The State of Communication Privacy Law in Chile

Katitza Rodriguez,
International Rights Director
(EFF)

Veridiana Alimonti,
Latin American Senior Policy
Analyst (EFF)

In collaboration with:

Pablo Viollier (Derechos
Digitales)

Authors: Katitza Rodriguez and Veridiana Alimonti
Collaborators: Pablo Viollier (Derechos Digitales)

This report builds on the *State Communications Surveillance and the Protection of Fundamental Rights in Chile* 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 Chile. 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, Chile became the first Latin American country with a data protection law in 1999 - Law 19.628.[1]

2. Is there a data protection authority?

Chile does not have a proper data protection authority that oversees companies' compliance with data protection law. Due to such limitations, in many cases legal violations must be addressed in courts, which imposes a higher barrier to complaints grounded in the law and impairs their enforcement.[2] However, the Access to Information Law created the Council for Transparency (*Consejo para la Transparencia*), an oversight body to monitor government administration bodies' compliance with data protection law.[3] Although the Council for Transparency meets relevant independency requirements, such as administrative autonomy,[4] it cannot impose penalties,[5] and has a limited range of action in regard to data protection.[6]

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

Law 19.628/1999 applies to the processing of personal data by companies and government entities,[7] with no specific exception for law enforcement activities. Government entities can process personal data for matters within their authority, which does not require data subject's consent.[8] Government entities that process personal data related to convictions for criminal, administrative, or disciplinary offenses will not be able to use such personal data if the criminal or administrative action has reached the end of its limitation or prescription period.[9] The Public Prosecutor's Office has

[1] Data Protection Law - Law n. 19.628/1999 (*Ley 19.628 - Sobre protección de la vida privada*). https://www.leychile.cl/Navegar?idNorma=141599 (Spanish).
[2] *See* Articles 16 and 23, Data Protection Law.
[3] Article 33, m, Law 20.285/2008 (*Ley 20.285 - Sobre Accesso a la Información Pública*) https://www.leychile.cl/Navegar?idNorma=276363 (Spanish).
[4] *See* Articles 31,36, 38, and 41, Law 20.285/2008, https://www.leychile.cl/Navegar?idNorma=276363 (Spanish).
[5] *See* Derechos Digitales, "El Estado de la Protección de Datos en Chile," 2017, p.26-27 https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf (Spanish).
[6] The Asociación por los Derechos Civiles' report on the data protection system in Latin America highlights that experts disagree whether it's a broad or limited oversight power in regard to personal data processing by Chile's public administration. *See* more in page 31: https://adcdigital.org.ar/portfolio/sistema-proteccion-datos-personales-latam/ (Spanish).
[7] Article 1, Data Protection Law, https://www.leychile.cl/Navegar?idNorma=141599 (Spanish).
[8] Article 20, Data Protection Law.
[9] Article 21, Data Protection Law.

developed a protocol procedure for communications interception and other requests that ISPs have agreed to. However, it is secret to the general public.[10]

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

Chile's data protection law does not provide any specific rules regarding transfer of personal data to third countries.

[10] This protocol is mentioned in Entel's transparency report (*Protocolo de implementación y coordinación en materia de solicitudes de interceptación de comunicaciones telefónicas, otras formas de telecomunicaciones y otras solicitudes emanadas del Ministerio Público de Chile*): http://www.entel.cl/legales/pdf/Requerimientos-de-Datos-Personales-2019.pdf (Spanish).

COMMUNICATIONS PRIVACY LAW

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

Chile's Constitution ensures the inviolability of all forms of private communications. The interception, access to, or recording of any private communications or documents are only allowed as per the cases and means set by law.[11] Article 9 of Chile's Criminal Procedure Code requires prior judicial authorization to all proceedings that affect, deprive, or restrict the constitutional rights of the accused or a third party.[12]

Interception of communication

The Criminal Procedure Code requires that the interception and recording of communication be authorized by a judge (*juez de garantía*).[13] A judge can order the interception and recording of telephone communications or other forms of telecommunication at the request of the public prosecutor.[14] Such an order must indicate the name and address of the person affected, the type of interception, and its duration, which may not exceed sixty days. The judge may extend this term for equal periods, each time examining the interception requirements set in the law.[15] In case of drug trafficking- or money laundering-related offenses, name and address may be replaced by other information sufficient to identify or determine the person affected.[16] There is no additional requirement in the law that addresses terrorism offenses and authorizes the public prosecutor to request the judge (*juez de garantía*) the interception of telephone and electronic communications.[17]

[11] Article 19 (5), Political Constitution of the Republic of Chile (*Constitución Política de la República de Chile)*, https://www.leychile.cl/Navegar?idNorma=242302 (Spanish).
[12] Law N. 19.696/2000 (Ley 19.696 - *Establece Código Procesal Penal*), https://www.leychile.cl/Navegar?idNorma=176595 (Spanish)
[13] *Juez de garantía* is a judge responsible for protecting the rights and guarantees of who's being investigated as well as the legality of the investigative process conducted by the public prosecutor. After the indictment, the case goes to a court formed by three judges (*Tribunal de Juicio Oral*). This seeks to ensure that the suspect is judged by an impartial entity that has not participated in the investigation stage.
[14] Article 222, Law 19.696/2000 https://www.leychile.cl/Navegar?idNorma=176595 (Spanish). The procedure is regulated by the Decree 142/2005 (Decreto 142 - Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación) https://www.leychile.cl/Navegar?idNorma=242261 (Spanish)
[15] Article 222 (4), Law 19.696/2000.
[16] Article 24, Law 20.000/2005 (Ley 20.000 - *Sustituye la Ley n. 19.366, que sanciona el tráfico ilícito de estupefacientes y sus sustancias sicotrópicas*) https://www.leychile.cl/Navegar?idNorma=235507 (Spanish) and Article 33 (a), Law 19.913/2003 (Ley 19.913 - *Crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos*) https://www.leychile.cl/Navegar?idNorma=219119 (Spanish)
[17] Art. 14, Law 18.314/1984 (Ley 18.314 - *Determina conductas terroristas y fija su penalidad*) https://www.leychile.cl/Navegar?idNorma=29731 (Spanish).

Specific sectors of the Chilean police covered by the Intelligence Law (*Carabineros de Chile*[18] and the *Policía de Investigaciones de Chile*[19]) are also entitled to request a judicial order to intercept communications.[20] Article 24 of the law authorizes special procedures to obtain information such as wiretapping and electronic recording, including audiovisual; the intervention of telephone, computer, radio, and correspondence communications in any form; the intervention of computer systems and networks; and the intervention of any other technological systems for the transmission, storage or processing of communications or information.

For all the procedures established in Article 24, the request will be examined by a Minister of the Court of Appeal (*Ministro de la Corte de Apelaciones*) of the territory in which the procedure is conducted or initiated.[21] A judicial order authorizing or denying the interception must be founded and will be issued without hearing or intervention of the affected party or third parties. The authorization must include specification of the means to be used, the identity of the person or persons affected, and the duration, which may not exceed 90 days, extendable only once for an equal period. The directors or heads of the requesting police agency may appeal the decision in case the request is denied.[22]

Access to the content of communications and metadata

At the request of a prosecutor, the judge may authorize, by reasoned decision, the retention of postal, telegraphic, or other type of correspondence as well as issue an order to obtain copies or backups of the electronic correspondence addressed to or sent by the accused.[23] A judge (*juez de garantía*) may also order, upon a prosecutor's request, any copies or versions of the communications transmitted or received by the hosting company.[24] The same requirement applies for accessing the list of authorized ranges of IP addresses, subscribers' IP numbers, and connection logs. Although the provisions demanding access to retained data do not explicitly mention the necessity of a prior judicial order,[25] such a measure is required by Article 9 of the Criminal Procedure Code.

Stored content and traffic data may also be obtained by the police through the broad provisions set in Article 24 of the Intelligence Law, which refers to the intervention of

[18] *Carabineros de Chile* (Carabiniers of Chile) is a military and technical police institution, which integrates the public security forces; its purpose is to ensure and maintain public order and internal public security throughout Chile's territory and to fulfill the other functions entrusted to it by the Constitution and the law. *See* Article 1, Law 18.961/1990 (Ley 18.961 - *Ley Orgánica Constitucional de Carabineros de Chile*), https://www.leychile.cl/Navegar?idNorma=30329 (Spanish)

[19] *Policía de Investigaciones de Chile* (PDI), or Chile's Investigation Police, is the main police institution in the country responsible for carrying out criminal investigations, assisting the Public Prosecutor's Office in the investigation procedures.

[20] Article 24 (c), Law 19.974/2004, https://www.leychile.cl/Navegar?idNorma=230999 (Spanish)

[21] Article 25, Law 19.974/2004.

[22] Article 28, Law 19.974/2004.

[23] Article 218, Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish). *See* also Article 14, Law 18.314/1984, https://www.leychile.cl/Navegar?idNorma=29731 (Spanish).

[24] Article 219, Law 19.696/2000. *See* also Article 24, Law 20.000/2005, https://www.leychile.cl/Navegar?idNorma=235507 (Spanish) and Article 33 (a), Law 19.913/2003, https://www.leychile.cl/Navegar?idNorma=219119 (Spanish).

[25] Article 222 (5), Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish) and Article 6, Decree 142/2005, https://www.leychile.cl/Navegar?idNorma=242261 (Spanish).

telephone, computer, radio, and correspondence communications in any form; the intervention of computer systems and networks; and the intervention of any other technological systems for the transmission, storage, or processing of communications or information.[26] In those cases, the Carabineros of Chile or the country's Investigation Police must request a judicial order following the Intelligence Law procedure described in the previous item.

Access to subscriber data

To the best of our knowledge, there's no specific provision about law enforcement access to subscriber data. However, procedures should consider the general requirement set out in Article 9 of the Criminal Procedure Code, which requires prior judicial authorization.[27]

Identification by IP addresses

According to the Criminal Procedure Code[28] and the communications interception regulation,[29] telecommunications companies must retain and disclose to the Public Prosecutor's Office the list of authorized ranges of IP addresses and of subscribers' IP numbers and connection logs. As previously mentioned, prosecutors must request a prior judicial authorization to have access to the retained information under Article 9 of the Criminal Procedure Code.[30]

Location data

Chile's legislation does not have explicit legal authorization for real-time tracking or specific provision for location data. For the use of malware, which could enable real-time access to location data, see question 10.

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

Content and metadata

According to the Criminal Procedure Code, a judge (*juez de garantía)* can grant a telephone and telecommunications interception order when it is indispensable for the investigation and there is reasonable suspicion, based on the particular facts, suggesting that a person has committed or is organizing a crime. The law limits the crimes that may be investigated in this way to those that would be punishable by at least five years and a day of imprisonment.[31] Hence, the lawful authorization of telecommunications

[26] Art. 24, Law 19.974/2004, https://www.leychile.cl/Navegar?idNorma=230999 (Spanish).
[27] Article 9, Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish).
[28] Article 222 (5), Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish).
[29] Article 6, Decree 142/2005, https://www.leychile.cl/Navegar?idNorma=242261 (Spanish).
[30] Article 9, Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish).
[31] Article 222, Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish). According to Article 222 , interception is only allowed to investigate suspects who have participated "in a punishable act that commands a crime penalty." Crime sentences start in five years and one day, as set out in Article 56 of Chile's Criminal Code - https://www.leychile.cl/Navegar?idNorma=1984 (Spanish). Article 24 of the Law

interception under this norm must comply with the proportionality test: necessity (the measure should be imperative to the investigation), adequacy (the circumstances and facts of the case should be analyzed), and proportionality, in the strict sense (the offense under investigation should be punishable as a crime subjected to at least five years and one day of imprisonment).[32]

The same standard applies to access to retained IP addresses and subscribers' IP numbers and connection logs, since the provisions for requiring retention and authorizing access are within the context of telecommunications interception rules.[33] As for correspondence retention and seizure, Article 218 of the Criminal Procedure Code states that it may be authorized by a judge when, for well-founded reasons, its usefulness for the investigation is foreseeable. Article 219 does not provide any specific standard for obtaining copies of communications and transmissions from communications' companies.[34] The law that addresses terrorism offenses, known as "Anti-terrorism Law," authorizes the interception and recording of telephone and electronic communications, and the access to the investigated person's correspondence by a reasoned judicial decision during the hearing that formalizes an investigation, or after it is formalized, when a pre-trial detention measure applies.[35]

The Intelligence Law sets a different legal standard when it comes to any of the procedures outlined in Article 24 (including telecommunications interception), all of which require a judicial order. According to Article 23, such special procedures may be used when certain information is strictly indispensable for the fulfillment of the objectives of the State Intelligence System[36] and cannot be obtained from any other public source. Moreover, such procedures will be limited exclusively to intelligence and counterintelligence activities that aim to safeguard national security and protect the country against terrorism, organized crime, and drug trafficking.

One important ruling of Chile's Constitutional Court, n. 2153-11, sets out in recital 40:

> The model designed by the legislator to intercept, open or register private communications and the documents associated with them, is consistent with the standards designed by this Court, which has required restrictive permissions

20.000/2005 and Article 33 (a) of the Law 19.913/2003 addressing the access to communications data for the investigation of drug trafficking or money laundering-related offenses, respectively, apply the regime set by the Criminal Procedure Code. *See* Question 5 (*Interception of communication/wiretapping*).

[32] Derechos Digitales, "State Communications Surveillance and the Protection of Fundamental Rights in Chile", July 2016, item 2.2.1. Available at: https://necessaryandproportionate.org/country-reports/chile#footnoteref36_4ck28s5. The report also mentions and details a Public Prosecutor's Office norm that outlines the procedure it should adopt for interception requests.

[33] Article 222 (5), Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish) and Article 6, Decree 142/2005, https://www.leychile.cl/Navegar?idNorma=242261 (Spanish).

[34] Article 218 and 219, Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish).

[35] Art. 14, Law 18.314/1984, https://www.leychile.cl/Navegar?idNorma=29731 (Spanish).

[36] Article 4 defines the State Intelligence System as the set of intelligence agencies, independent of each other, functionally coordinated, that direct and execute specific intelligence and counterintelligence activities, to advise the President of the Republic and the various higher levels of State conduction, with the objective of protecting national sovereignty and preserving the constitutional order, and that, in addition, formulate useful intelligence assessments for the achievement of national objectives. Law 19.974/2004, https://www.leychile.cl/Navegar?idNorma=230999 (Spanish).

(STC 389/2003), with objective, precise, and non-discretionary parameters (STC 198/95, 1894/2011), subject to control (STC 389/2003, 433/2005) and in which the affected party does not suffer excessive damages (STC 1365/2009).[37]

Subscriber data

To the best of our knowledge there is no specific legal standard to access subscriber data besides the prior judicial authorization by virtue of Article 9 of the Criminal Procedure Code.[38]

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

The competent authorities to request access to communications data through interception measures in criminal investigations are public prosecutors[39] and the directors or heads of the bodies that form part of the State Intelligence System.[40]

The System is composed of the National Intelligence Agency, the Defense Intelligence Directorate of the National Defense Staff (*Dirección de Inteligencia de Defensa del Estado Mayor de la Defensa Nacional*), the Intelligence Directorates of the Armed Forces (*Direcciones de Inteligencia de las Fuerzas Armadas*), and the Intelligence Directorates or Headquarters of Police Forces and Public Security (*Direcciones o Jefaturas de Inteligencia de las Fuerzas de Orden y Seguridad Pública*).[41] On the latter, Article 22 of the Intelligence Law states that the function of police intelligence corresponds exclusively to Chile's Carabiniers and the country's Investigation Police, as previously defined.[42]The directors or heads of the State Intelligence System's bodies are also entitled to request access to communications data obtained through the other special procedures established in Article 24 of the Intelligence Law.[43]

Public prosecutors are regarded as competent authorities who can request access to retained IP addresses, subscribers' IP numbers, and connection logs;[44] data obtained

[37] Chile's Constitutional Court (*Tribunal Constitucional*), ruling n. 2153-11, https://www.tribunalconstitucional.cl/expedientes?rol=2153 (Spanish).

[38] Article 9, Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish).

[39] Art. 222 (1), Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish); Article 24, Law 20.000/2005, https://www.leychile.cl/Navegar?idNorma=235507 (Spanish); Article 33 (a), Law 19.913/2003, https://www.leychile.cl/Navegar?idNorma=219119 (Spanish); and Article 14, Law 18.314/1984, https://www.leychile.cl/Navegar?idNorma=29731 (Spanish).

[40] Article 25, Law 19.974/2004, https://www.leychile.cl/Navegar?idNorma=230999 (Spanish)

[41] Article 5, Law 19.974/2004

[42] This does not exclude what is provided in Article 20 (2) of the same law: "exceptionally, within the police functions that correspond to the maritime and aeronautics authorities, naval and air intelligences may carry out the processing of police information that they collect."

[43] These procedures are: a) the intervention of telephone, computer, radio and correspondence communications in any of its forms; b) the intervention of computer systems and networks; and c) the intervention of any other technological systems destined to the transmission, storage or processing of communications or information.

[44] Art. 222 (5), Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish) and Article 6, Decree 142/2005, https://www.leychile.cl/Navegar?idNorma=242261 (Spanish).

through the request to access the companies' copies; or versions of the transmitted or received communications.[45]

The National Economic Prosecutor (*Fiscal Nacional Económico*), responsible for conducting administrative investigations to ensure free competition, may also require the access to communications data to the Minister of the Court of Appeals of the city of Santiago, provided that the Chilean Competition Tribunal (*Tribunal de Defensa de la Libre Competencia*) has given its prior approval. The request may include the interception of all kinds of communications and access to stored communications content. As per Decree-Law 211/1973, this applies to investigations of serious and qualified cases of collusion among competitors.[46]

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

As previously mentioned, Article 9 of Chile's Criminal Procedure Code asserts that "all proceedings depriving the accused or a third party of exercising the rights guaranteed by the Constitution, or restricting or disturbing them, shall require a prior judicial authorization." The same provision indicates that in urgent cases the order can be requested and granted by any means suitable for the purpose, such as telephone, fax, email or other. According to the provision, urgent cases are the ones in which an immediate judicial order is indispensable for the success of the measure.[47]

9. Is there any data retention mandate?

Article 222 (5) of Chile's Criminal Procedure Code states that telecommunications providers must retain a list of authorized ranges of IP addresses, subscribers' IP numbers, and connection logs for at least one year and disclose it to the Public Prosecutor's Office. Providers who refuse to cooperate are punished. Regulation controlling the interception and recording of telephone calls requires the retained information to be available to public prosecutors and any other institution that is authorized by law to request it.[48] The minimum retention period for subscribers' IP numbers in the regulation is six months. None of the norms set out a maximum retention period or an explicit requirement of a court order for accessing this data.[49]

[45] Articles 218 and 219, Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish). *See* also Article 24, Law 20.000/2005, https://www.leychile.cl/Navegar?idNorma=235507 (Spanish); Article 33 (a), Law 19.913/2003, https://www.leychile.cl/Navegar?idNorma=219119 (Spanish); and Article 14, Law 18.314/1984, https://www.leychile.cl/Navegar?idNorma=29731 (Spanish)

[46] Article 39, n, Decree-Law 211/1973 (*Decreto Ley 211 - Fija normas para la defensa de la libre competencia)*, https://www.leychile.cl/Navegar?idNorma=236106&idParte=&idVersion= (Spanish)

[47] Article 9, Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish).

[48] Article 6, Decree 142/2005.

[49] Sebastián Becker, Juan C. Lara & María Paz Canales. Derechos Digitales. "La construcción de estándares legales para la vigilancia en América Latina". Parte I: algunos ejemplos de regulación actual en América Latina, 2018. Available at: https://www.derechosdigitales.org/wp-content/uploads/construccion-estandares-legales-vigilancia-II.pdf (Spanish).

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

Although not expressly stipulated, Article 24's broad definition of special procedures for obtaining information in Chile's Intelligence Law might serve to authorize remote access to a device through the use of malware. Such understanding, however, seems to run afoul of the country's Constitutional safeguards and proportionality requirements.[50] According to the law, the special procedures are: the intervention of telephone, computer, radio and correspondence communications in any form; the intervention of computer systems and networks; electronic wire and recording, including audiovisual; and the intervention of any other technological systems for the transmission, storage, or processing of communications or information.[51] The provision does not address or authorize the use of deceptive means, which should prevent, in any case, phishing techniques from being applied.[52] Finally, these procedures are limited to intelligence and counterintelligence activities that aim to safeguard national security and protect the country and its people from threats of terrorism, organized crime, and drug trafficking.[53]

In 2015, press leaks revealed that the Chilean Investigation Police purchased and used the "Phantom" system, highly intrusive malware that allows the user to track phones through a GPS tool; intercept and collect text messages, emails, and call log histories; and record phone calls, among other capabilities. Even though specific cases of the use of "Phantom" are unknown, government entities have acknowledged its use only for the purpose of pursuing drug trafficking and organized crimes.[54] New allegations of police's use of malware were raised by the institution in 2018 amidst controversies around the Huracán Operation (*Operación Huracán*). Convened to investigate supposed links between Mapuche groups and terror organizations, it led to the arrest of eight Mapuches in September 2017.

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.

---

[50] Pablo V. Bonvin, Valeria O. Romo, "Cuando el Estado hackea: El caso de Operación Huracán", December 2019, p. 100. Available at: https://rchdt.uchile.cl/index.php/RCHDT/article/view/54436/58886 (Spanish).

[51] Article 24, Law 19.974/2004, https://www.leychile.cl/Navegar?idNorma=230999 (Spanish).

[52] Pablo V. Bonvin, Valeria O. Romo, "Cuando el Estado hackea," supra note 48, p. 101-103. The authors stress that the use of deceptive means by law enforcement requires explicit legal authorization, pointing to Article 31 of the same Intelligence Law as an example. Such article refers to undercover agents' activities.

[53] Article 23 (2), Law 19.974/2004.

[54] Derechos Digitales, "State Communications Surveillance and the Protection of Fundamental Rights in Chile", July 2016, item 2.2.3, op.cit. *See* also Chile's Investigation Police, National Public Affairs Department, "Press Release." Santiago, July 6, 2015. https://pbs.twimg.com/media/CJQdW9KW8AEg9Rl.jpg (Spanish).

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

Prosecutors are entitled to demand information from any person or public official, who are obliged to provide it, except in cases expressly exempted by law.[55] Natural or legal persons must comply with the proper judicial order for the special procedures set in Article 24 of the Intelligence Law.[56] In drug-trafficking and money laundering investigations, ordinary imprisonment penalties are imposed to notaries, curators, and archivists who fail to comply with prosecutors' requests for data.[57] Communications and telephone companies have to take the necessary measures to respond to communications interception and recording requests; failing to do so is punished as contempt.[58] The same may be applied if companies do not comply with data retention obligations.[59] Also, under no circumstances may these companies maintain or incorporate in their networks technology or equipment that hinders or impedes, in any way, compliance with interception or recording orders.[60]

[55] Article 180, Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish).
[56] Article 30, Law 19.974/2004, https://www.leychile.cl/Navegar?idNorma=230999 (Spanish).
[57] Article 29 and 29, Law 20.000/2005, https://www.leychile.cl/Navegar?idNorma=235507 (Spanish). and Article 33, c, Law 19.913/2003, https://www.leychile.cl/Navegar?idNorma=219119 (Spanish).
[58] Article 222 (5), Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish).
[59] Article 222 (5), Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish) and Article 6, Decree 142/2005, https://www.leychile.cl/Navegar?idNorma=242261 (Spanish).
[60] Article 5, Decree 142/2005, https://www.leychile.cl/Navegar?idNorma=242261 (Spanish).

TRANSPARENCY & COMMUNICATIONS PRIVACY

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

The State does not regularly report on the number of requests to access communications data. Nonetheless, in 2018, the number of telephone interception requests were revealed by a news media outlet based on an access to information request under Law No. 20.285/2008.[61]

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

To the best of our knowledge, there is no legal prohibition regarding disclosing aggregated or statistical data about government data demands under the Criminal Procedure Code. The Intelligence Law, which applies to police intelligence activities,[62] established the secrecy and restricted circulation of all records held by the states' intelligence entities or its staffers.[63] The obligation to maintain secrecy also applies to those who, without being officials of the intelligence agencies, learn about the requests for communication surveillance (as specified in Article 24), their justification, and related judicial resolutions.[64] However, the obligation to maintain secrecy does not extend to statistical or aggregated data. This is why Chilean companies have been publishing transparency reports containing aggregated information about communications data requests. However, they do not distinguish between criminal and national security cases. Companies such as Telefónica-Movistar[65] and Entel[66] explicitly mention national security legislation within the legal framework considered in the requests.

---

[61] *See* https://www.emol.com/noticias/Nacional/2018/01/07/890183/Fiscalia-pidio-91-mil-escuchas-telefonicas-en-los-ultimos-cinco-anos-a-un-promedio-de-50-diarias.html (Spanish).

[62] According to Article, 20 (2) of the law, police intelligence services comprise the processing of information related to the activities of individuals, groups and organizations that in any way affect or may affect the conditions of public order and internal public security. Law 19.974/2004, https://www.leychile.cl/Navegar?idNorma=230999 (Spanish).

[63] Article 38, Law 19.974/2004.

[64] Article 40, Law 19.974/2004.

[65] Telefónica's Transparency Report 2018 https://www.telefonica.com/documents/153952/183394/Informe-Transparencia-Comunicaciones-2018.pdf/5a54f445-e95f-4b71-e549-e9f6d1eb5b7d (Spanish).

[66] Entel's Transparency Report 2019 http://www.entel.cl/legales/pdf/Requerimientos-de-Datos-Personales-2019.pdf (Spanish).

15. Do telecommunication companies publish transparency reports?

- Telefónica-Movistar provides annual transparency reports.
- VTR published its first transparency report in 2019.
- Claro publishes transparency reports.
- Entel publishes transparency reports.
- GTD Manquehue does not publish transparency reports.
- WOM published its second annual report in 2019.

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

A judge may authorize an intrusive investigative measure to be carried out before the investigation is formalized[67] and without prior notification of the person affected. The request can be made by the prosecutor, when it is indispensable for the investigation.[68] After the investigation is formalized, a prosecutor's request for not notifying the person affected will only be granted by a judge if the secrecy is strictly necessary for the measure to be effective.[69] In the latter case, the prosecutor must set a term of no more than 40 days, which may be extended only for the intervening parties (not the defendant), for the same period and only once, with well-founded reasons.[70]

For interception measures, those responsible for carrying them out as well as the companies' employees have a duty to keep them secret.[71] However, Article 224 of the Criminal Procedure Code requires the person affected to be notified after the interception is completed if the aim of the investigation allows it, and if it does not jeopardize the life or physical safety of a third party.

The investigation of crimes under Chile's "Drugs Law" can be secret to the defendant and intervening parties when stipulated by the public prosecutor, for a maximum term of 120 days, successively renewable with judicial authorization for maximum periods of

[67] According to Article 229 of the Criminal Procedure Code, the investigation is formalized by the prosecutor's' communication to the accused, in the presence of the judge (*juez de garantía*), that he's under investigation for one or more specific crimes.
[68] Article 236 (2), Law 19.696/2000, https://www.leychile.cl/Navegar?idNorma=176595 (Spanish).
[69] Article 236 (3), Law 19.696/2000. See also Article 14 (3) of the Terrorism Law, Law 18.314/1984 https://www.leychile.cl/Navegar?idNorma=29731 (Spanish).
[70] Article 182, Law 19.696/2000.
[71] Article 222 (5), Law 19.696/2000.

60 days.[72] With regard to the special procedures for obtaining information set in Article 24 of the Intelligence Law, the judicial order authorizing or denying them must be issued without hearing or intervention of the affected party or third parties.[73] The law does not mention the possibility of subsequent notification. In turn, it sets forth a secrecy obligation that affects all documents, information and records kept by the agencies of the Intelligence System or that their staff become aware when performing their functions.[74] The same obligation applies to any person who has information about requests for special procedures, including the background that justifies them and judicial resolutions issued for that purpose.

[72] Article 38, Law 20.000/2005 https://www.leychile.cl/Navegar?idNorma=235507 (Spanish). For search and seizure of documents that may prove or unveil important facts to the investigation, see Article 27, b (2) of the same Law.

[73] Article 28, Law 19.974/2004, https://www.leychile.cl/Navegar?idNorma=230999 (Spanish).

[74] Art. 38, Law 19.974/2004.