to fulfill this responsibility; and incorporate elements of accountability, such as periodic intelligence and counterintelligence reports and records of authorized and conducted activities.[19]

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

Criminal procedure legislation stipulates that "competent authorities" shall be in charge of the technical proceedings for communication interception and its processing. Despite the vagueness of the law in relation to the authorities in charge of conducting the proceedings, the Constitutional Court states that the law does specify which authority gives the order and conducts the interception: the Office of the Attorney General of the Nation (*Fiscalía General de la Nacion*), which is granted by law the power to determine which authorities conduct the interception of communications.[20]

While the law does not identify who these "competent authorities" should be, this may be determined through a systematic interpretation of the regulations related to the technical proceedings of communications interceptions. Interpreting Article 46 of Act

[18] Art. 235, Criminal Procedure Law, http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

[19] Taking up the definition contained in the collection of the United Nations Best Practices Section about intelligence and counterintelligence. Constitutionality revision of the statutory bill nº 263/11 Senate and 195/11 House, "which issues regulations to strengthen the legal framework that allows the organisms conducting intelligence and counterintelligence organisms to accomplish their constitutional and legal mission, and which lays down other provisions," sentence C-540, Constitutional Court, July 12, 2012, http://www.corteconstitucional.gov.co/ relatoria/2012/c-540-12.htm

[20] Abstract from Colombia Country Report. Juan Camilo Rivera and Katitza Rodriguez, "State Communications Surveillance and the Protection of Fundamental Rights in Colombia," Comisión Colombiana de Juristas, the Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

938 of 2004, the Court lays down that the aforementioned competence devolves upon the judicial police authorities assigned to the case.[21]

Entities that have permanent powers of the Judicial Police are:[22]

- Office of the Attorney General of the Nation and its public servants who perform judicial functions
- Judicial Police: C.T.I., National Police, and D.A.S. (*Departamento Administrativo de Seguridad*) empowered by a commission of the competent judicial authority and by legal mandate
- Unified Action Groups "Anti-Kidnapping and Extortion[23]

Judicial Police in matters within their competence:[24]

- General Comptroller of the Nation
- Office of the Attorney General of the Nation
- National Directorate of National Taxes and Customs - DIAN
- Public entities that exercise functions of surveillance and control
- Mayors and police inspectors, in parts of the country where there are no members of the Judicial Police of the National Police
- National and regional INPEC directors, the directors of detention facilities and custody, and surveillance personnel, in accordance with the provisions of the Penitentiary and Prison Code
- Police Inspections

Law 734 of 2002 Single Disciplinary Code enumerated which are the competent authorities:[25]

- Police officers with authorization from the Public Ministry (Ministerio Publico) and order to investigate
- Summary judge in inquisitive Criminal Procedure Code
- State intelligence agencies with prior judicial authorization

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

[21] Dagoberto José Lavalle's complaint of partial unconstitutionality against Article 52 of Act 1453 of 2011, "Which reforms the Criminal Procedure Code, the Children's and Adolescents' Code, the rules on the extinction of property law and stipulates other measures in relation to security," sentence C-594, Constitutional Court, (August 20, 2014).
http://www.corteconstitucional.gov.co/RELATORIA/2014/C-594-14.htm
[22] Article 312 of the code of Criminal Procedure.
[23] See also Telefonica, Transparency of the Communications Report, 2019.
https://www.telefonica.com/es/web/negocio-responsable/informe-de-transparencia-en-las-comunicaciones
[24] See also Telefonica, Transparency of the Communications Report, 2019.
https://www.telefonica.com/es/web/negocio-responsable/informe-de-transparencia-en-las-comunicaciones
[25] See also Telefonica, Transparency of the Communications Report, 2019.
https://www.telefonica.com/es/web/negocio-responsable/informe-de-transparencia-en-las-comunicaciones

Article 38 (e) of Act 137 of 1994 allows the national government to intercept or record communications during situations of internal disturbance "with the sole purpose of finding judicial evidence or preventing the commission of crimes," as long as there is judicial authorization.[26] The authorization can be given verbally when there are "insurmountable circumstances of urgency and it is necessary to protect a fundamental right in grave and imminent danger". The authorizations should be registered in a special record where the verbal or written order must be registered, indicating the time, place, and reason, the names of the people affected by the order, and the authority requested by them.[27]

9. Is there any data retention mandate?

Yes. Decree 1704 of 2012 stipulates that "network providers and telecommunications service providers must keep their users' information up-to-date and store subscriber data (identity, billing address, type of connection) and geolocation for at least five years."[28]

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

There is no precise legal framework in Colombia that authorizes law enforcement use of malware to intrude or hack a computer or device. However, "hacking" (unauthorized access to an information system) is a criminal offense according to article 269 A of the Colombian criminal code.

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

Resolution 912 of 2008 sets out that telecommunications services providers must allow the Directorate of Criminal Investigation (*Dijín*, in Spanish) to make a remote connection to obtain subscribers' data, such as names, home address, mobile number, and service activation date. The[29] Resolution does not oblige telecom companies to grant any form of direct access to the companies' internal infrastructure and servers, which can affect the integrity and security of the companies' infrastructure. However, the Resolution does grant Dijín the ability to carry individualized "queries" for each subscriber and compels telecom companies to provide a username and password

[26] This rule was endorsed by the Constitutional Court in the Constitutional Revision of the draft statutory bill 91/92 Senate and 166/92 House "which regulates the state of emergency in Colombia," sentence C-179, April 13 1994: http://www.corteconstitucional.gov.co/relatoria/1994/C-179-94.ht (Spanish)
[27] Articles 301 & 302 Procedural Criminal Code.
[28] Abstract from Colombia Country Report. Juan Camilo Rivera and Katitza Rodriguez, "State Communications Surveillance and the Protection of Fundamental Rights in Colombia," Comisión Colombiana de Juristas, the Electronic Frontier Foundation, & Fundación Karisma, (2016).
https://necessaryandproportionate.org/country-reports/colombia
[29] Resolución 912 of 2008, published in the official diary on January 2009,
http://www.avancejuridico.com/actualidad/documentosoficiales/2009/47233/r_mdef_0912_2008.html
(Spanish).

for such individualized queries. The company is obliged to also provide access to a database (either a read-only copy of a repository or a database mirror or replica of their actual database) through a web interface as well as to send Dijín a copy of a CD-DVD with the list of subscribers every first five days of each month.

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

Article 2 of Decree 1704 of 2012 forces telecom and network providers operating in Colombia to provide the technical capability to intercept communications in "national defense, prevention of states of emergency, and public safety" cases. The decree compels them to implement and guarantee the "technological infrastructure to provide interconnection points and access to communications data by the judicial police, following a Prosecutor's Office's request." [30]

The Ministry of Information and Communication Technologies also forces telecom and service providers to comply with the above provisions as a precondition of their license renewal to use Colombian radio-spectrum.[31]

In case of intelligence and counterintelligence, Article 44 (1) of Law 1621 of 2013 forces telecom and service providers to provide the Attorney-General's office and the Ministry of Information and Communication Technologies with the necessary equipment to allow them to intercept communications if the technology changes.[32]

[30] Decree 1704 of 2012, https://www.mintic.gov.co/portal/604/articles-3559_documento.pdf
[31] Article 3 of Decree 2044 of 2013
[32] Article 44 of Law 1621 of 2013.

TRANSPARENCY & COMMUNICATIONS PRIVACY

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

To the best of our knowledge, the government of Colombia has not published reports on the number of requests to access personal data.

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

To the best of our knowledge, there is no normative framework that prohibits a company 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?

- Claro publishes a sustainability report that includes a chapter on a Transparency Report, but with no statistical information about communications data requests .[33]
- Telefónica-Movistar publishes its transparency report every year.[34]
- ETB's latest transparency report refers to 2017-2018.
- AT&T-DirecTV: AT&T publishes annual transparency reports with generic information about data requests made to all its subsidiaries, including DIRECTV. There are no country-level transparency reports for any country except Mexico.
- Millicom-Tigo publishes yearly transparency reports. However, the information on data requests that the company provides is aggregated per region, and not detailed per country. In 2018 Tigo-Une published a specific report for Colombia.
- EMCALI does not publish transparency reports.

[33] See page 41.
[34] Transparency report, available at https://www.telefonica.com/documents/153952/183394/Informe-Transparencia-Comunicaciones-2018.pdf/5a54f445-e95f-4b71-e549-e9f6d1eb5b7d

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

In Colombia, there is no legal provision that establishes a mandatory obligation to notify the user that their data was requested by the State.