State Communications Surveillance and the Protection of Fundamental Rights in Chile

By Valentina Hernández and Juan Carlos Lara
in collaboration with Katitza Rodríguez, EFF

December 2015

ELECTRONIC FRONTIER FOUNDATION

DERECHOS DIGITALES
América Latina

Valentina Hernández is a researcher at Derechos Digitales, a Latin American non-profit organization whose purpose is to develop, defend, and promote human rights in the digital world. She also has law degree from the University of Chile. Juan Carlos Lara is the director of research and public policies at Derechos Digitales, and is a lawyer with a law degree from the University of Chile.

This report was written in alliance with the Electronic Frontier Foundation (EFF). We would like to thank Katitza Rodríguez, International Rights Director at EFF, for her contribution to the substantial revision of this report; and to Kim Carlson and David Bogado of EFF for their copy-editing and formatting contributions.

This report is part of a larger regional project conducted in eight Latin American countries by the Electronic Frontier Foundation, an international non-profit organization that has been defending freedom of expression and privacy in the digital world since 1990.

Table of Contents

Introduction

Communications technologies play a fundamental role in society and provide individuals the ability to carry out tasks and communicate with ease. However, the benefits of these evolving communications technologies are often accompanied by new threats from States that have an increased technological capacity to conduct surveillance on all communications. As pointed out by the UN High Commissioner for Human Rights in 2014, although these technologies make life easier and are available to everyone, they are equally available to governments that are capable of conducting surveillance in an unprecedented, easy, cheap, and efficient manner.[1]

Due to the ease and efficiency of conducting surveillance—which States usually justify[2] with national security claims—it is necessary to pay attention to the fundamental rights that are often violated when States carry out communications surveillance, and to learn about the necessary safeguards that are required in order to prevent abuses of power. To do this is extremely important, especially when it comes to rights that are guaranteed by and explicitly recognized in the Chilean Constitution, as well as international human rights treaties that have been ratified by Chile.

The right to privacy, due process, and freedom of expression are liberties that are particularly vulnerable among all the rights that are affected by communications surveillance. But these are not the only ones: Freedom of assembly and association may also be affected. This is why it is essential for States to establish well-founded and consistent legislation aimed at protecting individuals against violations of these rights and interferences into their private lives.

Chile has yet to achieve this. The biggest problems are stagnant laws, which fail to adapt to the current situation and rapid technological advances, as well as provisions that are too general. Moreover, current Chilean legislation that is aimed at protecting human rights is scattered and spread across theConstitution, laws, and administrative legislation that is difficult to follow and control. Thus, the protections of those affected by surveillance activities are also scattered and consequently less effective than if there were a consistent set of regulations authorizing surveillance to be carried out on the population.

Chile is not unfamiliar with cases of surveillance in the digital world. Over the past few years, there have been cases whose common thread involve online communications collection and surveillance carried out by public bodies. These collection and surveillance activities have been conducted in ways that clash with the right to due process. Like, for example, when the police, without a judicial order, requested that web site administrators

and international companies turn over information about the IP addresses of users who posted comments on certain websites[3]. Or when a student was accused of allegedly attacking a police officer during a protest in Santiago in May of 2014 after the police intelligence unit used a screenshot from a video recording of the incident where only part of the aggressor's face was visible, and searched Facebook profiles, with the help of face recognition tools, in order to find a picture of someone who looked like the aggressor. The judge rejected the evidence, and then asked the Public Prosecutor's Office to "be more serious when conducting investigations."[4]

This report first provides an analysis of the legislative framework on the protection of fundamental rights against State surveillance in Chile. The main Chilean laws that empower authorities to conduct surveillance online will be presented herein; specifically the ones belonging to the criminal procedure system and the National Intelligence Agency (*ANI, in Spanish*).

Following this analysis, we examine whether national legislation complies with standards set by the International Principles on the Application of Human Rights to Communications Surveillance.[5] It is not just a matter of academic or theoretical concern. The compliance with such standards is identified as the adherence to the respect for human rights, which is now found both in domestic constitutional regulations and in international documents on human rights subscribed and ratified by Chile. Therefore, compliance with these Principles amounts to the respect for the supralegal regulations in force. From the perspective of fundamental rights, their respect is fully enforceable to the State.

Finally, based on the facts and analysis presented, we provide the Chilean State with a list of recommendations to effectively protect fundamental rights against communications surveillance conducted by State agents or officials.

This report defines “communications surveillance” set forth by the aforementioned Principles as: "the monitoring, intercepting, collecting, obtaining, analyzing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person’s communications in the past, present, or future."[6]

1.
Constitutional Framework for the Protection of Rights Affected by State Communications Surveillance

State communications surveillance activities are capable of infringing on a plethora of fundamental rights, like the right to privacy, freedom of expression, and freedom of association, among others.

Below, we analyze how these rights are recognized in Chile's Constitution and analyze how they are acknowledged in instances of surveillance case law. Pursuant to Article 5 of the Constitution,[7] we defer to the American Convention on Human Rights, fully applicable to the Chilean national legislation at the supralegal level.[8]

1.1 Privacy

Article 19, Section 4 of the 1980 Chilean Constitution guarantees "the respect and protection of private life and the honor of the person and his or her family." Then, Article 19, Section 5 refers to "the inviolability of homes and all forms of private communication," presenting the notion of privacy with a special meaning. The guarantee given by Article 19, Section 4 uses the concept of "private life," and not "privacy." The notion of "private life," according to the members of the commission in charge of writing the Constitution, was significantly more developed in everyday language. The community recognized the concept of respecting the private life, but "privacy" was a lesser known term, and not yet colloquial in our language.[9] As such, while the Chilean Constitution does not regulate the right to "privacy," the interests linked to it are presented in the constitutional legislation.

From this perspective, Chile's privacy protection standards seem to be broken in different aspects of intimacy, each with different consequences. The protection of personal data has been outlined on the basis of the guarantee of protection of private life, as we will see below. However, before Law 19.628 was passed, the illegal handling of this data was only able to be challenged by a constitutional complaint (or "remedy") of protection. Although the Constitution considers the right to a "private life" a legal interest worth protecting, there is no definition of it—nor what it encompasses—in the Constitution nor in law, which leaves the task of defining it to case law.

The protection of personal data is not referenced directly as an independent right in the Constitution, nor is it outlined as one of the rights linked to private life,[10] absence which is

attributed, among other reasons, to the Chilean Constitution. Notwithstanding, the Constitutional Court case law elaborates on the protection of personal data based on this right, in specific cases and with non-binding characteristics. [11]

This does not take into account the attempts to reform the Constitution, which tend to provide safeguards for personal data.

In relation to other aspects, the Constitutional Court has yet to rule on how State communications surveillance violates this right. For the most part, the laws closely related to surveillance provide for oversight mechanisms to control such activities. Still, as we shall see in this report, it is questionable whether these standards and legal mechanisms meet the constitutional requirements.

Section 2, Article 11 of the American Convention on Human Rights—on the protection of honor and dignity—deals with the right to privacy. It states that "no one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor and reputation." Section 3 adds that "everyone has the right to the protection of the law against such interference or attacks."

In 2009, the Inter-American Court of Human Rights ruled on the case *Escher et al. vs Brasil,* in which telephone conversations between members of a rural union were intercepted. In paragraph 114, this international court referred to the application of the aforementioned Article 11 in relation to police surveillance activities, stating that:

> *"(...) Article 11 protects conversations using telephone lines installed in private homes or in offices, whether their content is related to the private affairs of the speaker, or to their business or professional activity. Hence, Article 11 applies to telephone conversations irrespective of their content and can even include both the technical operations designed to record this content by taping it and listening to it, or any other element of the communication process; for example, the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls, aspects that can be verified without the need to record the content of the call by taping the conversation. In brief, the protection of privacy is manifested in the right that the individuals other than those conversing may not illegally obtain information on the content of the telephone conversations or other aspects inherent in the communication process, such as those mentioned."*[12]

Then, in the following paragraph, the Court emphasizes the risks that the right to private life in relation to the flow of information is subjected to, especially given the technological

tools currently available and increasingly being used. It draws on the fact that the individuals affected by collection or recording of telephone communications are not to be left unprotected by the State or private entities. On the contrary, the State must adapt traditional rules to better protect their rights.[13]

From this, it can be inferred that the standard of the Inter-American system in relation to surveillance and privacy includes:

- Article 11.2 and 11.3 outlines, within the protection of the right to private life, protection against all interferences with this right, be that through telephone communications, correspondence or digital communication media.
- On this subject, it is necessary to adapt this right to the current technologies that may infringe upon it. In order to achieve this, the State is required to adapt its policies and forms of protection to this right, as mandated by Article 11.3 of the Convention.
- Surveillance activities violate the right to privacy not only in the cases in which the content of the communication is recorded, but also when any other element of the communication process is recorded.
- As displayed in the 2009 case of *Tristán Donoso vs. Panama*, this is not an absolute right, and thus, it may be interfered with by States as long as the interferences are not abusive or arbitrary. That is, they must be provided for by law, pursue a legitimate aim, and meet the requirements of adequacy, necessity and proportionality.[14]
- In 2013, the Special Rapporteur on Freedom of Expression of the OAS expressed the same views as the Court in the Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression.[15] Sections 9 and 10 refer to the need to limit such surveillance programs and emphasize the requirements, cited by the Inter-American Court, that States must comply with in order to limit the right to privacy. The declaration adds that any activity violating the right to privacy and freedom of expression must be monitored by an independent oversight mechanism and that must provide essential guarantees of due process and judicial oversight. The Declaration references the cases of police prosecution against journalists and independent media as an example of illegal interference of these rights.

Within this section, we see that what the Chilean Constitution defines separately as "private life" and "inviolability of private communications" and home is recognized at a constitutional level.

1.2 Freedom of Expression, Freedom of Assembly, and Freedom of Association

Freedoms related to expression are included in the Chilean Constitution in Article 19, Section 12, Subsection 1, as the constitutional guarantee of "freedom to express opinion and to inform, without prior censorship, in any form and by any medium, without prejudice to responsibility for any crimes or abuses committed in the exercise of these freedoms, in conformity with the law (...)."

The national doctrine, Nogueira (2004), complements the constitutional definition by stating that this right encompasses "the individual's right to express in any way and through any means, with no previous censorship, their moral, cognitive and symbolic universe, which has its origin and elaboration in the psyche of the person and is expressed in free will (what the person believes, thinks, knows or feels), through ideas and value judgments (without them being vexations or insults, which are unnecessary to express ideas), which are subjective in nature and may be changed and disseminated. This also includes the right to remain silent and abstain from delivering an opinion."[16]

It follows from this that the right to freedom of expression encompasses, according to Chilean law, the following elements:

- Freedom to express opinions, with no prior censorship
- Freedom to be informed
- Freedom to receive information (including public information)
- Freedom to have limit to this right (in the cases of, for example, hate speech).[17]

The Constitutional Court has linked the historical evolution[18]of this right to the rejection of prior censorship, and to the characteristic pluralism of a healthy democracy. In the first constitutional texts, the right to freedom of expression presented a series of prior limitations usually related to the respect for honor, moral, and faith. Consequently, the version originally in force in the 1980 Constitution vetoed a series of political groups, establishing the so-called regime of "protected democracy."

The current provision of this right eliminates those heavy restrictions, and lays the foundation for freedom of expression in a political sphere, which includes the freedom to develop ideas, the right to disseminate them, and the freedom to gather and implement them—as well as the right to association, for the building blocks of a democratic society.[19]

In fact, to use the words of the Constitutional Court, freedom of expression and the right to freedom of association are related as follows: "The right to association protects the individuals' power to gather with the purpose of promoting certain shared ideals. If there

wasn't freedom to elaborate, adhere to or express such ideals, the right to association would lose its reason for being."

Thus, freedom of expression plays a fundamental role in a democratic society, because it allows for the discussion of ideas, the exchange of viewpoints and messages, the freedom to criticize, the freedom to conduct scientific investigation and debate, artistic creation, unrestricted dialogue, no censorship or fear, and an informed public opinion."[20]

Regarding the constitutional guarantee on the freedom of assembly, including those with the purpose of expressing oneself, Article 19, Section 13 of the Political Constitution guarantees "the right to assemble peacefully without prior permission and without weapons. Meetings at squares, streets and other places of public use are ruled by the general provisions [concerning] the police."

Consequently, the doctrine establishes that this right consists in the "freedom that individuals have to gather unintentionally or temporarily with the purpose of communicating an event, discussing any matter or expressing a feeling or opinion."[21] Hence, public gatherings are recognized in both aspects: the characteristic of a meeting and the contents expressed in the speeches given in that meeting.

To this, we can add the right to association, provided for in Article 19, Section 15 of the Chilean Constitution, as a guarantee on "the right to associate without prior permission." The national doctrine has interpreted this right as one that allows an individual to meet with others voluntarily and consistently to achieve certain aims—that is, to gather or attend an already-existing one without prior permission—(individual dimension of freedom of association) and the association's right to self-government (collective dimension.)[22]

It is precisely this duty of non-interference that affects freedom of expression as well as freedom of assembly and association. The first freedom has no prior censorship. Civil or criminal liability are attributed subsequently. There is no prior filtering of content. In the other two cases (freedom of assembly and association), it is important to mention that as long as the legal requisites are met and the group (gathered or associated) does not threaten morals, public order or state security, the latter can't prohibit the creation of a new organization. These rights are relevant because they are the channels for which individuals express ideas and are necessary for a democracy.

Disproportionate surveillance programs are capable of affecting all of these rights. Even though the Constitutional Court of Chile has not made any specific declarations on surveillance programs such activities that do not comply with the requirements of legality, necessity, and proportionality which directly conflict with them.

For example, those subject to unwarranted surveillance may fear persecution and are often silenced when freely expressing themselves. Moreover, such disproportionate surveillance have a similar effect upon the rights to assembly and association, creating an indirect interference with the individual aspect of the rights: The fact that the State may be able to identify who the participants of a public gathering are, who the members of a particular association are, is sufficient reason for those individuals not to exercise these rights, which undermines the speech value of a democracy.

Specific cases have been verified over the past few years. In 2011, the Chilean Ministry of Internal Affairs submitted a draft bill aimed at combatting the negative effects caused by student social protests. The bill intended to sanction both participation in and convocation to any public demonstration that ended in disturbance or damage.[23] At the same time, the public authority allowed for the revision of the activity and online comments made by Chilean social networks users, regarding their opinion about the government performance.[24] There was also a public tender where the State sought a service that allowed for the monitoring of geolocation information, and an analysis of social media discussions.[25]

In mid-2015, a leak disclosed that the Investigations Police of Chile (*PDI, in Spanish*) was linked to the purchase of malware from the Italian company, Hacking Team. Called Galileo, the software enables access to computers in a remote, fast and simple way.[26] In the beginning, the PDI denied such a link, emphasizing the illicit nature of said surveillance practice and the need for prior judicial authorization to conduct such purported activities. Later the PDI confirmed the purchase of this system.[27] The leak included a series of e-mails in which the chief of the Department of Telephone Monitoring indicated that deploying Galileo helps collect IP addresses of customers and at obtaining data that cannot be accessed without a prior judicial authorization.[28]

2.
State Communications Surveillance Legal Framework

2.1 Telecommunications General Law

In Chile, the Telecommunications General Law Nº 18.168 regulates all transmissions, emissions or receptions of signs, signals, documents, images, sounds and information of any nature, through a physical line, radio-electricity, optical technologies or other electromagnetic systems, providing for rules on interception, dissemination and user protection. Its goal is to regulate telecommunications as a service and the relation between the different operators of this system.[29]

Article 24 of the Telecommunications Law lists obligations that public service concessionaires have to provide as a service to Internet service providers, and to any other natural or legal persons providing commercial services of connection among users or their Internet networks. The preservation of Internet users' privacy is listed among these obligations.

Apart from this general reference, the Telecommunications Law does not provide for hypotheses allowing to conduct telecommunications surveillance activities. However, it is necessary to review two supplementary regulations of this law: The Regulations on the Telecommunications Law (2014) and the Regulations on the Interception and Recording of Telephone Communications and other Telecommunications (2005).

The Regulations on Telecommunications Services, Decree Nº 18, of January 2014, specified the application of the provisions established in the Telecommunications General Law. With respect to privacy, and together with the constitutional safeguard for the inviolability of private communications, the law lays down that the telecommunications service concessionaires' main obligation is to preserve user privacy. Hence, it prohibits interceptions or malicious collections, without due authorization, of any type of signal emitted through a public service, with penalties of incarceration or fine.

Complementing surveillance and privacy law, the Regulations contain two articles of special importance. The first, Article 24, refers to the personal data of users of telecommunications services in Chile. This regulation indicates that such data may only be used with specific purposes related to the provision of the service. Furthermore, they must be subject to the provisions in the Law on the Protection of Private Life (Law Nº 19.628, which only

regulates personal data).

One of the key points of the supplemented law is Internet service providers' (ISPs) obligation to protect the privacy of their users. This obligation is not only fulfilled by prohibiting unlawful interception, but also by preventing data that may affect individuals' privacy from being leaked by the ISPs.

These regulations go back to the topic of user privacy in Article 50[30] by stating that ISPs shall preserve the privacy and safety of their users when making use of Internet access services. Unlike the previous regulation, these regulations reference privacy in relation to Internet use. Besides, this is not a general obligation for all types of telecommunications,[31] but only for the Internet, though it follows the same basic idea.

The second set of regulations, which is more relevant in this report, is the September 2005 Decree Nº 142 of the Ministry of Transport and Telecommunications, also called "Regulations on the Interception and Recording of Telephone Communications and other forms of Communications." Its purpose is to regulate the proceedings that must be followed by telecommunications service providers in regards to the legal requirements for interception and recording communications held by telephone service users and all types of telecommunications in general.

The procedures for the interception of communications, which are authorized and rule-based specifically in this last set of regulations, are regulated in the following criminal prosecution rules. Decree Nº 142 is the legislation that completes the Telecommunications Law in relation to the legal modifications in the criminal field that began to include certain obligations in connection with logs. It also authorizes intrusive proceedings that the law does not provide for, given its age.

2.2 Special Rules in the Criminal Procedure System

The Chilean procedure system for regulating intrusive measures of information collection, is divided between a general system applicable to offenses and common crimes, and special exceptions and rules for sensitive issues.[32] The latter shall be analyzed separately in two laws of interest: Law Nº 18.314, which identifies terrorist acts and imposes punishments (more commonly known as the "Anti-terrorism Law") and Law Nº 20.000, which sanctions the illegal trafficking of narcotic drugs psychotropic substances (commonly known as the "Drugs Law").

In general, the regulation of the investigation and prosecution of crimes, contained in the 2000 Criminal Procedure Code, aims at balancing the interests between criminal prosecution and the rights of those involved in it. In the specific regulation of the

investigation proceedings that may be mandated by the Public Ministry (the body in charge of criminal investigations also known as the Public Prosecutor's Office), the Code provides for a series of intrusive measures regulated and aligned with the Principles of Legality, Necessity, and Proportionality as foundations for the appropriateness of the proceedings. These regulated proceedings include body and medical examinations, entry and check-in in closed places, data retention and seizure of correspondence, telecommunications interception, and the seizure of objects and documents.

Although a series of intrusive measures in particular are taken into account, as are the ones already mentioned, the general principle on evidentiary and prior judicial intervention may be found within the basic informative principles of the Chilean criminal procedure system. Thus, Article 9 of the Criminal Procedure Code, titled "Prior Judicial Authorization," indicates 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."

To do so, any kind of evidentiary proceeding conducted by the Public Prosecutor's Office or the police that affects the aforementioned fundamental rights and concern surveillance activities, whether provided for and regulated in a special manner in the Code or not, requires authorization by a competent supervising judge. The standard in Chile, to which the judge should adhere, is the *test of proportionality* which compares the potential infringement upon the fundamental rights of the accused versus the requested measure.

In accordance with this test, the judge shall strictly consider the adequacy, necessity and proportionality of the measure in relation to its purposes and the potential infringement upon rights. While Article 9 does not specifically provide for this proportionality test as the standard, it is possible to find elements of this test in other provisions. For instance, in order to be authorized, the measure of the interception of telephone communications or another type of telecommunications requires that the punishment of the crime in question must be, at least, five years and one day of imprisonment. Moreover, this proceeding requires that its the communications surveillance activities be imperative for the investigation.

Apart from this proportionality test applicable when considering the rights of those being investigated and the advantages such intrusion may bring for the criminal investigation, it is necessary to highlight that Chilean legislation on each of these intrusive proceedings changes according to the measure chosen. Thus, each of the measures has different requisites and standards, which makes their regulation unequal and mismatched.

Exceptionally, whenever judicial authorization is necessary for the success of a proceeding, and the success of the measure depends on the unawareness of those affected, the subject under investigation shall not be notified about it.

Given this general rule, even if the public bodies (Public Prosecutor's Office or the police) participating in the criminal process want to conduct some type of evidentiary activity that is not explicitly provided for or regulated in the Criminal Procedure Code, they could, in theory, carry it out, provided it does not affect the investigation, with a prior authorization from a supervising judge. The natural limit, as explained, is the possibility of violating the fundamental rights of those under investigation.

The Code also establishes regulations on how the criminal procedure must unfold. Regarding the requirements for confidential information that the Public Ministry and the courts competent in criminal matters request from other State bodies, the Code stipulates that "this shall be provided abiding by the provisions laid down in the pertaining law, if there are any, or alternatively, by adopting the necessary precautions to guarantee that the information shall not be disseminated" (Article 19, Section 2); then, it grants the Supreme Court the power to decide whether its publicity will affect national security (section 4).

With regard to the secrecy of investigation proceedings, where information obtained through State surveillance activities may be found, Article 182 stipulates that, during investigations, these proceedings shall be secret in relation to third parties that are outside of the procedure. Only the accused and others involved in the process have the power to examine and obtain copies of the investigation records and documents. Exceptionally, some parts of the investigation or some of its proceedings pointed out by the prosecutor can be kept in secret from the accused and those involved whenever it is required for the effectiveness of the investigation. This period of secrecy may not be longer than 40 days.

In this regard, it is not possible to keep the proceedings secret when the accused has intervened in the process or when he or she has had the right to do so. Neither is it possible to classify the proceedings as secret in cases where the court has participated nor can the reports written by the expert witness about the accused or his or her defense counsel be secret. The officials who participate in investigations or who have knowledge about the proceedings are obligated to secrecy; failure to comply is a violation of secrets according to the Criminal Code.

Articles 218, 219, and 220 of the Criminal Procedure Code refer to the retention and seizure of correspondence. Even though they do not refer to electronic correspondence explicitly in the original list of types of communications, there is the item "others" at the end of it, which makes this enumeration significantly exemplary. Hence, after a reasoned decision has been made —in accordance with the system, pursuant to generic Article 9—the supervising judge may authorize the retention and seizure of this correspondence, and even authorize its copy if the prosecutor demands so, besides correspondingly applying these procedural provisions.

Apart from a prior judicial authorization, the other requirement established by law is that, under special circumstances, the communications are considered to be emitted or received by the person under investigation. Retaining and seizing correspondence must be useful for the investigation in order for it to be justified and feasible.

Nonetheless, there are specific references to electronic correspondence further on in the Code, especially in connection with copying correspondence, in both Articles 218 and 219. The first of these provisions establishes that it shall be possible to require copies or back-ups of electronic correspondence sent to or by the accused. The prosecutor shall examine the correspondence and shall keep whatever information related to the object of investigation. Secondly, the special regulation on the copies of the correspondence indicates that the supervising judge shall be able to authorize, upon the prosecutor's request, from any communications companies copies of the communications transmitted or received by them.

2.2.1 Telecommunications Interception

In simple terms, a communication is considered intercepted when, if during its transmission, as the result of the interference with the system of its transmission or of a process of monitoring of communications, the partial or total content of it becomes available to a third party, different from its issuer and its recipient.[33]

Telephone and other telecommunications interception is regulated in Article 222 of the Criminal Procedure Code. The provision stipulates that, in case there are reasoned suspicions, based on particular facts, that suggest that a person has committed or participated in a crime or its organization, or that the person is currently organizing the commission or participation in a punishable act sanctioned as a crime —that would be punishable by at least five years and one day of imprisonment—, and if the investigation so requires, the supervising judge, upon the Public Ministry's request, shall be able to order the interception and recording of this type of communications.

The requirement of having "reasoned suspicion" refers to the fact that, considering the specific circumstances of the case and concrete punishable crimes, there should be a justified belief that the person being investigated has participated in the organization or commission of a crime, or that he or she will do so in the future. Moreover, a requisite of necessity is established in order to proceed with the interception: It must be crucial to the process of the investigation.

This way, in order for this type of telecommunications interception to be legally authorized, in must comply with a 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: that is, at least five years and one day of imprisonment).

The Public Ministry has delineated the implementation of this measure in the Official Letter on page 060/2014, of January, 2014. This document notes that the Public Prosecutor's Office provides for the use of this measure in investigations in which the cases are complex: abduction, homicide, drug trafficking, money laundering, certain economic crimes, political corruption, sex crimes, and, in general, the investigations relative to particular groupings or simply to cases of organized crime.[34]

The following is a list of general procedural criteria that the Public Ministry must comply with before submitting a request to the supervising judge in these cases. In short, it requires:[35]

- First, that the prosecutor(s) in charge of the investigation in which this intrusive measure is to be conducted demand that the pertaining police force draft a written report justifying the deployment of the interception measure.
- Second, that the prosecutors assess both the appropriateness and the scope of the communications interception. To do this, they shall take into account the records submitted by the police and the circumstances of the case contained in the investigation file.
- Third, that the prosecutors, in their request submitted to the supervising judge, indicate the scope of the interception request submitted. This is extremely important, since, in accordance with the document: "(...) in which they shall explicitly indicate whether the interception request is related to voice interception or if they need the court to authorize them to obtain the call traffic, the information springing from message systems or other types of telecommunications that are possible to intercept, in accordance with the technical capabilities of the operators." As can be seen, the prosecutors may request not only the contents of the communication, but also the communication data (metadata) related to it.
- That once the request is granted, the prosecutors check that the judicial decision explicitly authorizes all the contents therein.
- Finally, that the regional prosecutors shall assess and request the use of the Backup Telecommunications Service from the Director of this specialized unit.

The Regulations on the Interception and Recording of Telephone Communications and Other Forms of Telecommunications by the Ministry of Transport and Telecommunications of 2005 are complementary to this rule. These establish general guidelines on the interception of telecommunications, aimed at protecting privacy and, at the same time, facilitating the police's job in relation to the criminal investigation.

Such interceptions must meet certain requirements:

- The communications between the accused and his or her lawyer cannot be intercepted, except for cases in which the supervising judge requests so, due to a well-founded belief that the lawyer may be criminally responsible for the events under investigation based on the background information that shall be placed on record in the corresponding decision.
- The authorization allowing interception and recording shall indicate in each circumstance the name and address of those affected by the measure, and identify the form of interception and its duration, which shall not be longer than sixty days.
- Telephone and communications companies must comply with this. Companies must provide the officials in charge of the proceedings with the necessary and timely help required.

Article 223 of the Criminal Procedure Code refers to recording. This provision stipulates that:

- The interception shall be registered through audio recording or other similar technical means guaranteeing the accuracy of the recording.
- This recording shall be directly given to the Public Ministry, which shall keep it secure and make sure that it is not disclosed to third parties. When appropriate, the public ministry shall be able to require a written transcript. This task shall be conducted by an official, who will work, in this case, as a public officer in relation to the accuracy of this transcript. Notwithstanding, the Public Ministry must keep the original recordings.
- All communications that are irrelevant to the proceedings shall be given, when appropriate, to the affected individuals, and all of their transcripts or copies shall be destroyed by the Public Ministry.
- This shall not be so in the case of the recordings that do contain information relevant to other proceedings in connection with acts that could result in punishable criminal offenses. In such a case, the intercepted information may be used in accordance with the preceding regulations.

As we have already covered the general framework on the interception and recording of content obtained from such measure provided for in the Criminal Procedure Code, it is necessary to draw the reader's attention to Decree 142 of the Ministry of Transport and Telecommunications; Under-secretariat for Telecommunications of September 2005, also known as the "Regulations on the Interception and Recording of Telephone Communications and other types of Communications."

The regulations indicate, in the first article, that their aim is to regulate the proceedings that telecommunications service providers must follow to comply with the legal requirements to intercept and record their users' communications.

A specific case exemplifies the use of these powers, apart from their use in legal proceedings. In April 2012, the former chief of the Directorate of the Intelligence Police (Dipolcar, in Spanish), Major Gonzalo Alveal Antonucci, was investigated due to alleged illegal interception of an officer's cellphone and the use of wiretappings to force this officer to quit his job.[36]

According to the investigation, between May and July of 2010, the then-chief of internal affairs of Dipolcar required, without judicial authorization and in the context of a police investigation, the telephone interception of the cellphone lines of two officers from the same institution. In accordance with the Public Ministry, this information was used with a purpose different from the ongoing investigation. This is why Major Alveal Antonucci was sued for obstructing an investigation and recording private communications without judicial authorization. The investigation came to an end without a sentence.

2.2.2 Mass Surveillance: Mandatory Metadata Retention

Article 222 of the Chilean Criminal Procedure Code, which refers to the mandatory collaboration between telecommunications companies and criminal investigations bodies, stipulates that the "providers of such services must keep, confidentially, and at the disposal of the Public Ministry, an updated list of their authorized ranges of IP addresses and a record of the IP numbers of their users' connections for at least a year. Denial or obstruction of this measure of interception and recording shall be considered an offense of contempt. Those in charge of carrying out the proceedings and the employees of the aforementioned companies shall be bound to secrecy, unless they are summoned as witnesses in the proceedings."

These "Regulations on the Interception and Recording of Telephone Communications and other types of Communications" establish in Article 6 that Internet service providers are compelled to keep information about their users' communications. Consequently, Internet service providers must keep: an updated list of their authorized ranges of IP addresses, and a record of the IP numbers of their subscribers' connections, for at least one year.

The obligation to keep a record requires having a computer system that automatically logs certain operations conducted by an Internet user that is then stored on the ISP servers; usually, the record contains the users' IP address—which is assigned by the ISP—and also the time of network connection and disconnection. This way, its subsequent processing allows to locate or identify the computer from which a certain operation was conducted using the Internet. This system is similar to the system that telephone companies use to control the calls made by their users, for billing purposes. [37]

The Regulations establish the obligation to keep that information secret, but "at the disposal of the Public Ministry and any other institution empowered to request it," without requesting judicial authorization. Conversely, they do not provide a rule for disposing of such data. If we take the IP address number as a series of numbers identifying a device connected to the Internet, which has been recognized as personal data by foreign legal systems, such as the Spanish system,[38] the general regulations on data protection, established by Law 19.628, must be applicable to it, including the possibility to eliminate it.

The Inter-American Court of Human Rights' judgement in the case of *Escher et al. vs Brazil* extends the scope of the protection of private life in Article 11 of the Inter-American Convention on Human Rights. The Convention protects not only content of private communications, but also metadata. In other words, it also protects the data related to the processes of communications.[39]

Regarding the interceptions and recording of communications, telecommunications service providers must comply with the time limit and the form defined by the court in charge of the case. There is no reference to the rules that the police should follow either the Investigations Police (*Policía de Investigaciones, in Spanish*)[40] nor the Policemen of Chile (C*arabineros de Chile, in Spanish*.)[41]

2.2.3 Targeted Surveillance: Malware

Recently, press leaks revealed that the Chilean Investigations Police purchased and used the system "Phantom." According to some reports, the system "Phantom" is highly intrusive. Whoever uses it can track phones using a GPS tool, and intercept and collect text messages, e-mails and call log histories, and record phone calls, among others.[42] Even though specific cases in which this software was used are unknown, this auxiliary tool is employed in investigations of crimes related to terrorism and drug trafficking.

In fact, the PDI[43] stated that the purpose of "Phantom" was to collaborate with the investigations of organized crimes and international networks, taking into account that these groups possess vast resources, both financial and technical.

However dangerous those crimes might be, and even though there are concessions allowing these special punitive laws, the requirement to have a judicial authorization in order to conduct investigative activities infringing upon fundamental rights and freedoms is still applicable. According to the PDI, all the provisions typical of a public purchase were met. However, the PDI refrained from giving more details about this, claiming that doing so would compromise national security.

The PDI could have used this system to access data, including data that does not generally require judicial authorization, such as the information about the use of communication

equipment separate from the communication itself. This is extremely serious; judicial authorization is a crucial element because it's at this stage where in which the judge should apply the proportionality test, and where he or she evaluates the proportionality between the evidentiary purpose and the violation of rights of those investigated.

A system like this does not comply with the legality requirement, because it does not comply with Article 9 of the Criminal Procedure Code. In other words, prior judicial authorization is circumvented, as are the rules related to the interception and retention of correspondence and telephone communications, as well as their procedural protections.

When analyzing surveillance that's carried out on an individual using "Phantom,"it is difficult to assure the proportionately given the wide range of capabilities the system provides: monitoring, tracking, interception, and recording of communications. The Criminal Procedure Code is clear when establishing that these measures must be extremely limited and must allow access to only exceptionally necessary data. Moreover, they must be used solely when no other measures that are less intrusive and detrimental to the right to privacy are available.

From merely monitoring publicly-available information on social networks to using highly invasive tools, the State has an extraordinary power to collect information and carry communications surveillance. State agents are able to carry out the simplest tasks—like identify organizers of a protest or demonstration; or they can conduct surveillance activities that are a bit more difficult, like request jurisdictional authorizations to obtain personal information and identify certain online users. State agents can also carry out complex surveillance activities; they can use invasive surveillance technology to track and identify and prosecute suspects, and can consider the obtained evidence as the only proof of the suspects' criminal involvement.[44] All these scenarios are in conflict with the right to due process, according to the Inter-American System of Human Rights.[45]

2.3 Investigation of Terrorist Acts

Law Nº 18.314, and Chile's general criminal legislation, apply to cases in which the crime in question is considered an act of terrorism, pursuant to the guidelines set in Article 1 of this law.

Given that Law Nº 18.314 specifically allows communications interception and recording, together with the aforementioned general evidentiary mechanisms of the criminal procedure system, this law facilitates State surveillance practices greatly. It facilitates its powers of intrusion and makes the whole process secretive.

One common critique of the law is that it defines "terrorist acts" in a vague and unclear manner;[46] so much so that the Inter-American Commission on Human Rights indicated that differentiating and classifying a common offense versus a terrorist one will have to be left to the judge's discretion.[47]

In fact, in 2013, the UN Office of the High Commissioner for Human Rights shared this opinion, highlighting the lack of a clear, consistent criterion when classifying a crime as a terrorist act:

> *"The various justifications put forward have been subjective and lacking in legal rigor. A comparison of the cases which have been charged as terrorism with those which have not bears this out. It is impossible to distinguish any clear and consistent dividing line between cases which have been charged as common criminal offenses (such as arson, frustrated murder and firearms offenses) from those in which the counter-terrorism legislation has been invoked, in order to aggravate the sentence and provide additional procedural advantages to the prosecutor. The Special Rapporteur reluctantly concludes that subjective, arbitrary and/or political considerations have played a role in the selection of those cases in which the anti-terrorism legislation is invoked."*[48]

When an act is classified as a "terrorist" act, it brings about a series of additional safeguards for those who participate as witnesses in a trial, like: compensated denouncement mechanisms, extended timelines throughout the criminal process (like an extension for the period of detention or pre-trial detention), greater secrecy of the investigation process and the evidence obtained, and greater restrictions to exercise some constitutional rights by those accused in these cases.

In relation to the evidentiary activity and its connection to State surveillance, Article 14 of the law allows the interception, tapping or recording of telephone and computer communications and their epistolary and telegraphic correspondence. This permission is given whenever the law classifies that offense as a terrorist one, or when the purpose of an offense was to instill terror. This measure can be granted upon the request of the Public Ministry to the Supervising Judge.

Moreover, since acts classified as "terrorist acts" are especially dangerous, the law is lax when it comes to setting standards for telephone communications and other types of communications interception. It removes the several requirements established in the Criminal Procedure Code, and only forbids the interception of the communications between the accused and their lawyer.

2.4 Investigation on Illegal Drug Trafficking

Law Nº 20.000, which sanctions the illicit trafficking of narcotics and psychotropic substances, establishes among many technical means for the investigation of the crime, the retention or seizure of correspondence, obtention of copies of communications and transmissions, and the interception of communications. To carry out these surveillance measure, it only needs to identify the circumstances that individualize or determine the person affected by the surveillance measure, without the need to identify the name and address as per Article 24 of this law.

Whenever the Public Ministry orders so, the investigation can be conducted in secret for a maximum period of 120 days, and is renewable for a maximum period of 60 days; there cannot be judicial control prior to the formalization of the investigation set forth by the Criminal Procedure Code, through which any person affected by the investigation, who had not been previously formalized by the judiciary, can request from the judge that the prosecutor report on the facts of the investigation or set a time limit for it. Furthermore, it sanctions whoever reveals, disseminates, or discloses information related to an ongoing investigation (of one that needs to be kept in secret) with a penalty that ranges from medium-term rigorous imprisonment to maximum-term rigorous imprisonment.

In line with Law Nº 18.314, it provides for compensated denouncement mechanisms and witnesses protection. Also, Article 38 establishes measures to increase time periods and circumstances of secrecy of the investigation.

Another shared similarity between the two is the vague language they both use to characterize what constitutes a crime. Like in the "anti-terrorism law," the qualification of what constitutes a crime according to the law is also ambiguous—similar to the surveillance measures authorized by Law Nº 18.314—and of what acts go unpunished. Hence, this is left to be determined by those interpreting the law and those using it to investigate and prosecute the offense.

Article 24 establishes that in the case of investigations of crimes typical of this law, retention, seizure, and interception of communications and telephone communications are exempt from the requirements established in Article 222 of the Criminal Procedure Code on the specification of the judicial authorization. Giving the name and address of the accused is enough.

Notwithstanding, this intrusive activity may be conducted in connection with the crimes listed in Law 20.000, as stated before, regardless of their corresponding punishments. In the case of communications interception, Article 222 of the Criminal Procedure Code, requires that the crime under investigation be associated with a penalty of a crime in order to conduct this measure.

2.5 Regulations on Surveillance Activities in the National Intelligence System

We define "intelligence activities" as measures taken to obtain information relevant to the security and defense of the State, its territory, or the nation. These intelligence activities are usually kept secret from the general public, in order to protect internal and external security issues while countering international terrorism and the national and international contingency.[49]

The Chilean intelligence system extends its reach to combat organized crime and drug trafficking. This means the Chilean intelligence system also needs to protect the State and its society against other complex domestic threats, even when they are usually protected by ordinary criminal investigation and persecution bodies.

According to the Constitution, all the State's acts, reasons, and proceedings are public. Nonetheless, a qualified quorum (*quórum calificado in Spanish*) reserves the right to determine when confidentiality is appropriate. In other words, the legal reserve requires a high parliamentary approval to authorize the State to conduct secret or confidential activities, apart from having specific aims.

Any reform of the intelligence activities requires that standard of authorization, including those activities covered by Law 19.974 on the State Intelligence System of 2004 which are subjected to this standard of approval.

2.5.1 Institutional Framework of the State Intelligence System

In 2004, Chile created the National Intelligence Agency (*ANI, in Spanish*), what operates today as the current State intelligence system. The ANI distinguishes between intelligence and counterintelligence, defined as “the section of intelligence activities whose aim is to detect, locate and neutralize the intelligence activities conducted by other States or individuals, foreign organizations or groups, or their local agents, directed against the security of the State and national defense.”

According to the ANI, intelligence is conceptualized as “useful knowledge, springing from information processing, to advise the higher levels of the State when making their decisions, with the purpose of preventing and informing about the risks to national interests and the achievements of the country, the security and defense.”

The ANI is at the forefront of Chilean intelligence services. The whole intelligence system is also made up of services belonging to the several branches of the Armed Forces and Security Forces, including the Department of Intelligence of the National Defense General Staff the Departments of Intelligence of each of the Armed Forces and the Departments or Agencies

of Intelligence of the Security Forces and Public Safety.

This National Intelligence Agency conducts collection and information processing activities at a national and international level; it prepares secret, periodical reports to submit to the President of the Republic; it suggests rules and proceedings for the protection of information systems; it requests information from the intelligence organisms of the Armed Forces and Security Forces, among others; it mandates the implementation of intelligence measures with the purpose of detecting, neutralizing, and counterbalancing transnational criminal and/or terrorist activities nationally or internationally; and it orders counterintelligence activities.

Strictly speaking, the ANI does not have the operational power to intercept communications for the purpose of intelligence gathering: Even though it can collect and process information, the means to obtain it are reserved for the aforementioned intelligence organisms. Thus, the ANI holds a power of strategy and politics.

2.5.2 Collection of Information and Intelligence Activities

The first collection procedure within the legal powers of Article 8 of the law, entails collecting and processing information, reports, and suggestions from other public agencies. In short, it is useful to collect and process both the information reported by the required agencies and the information reported by sources like the press.

Among the agencies that may be requested to submit information, we have the Armed Forces as well as the Security Forces (the police: the Chilean police force and the Investigations Police of Chile) and gendarmerie. Additionally, the information considered necessary may be requested from the several bodies belonging to the Administration of the State and from companies and institutions that have State support.

Alternatively, when it's impossible to obtain information through open sources, meaning publicly available information and information that requires a prior request for information made by a State body, a "special proceedings to obtain information" is authorized. This happens if the information is strictly indispensable for national security and the protection of Chile and its people against terrorism, organized crime and drug trafficking. These special proceedings grant access to relevant, classified background information, and provide necessary background information for the success of the investigation (Article 24).

These measures provide for proceedings of telephone, computer and radio interception; interception of computer systems and networks; electronic tapping and recording; interception of any other technological system destined to the transmission, storage or processing of electronic communications.

The law stipulates that the special proceedings shall only be used when they are strictly necessary to achieve the objectives of the System (Principle of Necessity). Also, the law limits their implementation to intelligence and counterintelligence activities with the objective to protect national security, Chile and its people against threats of terrorism, organized crime and drug trafficking (Principle of Proportionality), pursuant to Article 23 of this law. The Adequacy Principle, which is a pre-requisite for the Proportionality Test, can be justified when a less harmful public source (a less intrusive means) to obtain this data is unavailable.

In order for the special proceedings to be used, judicial authorization is mandatory, and must be requested by the directors or heads of the intelligence agencies, with and the sole purpose of protecting national security, Chile, and its people against threats of terrorism, organized crime and drug trafficking.

The authorization is issued directly by the Ministry of the Court of Appeal of the territory in which the measure is conducted or where it is initiated, or through the pertaining institutional judge. Hence, the authorization cannot be given by a supervising judge, but by a court minister or by a judge in the military justice system. Exceptionally, the law authorizes the use of secret agents undercover (Article 31) and whistleblowers (Article 32), without the need for a judicial authorization.

2.5.3 Possible Uses of the Information Obtained by the ANI and other State Organisms

Article 42 of the law establishes that the information collected, elaborated by or exchanged between the organisms belonging to the system shall be exclusively used to achieve their respective aims.

In this regard, the main objective of intelligence organisms is to advise the president who shall receive briefings from these agencies. These agencies shall also draw up reports, recommend rules and proceedings for protection, and determine the appropriateness of intelligence and counterintelligence measures, among other functions mentioned in Article 8.

As a general rule, State agencies don't have access to the information obtained by the ANI, for it is secret and has restricted circulation. Exceptionally, data can be submitted upon the request of the House of Representatives, the Senate, Courts of Justice, the Public Ministry, the Court of Auditors of the Republic via Ministers of Internal Affairs, National Defense and the Head of the Agency, regardless of the fact that the authorities and officials mentioned in the previous subsection shall be compelled to keep the confidentiality of its existence and its content, even after their corresponding duties are terminated.

2.5.4 Cases

There is no public information about the activities conducted by intelligence agencies, or about the intrusive measures adopted with the purpose of protecting national security and defense, and of achieving State aims. Their practices only become known in certain situations and conflicts.

An example is the investigation into the use of explosive devices known as “Bomb Case” (*caso Bombas, in Spanish*)[50] and the participation in a conflict in the South of Chile in relation to violent acts linked to protests by the Mapuche people. Many State bodies have classified these protests as terrorist acts. In this regard, the Defense Commission of the Senate organized a (secret) session and summoned the head of the ANI at the beginning of 2013, with no further information about the proceedings in the area. [51]

The Bombs Case was not classified as a "terrorist crime," despite the Public Ministry, the Investigations Police, and the ANI's efforts. However, the press accused these agencies of conducting a secret investigation that included telephone tapping and e-mail surveillance with no prior judicial authorization. and little regard for constitutional safeguards. The head of the ANI was summoned multiple times to the same commission of the House of Representatives to account for such a secretive and overreaching investigation.

Nonetheless, given that there is no public information about the activities of the ANI, the intelligence practices that came to be known for their infringement upon privacy have been mostly conducted by foreign governments, by means of information leaks or non-specific public information. Both the oversight activities by the Courts of Appeals and the political oversight by the National Congress are not subjected to public scrutiny.

3.
Analysis of Chilean Legislation vis-á-vis the International Principles on the Application of Human Rights to Communications Surveillance

This section deals with each of the Principles mentioned in the title of the section and assesses the extent to which national legislation adheres to these Principles when carrying out communications surveillance.[52]

Legality

> *Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.*

This principle establishes that all limitations to human rights must be prescribed by law: Otherwise, an activity infringing upon them that is not legally authorized is not legitimate.

As stated before, the whole criminal procedure system, from general (Criminal Procedure Code) to specific (laws on the persecution of particular crimes), is based on the general principle provided for in Article 9 of the Criminal Procedure Code: Any activity of the procedure affecting the fundamental rights of those under investigation or of third parties must have prior judicial authorization. Thus, each of the specific intrusive measures needs this authorization, apart from other legal requisites.

Chilean procedure legislation does comply with this principle, but we must pay attention to the indetermination mentioned above when discussing the classification of crimes related to laws Nº 20.000 and Nº 18.314. It is imperative to clarify the cases in which the proceedings carried out should firmly stick to these laws, as pointed out by international organizations on this matter. Notwithstanding, there are also still issues that need to be addressed, like when the investigatory agencies use "Phantom," which circumvents current legislation.

The Law on the Protection of Personal Data allows public agencies to deal with data without authorization from the data subject, as long as the activities are conducted within the framework of their duties. This, even though it is a legal exception to the legislation, creates an indeterminate space for secretive processing of personal data, which may be conducted on the basis of data obtained through State surveillance activities.

Legitimate Aim

> *Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.*

The general idea here is that in the Chilean legal system, State surveillance activities are directed to criminal persecution. As we see in both the Criminal Procedure Code and laws on specific crimes, in order to resort to these intrusive measures, basic requirements must be met—either when an act is classified as an especially dangerous crime (such as terrorist or drug crimes), or when a common offense is punishable as a felony (that is, five years and one day of imprisonment).

This means that the legal safeguards suggest that extremely harmful measures, like the interception of telecommunications, should aim at obtaining information from the persecution of particularly serious crimes, and the individuals involved in them.

Although this is true for the interception of telecommunications, it is not equally true in relation to other measures, such as the retention and seizure of communications, whose regulation is the one used in practice to request the physical seizure of devices that store copies of e-mails.

Pursuant to Article 218 of the Criminal Procedure Code, under the previous request of the Public Ministry, the judge may order the retention of any type of correspondence where the accused is the sender or the receiver, and when well-founded reasons justify their usefulness to the investigation. In these cases, it is this potential usefulness that shall make this measure appropriate, regardless of whether a less serious crime is under investigation.

Necessity, Adequacy, and Proportionality

> *Necessity: Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.*
>
> *Adequacy: Any instance of Communications Surveillance authorized by law must be appropriate to fulfill the specific Legitimate Aim identified.*
>
> *Proportionality: Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.*

These Principles are dealt as part of the proportionality test, recognized by the doctrine and case law. It must be carried out by a judge before he or she authorizes evidentiary activities that interfere with fundamental rights. This test should also be applied by a judge when these type of rights are in conflict.

The legislation does not specifically reference these principles, but they are underlying in the text. For instance, Article 222 of the Criminal Procedure Code outlines time limits for the intrusive measure, a scope that limits the intrusion to only the data strictly necessary to the investigation, a required certain level of probability ("well-founded suspicion"), and a required minimum sanction or special classification referable to the criminal act; all of these factors determine the appropriateness of such measures, delimiting what can be intercepted and recorded.

In addition to this, in the case of telecommunications interception, telecommunications companies are obligated to keep the confidentiality of said communications, and provide safeguards when conducting intrusive activities. Finally, the companies are compelled to eliminate the content that has been obtained when they exceed what is legally allowed, and, after a certain time period of time has elapsed.

The Principle of necessity is implicitly complied with, since the supervising judge shall only authorize these measures when they are essential to the investigation. Once again, it is possible to see these principles recognized and effectively applied in the legislation on the

interception of communications by the supervising judge.

Looking at the case of "Phantom" again, we take into account that this software allows the interception of communications in a remote and quiet way. It would be a clear violation of these three principles if this software were to be used to intercept communications, without complying with Article 222 and without explicit judicial authorization,

Moreover, the seizure of correspondence, whenever it applies to e-mails, does not pass the proportionality test, neither does it appear as adapted to a constitutional standard for the protection of fundamental rights.

Even when accepting the adequacy of the seizure of computer equipments that store e-mails, its appropriateness as a measure for a criminal investigation, according to the legal language, does not require to be necessary, but to merely be convenient for the investigation. Furthermore, it excessively affects the privacy of the person whose computer equipments are seized, which store all of his or her e-mails with the same level of accessibility, as opposed to what would be useful for an investigation.

Judicial Competent Authority

> *Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.*

Apart from the requirements mentioned in relation to each intrusive measure, including communications interception, we should mention once again Article 9 of the Criminal Procedure Code, which functions as the principle that shapes the entire criminal procedure legislation. This provision highlights the need for a prior judicial authorization in the cases in which criminal proceedings may affect or infringe upon the fundamental rights of those investigated or of third parties. That is the general rule.

However, the practice related to the delivery of communications data shows that, in some cases, the police request data without requesting judicial authorization.[53]

Due Process

> *Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public.*

> *Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law,10 except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorization must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorization.*

This principle is highly respected in Chilean legislation, both by the Constitution and by International Treaties on Human Rights that are applicable as part of the constitutional block, in criminal procedure legislation.

In fact, the constitutional regulation of this right, although it does not use exactly the same term—it calls it a right to a rational and fair process and investigation—its core concept is similar to the one in Article 8.1 of the American Convention on Human Rights.

Similarly, the first ten articles of the Criminal Procedure Code, under the first title of this regulation, called "Basic Principles," provide for a series of safeguards related to this human right, such as: single trial, exclusiveness and uniqueness of the criminal investigation, presumption of innocence, legality of the measures restricting and affecting freedoms, protection for the victim, scope of the defense, safeguards for the accused, the provision of a hearing to control safeguards, and the need for a prior judicial order authorizing investigative activities infringing upon fundamental rights.

More importantly, the rules of the Criminal Procedure Code that allow for the exclusion of illegal evidence; that is to say, of the evidence obtained by violating the legal requirements needed, including the general safeguard for the respect of fundamental rights and prior judicial authorization.

User Notification

> *Those whose communications are being surveilled should be notified of a decision authorizing communications surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorization. Delay in notification is only justified in the following circumstances:*
>
> *Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorized, or there is an imminent risk of danger to human life; authorization to delay notification is*

granted by a Competent Judicial Authority; and the User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.

The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.

Article 224 of the Criminal Procedure Code is clear when discussing communications interception: "The measure of interception shall be notified to the affected after it is conducted, whenever the object of investigation allows so, and as long as it does not jeopardize the life or physical integrity of third parties."

This provision then redirects the reader to Article 182 of this Code, which outlines that the activities of investigation carried out by the Public Prosecutor's Office are secret for those who are not involved in the process, but are not secret when it comes to those who are involved in it, except for certain instances in which secrecy is accepted, in which case, it shall have a limit of 40 days.

Transparency

States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each.

States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting Communications Surveillance.

States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance.

The annual report by the Public Ministry does not account for the number of times these measures are implemented. Similarly, there is no regulation allowing the affected individuals to know that they exist, or to receive notice that their data is being taken.

Any report on these measures may, in theory, be requested after their implementation and through passive transparency mechanisms. This characteristic differs from the Chilean criminal persecution system, in which the implementation of intrusive measures on communications becomes known the moment it is effectively applied as evidence in the criminal process.

Platforms such as Facebook and Twitter publish annual transparency reports,[54] where they outline the number of information requests submitted by different governments, including Chile's.

Public Oversight

> *States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance.*

Chile does not have an independent organism that oversees this type of practice. The closest thing is the High Courts of Justice through the remedies established in the Criminal Procedure Code and the Constitutional Court in the case of a constitutional file referred to cases of abuse of measures affecting fundamental rights.

Moreover, the supervising judges have monitoring capabilities at some instances, such as the precautionary principle for safeguards and the grounds for rejecting evidence, where the use of illegal evidence is forbidden. Apart from that, the criminal procedure system of Chile lacks an independent oversight mechanism to guarantee transparency and accountability of communications surveillance.

The case of surveillance activities, in which the measures undergo a judicial control, is slightly different, because there is a possibility of democratic control by Congress. Notwithstanding, the instances are only informative, they undergo a political control, and have no publicly verifiable results, for these are secret commissions.

Integrity of Communications and Systems

> *In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes.*

> *Data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users.*

Criminal legislation compels ISPs to keep a record of IP numbers and connections their users make for at least one year, with the purpose of facilitating the implementation of the intrusive measure of communications interception established in Article 222 of the Criminal Procedure Code.

As stated before, it is possible to find further information on how this is carried out in the corresponding regulations. Even though there are no obligations in relation to the setting up of surveillance mechanisms in the technical, physical, or logical characteristics of communication systems, this mandatory data retention is in clear contradiction with this principle.

Safeguards for International Cooperation

> *In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service providers and States. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to Communications Surveillance, the available standard with the higher level of protection for individuals is applied.*
>
> *Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for Protected Information to circumvent domestic legal restrictions on Communications Surveillance.*
>
> *Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.*

Article 2 of the Inter-American Convention on Mutual Assistance in Criminal Matters,[55] when referring to the application and scope of the Convention, indicates that it solely applies to the mutual assistance among the State Parties, thus, its provisions do not grant private parties the ability to obtain or reject evidence, or to impede the submission of any request for assistance.

This is the only provision in this treaty applicable to surveillance matters. This is so because whenever legislation provides for a protection minor to the privacy of its population, this international document may not be used to circumvent a greater guarantee scheme.

At the same time, it can work the other way around: a State Party that has a legislation with higher standards for the protection of fundamental rights could neither be rejected before a request submitted by another State in which the framework of protection is more permissive, irrespective of the provisions of the Inter-American Convention on Human Rights relative to the respect and adequacy of the internal legislation to such rights.

On the basis of this treaty, there was an information exchange in a case called "Los Luksic." The Luksics, in which a Chilean owner of a Twitter account used their account for parody and was prosecuted—accused of appropriation of another person's name. Following the diplomatic means of the treaty, the United States requested information from Twitter, who delivered the information under the assumption that "identity theft,"had occurred, which is a crime in that country.[56] However, both crimes are not comparable in the elements of criminal type. The cooperation in the delivery of data was, in this case, beyond any guarantee for the rights of the affected individual, including the necessity of the principle of dual criminality. At the end, the case was dismissed due to lack of proof of the commission of a crime. [57]

Apart from the regional MLAT, there also exists, since 2014, the Agreement for preventing and combating serious crimes between Chile and the United States.[58] This is a bilateral treaty that does not provide for a provision indicating the mandatory implementation of the legislation of the State party with a greater protection of privacy for those affected.

Despite this absence, it does consider a series of safeguards for the protection of fundamental rights, within which we find: data shall not be delivered until the recipient State has adopted all the appropriate measures for protection; the State sending the data cannot establish as a condition for the delivery that the recipient State change its legal criteria of personal data processing (this means that this treaty may not be used to circumvent domestic legislation); the principle of transparency is provided for in the delivery of information to the owners of the data and the document makes reference to mechanisms of correction, blocking and elimination of data.

Safeguards Against Illegitimate Access and Right to Effective Remedy

> *States should enact legislation criminalizing illegal Communications Surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is*

inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information.

States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.

Although the Chilean Law on Computer Crimes has been widely criticized for being short and out-of-date, it does provide for a crime type associated with the illegitimate access to computer systems in Article 2 of Law Nº 19.223, which classifies types of crimes related to computing, and states that "Those who, in the unlawful attempt to take possession of, use, or become aware of the information contained in an information processing system, intercept interfere with or access it, shall be punished with a penalty that ranges from minimum-term rigorous imprisonment to medium-term imprisonment."

As we can see, this provides for[59] crimes of cyber spying, but it has some flaws, for this law does not classify the crime of the non-authorized communications interception. It only outlines that the companies in charge of complying with this measure may not reveal the content of the intercepted communication, except when they are summoned to declare in the context of a criminal process. It is extremely serious that, in case of violation of the above, there is no specific sanction established.

Article 161-A of the Criminal Code provides for a generic type of crime related to those who seize, intercept or disseminate private conversations with no authorization. The penalty for this offense is imprisonment or a fine, whose sum is increased when the individual who disseminates the conversations is involved in them.

In relation to this, we can find regulations on evidence in the criminal procedure system, both as regards the prohibition of the evidence obtained through the violation of fundamental rights (illegal evidence) and in the prohibition of the implementation of the results obtained from a telephone interception or any other intrusive measure, as evidence in cases where they do not comply with the legal requirements.

Moreover, this legislation establishes that once the time limit to conduct interceptions has expired, interception must end and the data obtained from it must be eliminated. Similarly, all the background information that exceeds the content of the authorization given must be eliminated. These limits are set by judicial authorization.

4.
Recommendations

In accordance with the comparisons made in the previous section, we shall present a series of recommendations to the Chilean State in relation to the proper protection of human rights against communications surveillance conducted by public entities.

- Establish a classification of types of crimes so to clearly define when offenses are prosecutable by special criminal laws, since these regulations lower the standards when authorizing invasive activities for a criminal investigation.
- Expand the obligations that are required to proceed with intrusive communication surveillance measures, including telephone interception.
- Set minimum penalties for the investigated act in order to have access to greater intrusive surveillance measures. The danger posed by a crime should match the intrusive measures associated with its investigation.
- Establish specific and stronger penalties for telecommunications companies in charge of intercepting and recording communications in case they reveal, keep, or misuse the obtained data.
- At the same time, replace the outdated Law on Computer Crimes with one that classifies and sanctions illegitimate surveillance practices.
- Apply greater legal and police severity both when authorizing surveillance measures and when implementing them.
- Be stricter with regards to complying with the requirements to conduct surveillance measures, especially when it comes to judicial authorization.
- Be more actively transparent when the Public Ministry reports the numbers of requests sent to the court and the number of intrusive measures taken.
- Include provisions for the implementation of whatever legislation best guarantees the human rights of those affected, in subsequent agreements of mutual assistance in relation to the combat of crime.
- Reduce surveillance activities to a minimum. Their implementation should only depend on the commission of highly dangerous crimes. A conceptual and temporal framework previously delimited by a judge should be imposed; the measures should be listed in the law together with specific reasons that allow their implementation and, under no circumstances should this measure be used to track political dissidents or to conduct mass surveillance on the population.[60]

5.
Conclusion

As we have seen, there is no legislative body in which all the legal bases for State communication surveillance activities are contained. At the same time, the safeguards for Chileans against interferences with their rights to privacy and freedom of expression are spread between the Constitution, special laws, and international treaties.

Constitutional case law has not referenced the violation of these rights as a consequence of State surveillance acts, but we can turn to Inter-American case law where such pronouncements do exist and apply those standards to the cases in which those rights were infringed upon at the national level.

In Chile, the legal framework that supports State surveillance is found in criminal persecution—which mainly uses the Criminal Procedure Code as its guiding regulation, along with a series of legislations on crimes and services, which are based on the Code, and introduce some changes to the way in which the State communication surveillance must be conducted. This legislation is generally more permissive in its implementation, considering the danger these crimes pose, apart from being worsened by the vague and general criminal classifications.

The measure of telephone interception and other types of telecommunications is taken as the basis, for it is the most common. It is necessary to insist on the fact that even though one is regulated in a strict and rights-based way, its implementation—and the implementation of measures of a similar scope—does not always respect human rights. There is also an arbitrary discrimination in which telephone interceptions need to meet higher requirements, and the rest of the intrusive measures do not, despite the fact that they are all equally if not more invasive.

For instance, nowadays a cellphone is not used with the sole purpose of making calls. It would be easier to seize the mobile device of the accused than to request the interception of the phone calls made through the device, since it is not only a measure that is simpler to authorize, but it can also enable access to e-mails, social networks, messaging applications, call logs, and browsing histories, among others.

It should be noted that, except for the aforementioned problems, Chilean legislation complies with the International Principles on the Application of Human Rights to Communications Surveillance for the most part.

However, we should pay attention to State surveillance acts that are not specifically authorized by law. In particular, the recent purchase of the system Galileo, which in Chile was renamed as "Phantom," which the Chilean Investigations Police (PDI) acquired from Hacking Team—and the implications they have in relation to the violation of these principles.

1 United Nations, “The Right to Privacy in the Digital Age.” Report of the Office of the United Nations High Commissioner for Human Rights, 2014. pp. 3-4. https://eff.org/r.hz9z [Accessed on July 24, 2015.]

2 In Chile, the law (Law N° 19.974) establishes that whenever certain information is "strictly indispensable for the compliance with the aims of the State Intelligence System and it cannot be obtained from publicly accessible sources," (Article 23) special procedures may be conducted to obtain such information. These procedures are limited "to intelligence and counterintelligence activities which have the purpose of safeguarding national security and protecting Chile and its people from terrorist threats, organized crime and drug trafficking" (Article 23.) The procedures include: “a) The interception of telephone, computer, radio and correspondence communications in any of their forms; b) The interception of computer systems and networks; c) Tapping and electronic recording, including audiovisual communications; and, d) The interception of any other technological system designed for the transmission, storage or processing of communications or information” (Article 24).

3 Derechos Digitales, “Policía de Investigaciones de nuevo vulnera privacidad en Internet” ["Investigations Police Violate Internet Privacy Again"], Derechosdigitales.org. October 15, 2010 https://eff.org/r.rf9p [Accessed on: June 3, 2015]. Ver también Andrés López, “Aumentan solicitudes de antecedentes a Twitter por amenazas” ("Requests of Criminal Records from Twitter Increase by Threats"), La Tercera. February 16, 2013. https://eff.org/r.6nuh [Accessed on: June 3, 2015].

4 Francisca Rivas, “En libertad queda joven acusado de agredir a carabinero: pruebas sólo eran fotos de Facebook” [“Young Men Accused of Attacking a Policeman is Released: Evidence was solely Based on Facebook Pictures”], Rabio Bío Bío, May 20, 2014. https://eff.org/r.4u9z [Accessed on: June 3, 2015].

5 International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/text; EFF, ARTICLE19, Background and Supporting Legal Analysis on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/AnalisisLegal; Access, Universal Implementation Guide of the International Principles on the Application of Human Rights to Communications Surveillance, available at: https://eff.org/r.4gac [Accessed on: July 20, 2015].

6 *Ibid.*

7 The Chilean Constitution, when dealing with sovereignty in Article 5, Section 2, states: "The exercise of sovereignty recognizes as a limitation the respect for the essential rights which emanate from human nature. It is the duty of the organs of the State to respect and promote those rights, guaranteed by this Constitution, as well as by the international treaties ratified by Chile and which are in force." As a consequence of this provision, Chile takes into consideration not only the Constitution itself as the domestic legislation on this type of rights, but also the "constitutional block."

8 The scope of the rights established in international treaties has been discussed in detail in the Chilean legal system; that is, whether they have constitutional or merely legal hierarchy. The case law of the last decade has established that they have a supralegal status and are, at least, equivalent to the constitution's.

9 We based our statements on the grounds laid down in Lara, J., C. Pincheira, and F. Vera (2014). La Privacidad en el Sistema Legal Chileno, p. 22. [Privacy in the Chilean Legal System] Santiago de Chile: Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf [Accessed on: June 4, 2015].

10 The Chilean Constitution stands out as one of the Constitutions in Latin America in which there is no explicit acknowledgment of the protection of personal data. Vd. Remolina, N. (2012). Constitutional approach for the protection of personal data in Latin America. Revista Internacional de Protección de Datos Personales vol. 1, n. 1. [International Magazine on the Protection of Personal Data]. Bogotá: UDLA.

11 Two sentences can be mentioned at this point: To begin with, the Sentence STC N.º 389 granted the power to

collect information with no limitations whatsoever, which infringes upon the right to privacy. Thus, it is argued that the granting of this power, which has no objective or verifiable guidelines or parameters guaranteeing that the organism has subscribed to them, violates privacy, the inviolability of communications, and human dignity.

Secondly, Sentence STC N.º 433 ruled that the power of the Public Prosecutor's Office to request documents with no limitations also affects the right to privacy, because such power may not be granted to a public organism without establishing objective and verifiable guidelines. This violates the right to rational and fair procedure and investigations, and it also violates the essence of the right to private life and confidentiality of private communications.

Both summaries were taken from Carmona, C. and Navarro, E. (editors) (2011.) "Recopilación de Jurisprudencia del Tribunal Constitucional (1981-2011)", pp. 191-192. ["Collection of Case Law of the Constitutional Court"] Santiago: Constitutional Court.

12 Inter-American Court of Human Rights. Case of Escher et al. vs. Brazil, final sentence, 2009. http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf p. 34, paragraph 114. [Accessed on: June, 2015].

13 *Ibid.*, p. 35.

14 OAS. Inter-American Court of Human Rights. Tristán Donoso vs Panama, final sentence, 2009. p. 19, paragraph 56.

15 UN Special Rapporteur for the Protection and Promotion of the Right to Freedom of Opinion and Expression, Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights of the OAS, Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression: https://eff.org/r.973v [Accessed on: June 5, 2015].

16 Nogueira, H 2004. "Pautas para Superar las Tensiones entre los Derechos a la Libertad de Opinión e Información y los Derechos a la Honra y la Vida Privada" en Rev. derecho (Valdivia) [Tips to overcome the tensions between the Rights to Freedom of Opinion and Information and the Rights to Honor and Private Life] v.17 Valdivia, December, 2004. Available at: https://eff.org/r.4130 [Accessed on: June 14, 2015].

17 Chilean Constitutional Court (2010), "Requerimiento de parlamentarios y otros para que se declare la inconstitucionalidad del Movimiento Patria Nueva Sociedad." [Parliamentarian and other requirements to declare the unconstitutionality of the Movement "Patria Nueva Sociedad"] STC 567-06. Recital 30º. Available online at: http://www.tribunalconstitucional.cl/wp/ver.php?id=1386 [Accessed on: June 14, 2015].

18 García, G. and Contreras, P. (2014) Diccionario Constitucional Chileno. [Chilean Constitutional Dictionary] Santiago de Chile, Tribunal Constitucional de Chile, pp. 621-622.

19 Chilean Constitutional Court (2010), "Requerimiento de parlamentarios y otros para que se declare la inconstitucionalidad del Movimiento Patria Nueva Sociedad." [Parliamentarian and other requirements to declare the unconstitutionality of the Movement "Patria Nueva Sociedad"] STC 567-06. Recital 22º. Available online at: http://www.tribunalconstitucional.cl/wp/ver.php?id=1386 [Accessed on: June 14, 2015].

20 Carmona, C. and Navarro, E. op. quote, p. 178.

21 Silva, A. (2009). "El Derecho de Reunión en la Constitución de 1980. Temas Actuales de Derecho Constitucional, Libro Homenaje al Profesor Mario Verdugo Marinkovic", p. 305. [The Right to Assembly in the 1980 Constitution. Current Topics of Constitutional Law, Homage to Professor Mario Verdugo Marinkovic] Santiago:

Jurídica.

22 García, G. and P. Contreras (2014). op. quote, op. quote, p. 334.

23 Ana Piquer, "¿Qué significa la ley Hinzpeter?," acuerdos.cl, [What does the Hinzpeter Law Mean?] https://eff.org/r.54wj [Accessed on: July 10, 2015].

24 El Mostrador, "Vigilancia del gobierno a redes sociales trasciende fronteras y lo expone a ciberataque internacional," [State Surveillance on Social Networks Goes beyond Borders Putting Government at Risk of International Cyberattack] El Mostrador, June 22, 2011. https://eff.org/r.zijh [Accessed on : June 10, 2015].

25 Ciper Chile, "La polémica del monitoreo virtual" [The Controversy around Virtual Monitoring], Ciper Chile, June 22, 2011. http://ciperchile.cl/radar/la-polemica-del-monitoreo-virtual [Accessed on: June 10, 2015].

26 Soy Chile, "La PDI aclaró que tiene un programa para espiar computadores, pero que lo usa con autorización judicial" [Investigations Police of Chile made it clear that they have a software to spy on computers, but that they use it with judicial authorization], Soy Chile, July 6, 2015. https://eff.org/r.54wj [Accessed on: July 6,J 2015].

27 Investigations Police of Chile, National Public Affairs Department, "Press Release." Santiago, July 6, 2015. https://eff.org/r.gb5t [Accessed on: June 20, 2015].

28 Partarrieu, B and Jara, M. "Los correos que alertaron sobre la compra del poderoso programa espía de la PDI" [The E-mails that Warned about the Purchase ofPowerful Spy Software by the Investigations Police of Chile], Ciper Chile, July 10, 2015. https://eff.org/r.dwgm [Accessed on: July 20, 2015].

29 Once again, we refer to the topics touched upon in "La Privacidad en el Sistema Legal Chileno" [Privacy in the Chilean Legal System] pp. 70-73.

30 Ministry of Transport and Telecommunications, Undersecretariat for Telecommunications. Decree Nº 18 of February 13, 2014. "Aprueba Reglamento de Servicios de Telecomunicaciones que indica." [Indicated Telecommunications Services Regulations are Passed]

31 *Ibid.*

32 Lara, J, et al, op. quote, pp. 48-50. Available online at: https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf [Accessed on: July 9, 2015].

33 "A person intercepts a communication in the course of its transmission if, as a result of his interference in the system or monitoring of the transmission, some or all of the contents are made available, while being transmitted, to a person other than the sender or the intended recipient of the communication" in Oxford University, "Legal Opinion on Intercept Communication" (2006). Available online at: https://eff.org/r.jzz3 p. 7 [Accessed on: July 9, 2015].

34 Public Ministry, Public Prosecutor's Office. "Official letter N.º 060/2014 on the General Guidelines providing procedural criteria applicable to the Stage of Investigation in the Criminal Proceedings." Santiago de Chile, January 23, 2014. p. 20.

35 Ibid., op. quote p. 21.

36 La Segunda, "Golpe a la inteligencia policial: Fiscalía formalizará a ex oficial por escuchas ilegales" [A Blow to Intelligence Police: Public Prosecutor's Office will Sue Former Officer due to Illegal Wiretaps]. Urzúa, M and

Candia, V, March 16, 2013.

37 Álvarez, D. and A. Cerda (2005). “Sobre la Inviolabilidad de las Comunicaciones Electrónicas. Ley Nº 19.927 que Tipifica los Delitos de Pornografía Infantil” [On the Inviolability of Electronic Communications. Law Nº 19.927 Listing the Offenses related to Child Pornography] in Anuario de Derechos Humanos 2005, p. 137. Santiago: Law School, University of Chile. Available online at: http://www.anuariocdh.uchile.cl/index.php/ADH/article/viewFile/13264/13539. [Accessed on: July 9, 2015].

38 To consider the IP address as personal data is not a universal conception, for it changes across the legal systems around the world. Among those that recognize the IP address as personal data is Spain, whose regulations have had a great influence on the drafting process of the Chilean legislation. In 2003, the Spanish Data Protection Agency (AEPD, in Spanish) issued a report entitled “Carácter de dato personal de la dirección IP. Informe 327/2003” [IP Addresses as Personal Data, Report 327/2003], in which the conclusion is that "even though it is not always possible for all Internet agents to identify a user solely on the basis of data from the Network, this Data Protection Agency considers that the possibility to identify an Internet user is high, and, thus, both fixed and dynamic IP addresses, irrespective of the type of access, are considered as personal information, which makes the regulations on data protection applicable to them." This fragment can be found in Chaveli, E. “La Dirección IP, Problemas que Plantea” [IP Addresses and the Problems they Pose], 2011. Available online at: http://www.gesdatos.com/wp-content/uploads/La-direcci%C3%B3n-IP.pdf [Accessed on: September 24, 2015].

The case law of the Inter-American Court of Human Rights, in the aforementioned case of Escher et al. vs. Brazil, considers that the protection of private communication covers not only their content, but also the metadata associated to them. Hence, any type of communication conducted through the Internet, according to this Court sentence, is under protection, just as the IP address of the computer used for its emission. Taking into account that Chile has recognized the competence of this international jurisdictional body and the notion of "conventionality check" drafted by the IACHR, both the articles of the Inter-American Convention on Human Rights and their interpretation made by the Convention are directly binding for the States parties. Cfr. Hitters, J. “¿Son vinculantes los pronunciamientos de la Comisión y de la Corte Interamericana de Derechos Humanos? (control de constitucionalidad y convencionalidad)” [Are the Declarations made by the Commission and the Inter-American Court of Human Rights Binding? (Constitutionality and Conventionality Check)] in Revista Iberoamericana de Derecho Procesal Constitucional, issue nº 10, July-December, 2008, pp. 131-156.

39 See note 38.

40 Chile, 1979. Ministry of National Defense. Decree Law N.º 2.460 “Chilean Investigations Police Organic Law.”

41 Chile, 1990. Ministry of National Defense. Law N.º 18,691 “Police Force Organic Law.”

42 Morelos, J. “¿Qué es Hacking Team y su herramienta DaVinci?” ["What's Hacking Team and What's its DaVinci Tool?"], luisgyg.com, July 7, 2015. http://www.luisgyg.com/blog/2015/07/07/que-es-hacking-team [Accessed on: July 20, 2015].

43 Investigations Police of Chile, National Public Affairs Department, "Press Release." Santiago, July 6, 2015. https://pbs.twimg.com/media/CJQdW9KW8AEg9Rl.jpg [Accessed on: July 20, 2015].

44 Peña, P. and F. Vera (2014). “Derecho a protesta y vigilancia policial en redes sociales” ["The Right to Protest and Police Surveillance in Social Networking"], Digital Rights Lac, June 30, 2014. Available online at: http://www.digitalrightslac.net/es/derecho-a-protesta-y-vigilancia-policial-en-redes-sociales [Accessed on: July 20, 2015].

45 OAS, UN. “Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression,” June 21, 2013. Available online at: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927 [Accessed on: July

20, 2015].

46 National Institute for Human Rights of Chile (INDH, in Spanish.) "Report on Issues to Consider in the Amendment of the Antiterrorism Law in Light of the Observation of Cases by the National institute for Human Rights." Passed by the Council of the National Institute for Human Rights on July 22, 2014. pp. 4-7. Available online at: http://bibliotecadigital.indh.cl/bitstream/handle/123456789/655/Informe%20Ley%20Antiterrorista.pdf?sequence=1 [Accessed on: June 24, 2015]

47 *Ibid.*, p. 7.

48 United Nations. Human Rights: "Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism," ohchr.org, July 30, 2013. Available online at: http://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=13598 [Accessed on: June 24, 2015].

49 Lara et al., op. quote pp. 63-69

50 Sentence "Caso Bombas" [Bombs Case] R.I.T. N.º 138-2011, R.U.C N.º 0700277303-6.

51 Senate of the Republic, Press Department. "Director de la ANI expuso en sesión secreta sobre situación de La Araucanía" ["Head of the ANI Presented the Situation of 'La Araucanía' in Private Session."] Available at: https://eff.org/r.p7np

52 International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/text; EFF, ARTICLE19, Background and Supporting Legal Analysis on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/AnalisisLegal; Access, Universal Implementation Guide of the International Principles on the Application of Human Rights to Communications Surveillance, available at: https://eff.org/r.4gac [Accessed on: July 20, 2015].

53 FayerWayer, "Chile: Derechos Digitales denuncia a la Policía de Investigaciones por no respetar la vida privada" [Chile: Derechos Digitales Files a Report against the Investigations Police for Violating the Right to Private Life], April 26, 2012. https://eff.org/r.z6r1

54 The Twitter annual report is available at: https://transparency.twitter.com/country/cl [Accessed on: September 24, 2015] and the Facebook report at: https://govtrequests.facebook.com/country/Chile/2014-H2/ [Accessed on: September 24, 2015].

55 OAS, "Inter-American Convention on Mutual Assistance in Criminal Matters," 1992. http://www.oas.org/juridico/english/treaties/a-55.html [Accessed on: July 22, 2015].

56 FayerWayer, "Chile: Formalizan a abogado por crear una cuenta de parodia en Twitter del empresario Andrónico Luksic" [Chile: Lawyer Sued for Creating a Twitter Account to Mock Businessman Andrónico Luksic], February 19, 2013. https://eff.org/r.2lnm

57 Ruiz, C. (2014). "Sobreseimiento definitivo en causa de Luksic versus parodia en Twitter" [Definite Dismissal of the Case of Luksic vs Parody in Twitter]. https://eff.org/r.rhzq

58 House of Representatives of Chile, Newsletter Nº 9243-10 "Agreement between the Government of Chile and the US Government on the Increase of Assistance in the Prevention and Combat against Serious Crimes Passed in Washington, D.C," May 20, 2013.

http://www.camara.cl/sala/verComunicacion.aspx?comuid=10784&formato=pdf [Accessed on: July 22,].

59 Lara, J, Martínez, M and Viollier, P (2014). "Towards a Regulation on Computer Crimes Based on Evidence," en Revista Chilena de Derecho y Tecnología [Chilean Magazine of Law and Technology] (2014), pp. 106-107.

60 United Nations, op. quote.