Chile

What is the legal framework that protects people's privacy in Chile?

Chile has the following constitutional and legal protections:

- 1980 Constitution: Article 19, paragraph 4. The respect and protection of privacy and honor of the person and his family; and paragraph 5: Invulnerability of the home and all forms of private communication. The home may be searched and communications and private documents intercepted, opened or registered only in the circumstances and manner prescribed by law.
- Law 19,628 of Personal Data Protection
- General Telecommunications Law No. 18.168 Art 24 M.: “Dealers and vendors will seek to preserve the privacy of users, protection against viruses and security of the network.”

What is the legal framework that allows for the surveillance of communications in Chile?

One of the biggest problems is that there are extremely vague rules and obsolete laws that are not tailored to rapidly changing technology and the current reality. In addition, the protective legislation is dispersed, divided amongst the Constitution, laws, and administrative regulations, which makes things difficult to monitor and control. Such legislation can be found below:

- Regulation of the Telecommunications Act (2014)
- Regulation of Interception and Recording of Telephone and Other Telecommunications (2005)
- Telecommunications Services Regulations, Decree No. 18 (2014)
- No. 18,314, better known as the “Anti-Terrorist Act,” which defines terrorist conduct and sets criminal sanctions; and Law No. 20,000, which penalizes illicit drug trafficking (usually called the “Drug Law”)
- Articles 218, 219, and 220 of the Criminal Procedure Code (interception of communications)
- Article 222 of the Criminal Procedure Code (wiretapping)
- The Public Ministry outlines its ability to carry out surveillance in the Office FN 060/2014. This document establishes that the persecuting body may contemplate the use of surveillance during the investigation of complex cases: kidnapping, murder, drug trafficking, money laundering, certain economic crimes, public corruption, sexual offenses and, in general, investigations linked to certain groups or organized crime.
Who has the authority to monitor communications in Chile?

The Public Ministry may grant the Investigations Police (PDI) (in particular the Phone Monitoring Department, Demtel) legal authority to intercept communications.

According to the Regulation on Interception and Recording of Telephone Communications and Other Forms of Telecommunications, Ministry of Transport and Telecommunications of 2005 (which establishes general guidelines on telecommunications interceptions in order to protect privacy and, at the same time, facilitates wiretapping for police work in criminal investigations) the following requirements must be followed in order to conduct communications interception:

- Communications between the accused and his lawyer cannot be intercepted. Exceptional cases include when a Judge of Guarantees (Juez de Garantía) requests the interception because the judge believes the attorney is suspected of being criminally involved in the case under investigation.
- A warrant to facilitate or order the interception and recording must indicate, in detail, the name and address of the affected and, simultaneously, detail the means and duration of the interception which may not exceed sixty days.
- Telephone and communications companies must comply with the request. They must provide officers the necessary means so that the officers are able to monitor communications as needed.

Regarding the recording of communications, Article 223 of the Criminal Procedure Code specifically states:

- The interception will be recorded via tape recording or other similar technical means to ensure the integrity of the recording.
- The recording will be delivered directly to the Public Prosecution Service who will keep it under seal and ensure it is kept private from any third parties.
- Under his consideration, the Public Prosecutor may order a written transcript of the recording and a public official will act as a notary to ensure the validity of the recording. Without prejudice to this, the Public Prosecutor shall preserve the original recording.
- Any communications that were captured, but were unrelated to the procedure, will be immediately delivered to those affected by the measure and any transcript or copy that has been made of them will be destroyed by the prosecution.
- This does not apply to captured recordings that may contain information relevant to the investigation.

How do I know if my communications have been intercepted in Chile?

According to Article 224 of the Criminal Procedure Code (CPP): “Those who have been affected by the measure of interception shall be notified after its completion, with the investigation permitting, and to the extent that such notification will not endanger the life or physical integrity of third parties.”

This law redirects to Article 182 of the CPP, which stipulates that the Prosecutor’s investigation must be kept secret from third parties outside of the process. The secret investigation has a time limit of 40 days, except in specific, exceptional cases.
What are the rules that the Chilean State must comply with when requesting data (content, metadata, subscriber information) from an intermediary Internet company?

The law requires Internet Service Providers to retain “an updated list of authorized IP addresses and a record of the numbers of connections their subscribers made for at least one year,” (Art. 222 CPP). The respective regulations (DS 142 2005) reiterate this rule, ordering companies to preserve metadata and subscriber data.

The law establishes this obligation in connection with the rules on wiretapping. Similarly, its procedural rules for requesting data are concise. It specifies that those “responsible for conducting diligence [interception and recording of communications] and employees of the companies mentioned in [the law] shall keep secret about it, unless they are called as witnesses in the investigation.” In that sense, the authority can perform this measure, upon court order, if there is a “justified suspicion, based on certain facts, that a person has committed or participated in the preparation or commission of a crime, or is currently planning on carrying out or participating in a crime punishable by law.”

There are no specific legal or regulatory rules concerning the application of personal subscriber data or metadata. At minimum, a court order (pursuant to Article 9 of the Criminal Procedure Code) is required, which is similar to most other cases involving the use of investigative measures that may violate fundamental rights.

Is the Chilean State legally authorized to use malware?

In theory, Law 19,974 on “The Intelligence System of the State” allows for the use of malware by establishing, in broad terms, special investigative procedures (Article 24, B and D), “The intervention of computer systems and networks” and “the intervention of any other technological systems for transmission, storage or communications or information processing.”

Such procedures are only legally valid when they are limited “to intelligence and counterintelligence activities that aim to safeguard national security and protect Chile and its people from the threats of terrorism, organized crime, and drug trafficking.” This power is exercised by the police and intelligence services of the armed forces that are part of the State Intelligence System, prior to judicial authorization.

Is the use of encryption legal in Chile?

Yes. There are no legal or regulatory limitations on encrypting communications or content encryption. Nor are there any legal or regulatory rules that require the decryption of communications and content.

How many communications have been wiretapped by the Chilean State?

The annual report by the Public Ministry does not reveal figures related to this. Likewise, there is no regulation that enables people who are directly impacted by these measures to know whether they have been, or are being monitored, or whether their information has been given over to the government.
Platforms like Facebook and Twitter release annual transparency reports where in which the number of requests for information from various governments is revealed. Chile is among those governments.

Is the Chilean government interested in protecting the privacy of its citizens?

Chilean legislation mostly complies with international human rights standards. However, it is important to look at the State surveillance occurring that is not specifically authorized by law, such as the investigative police’s recent purchase of “Phantom” from Hacking Team. We must look at the implications such systems may have and how they may violate privacy, and these principles. Also, we must give particular attention to the announced draft legislation on personal data which would replace the current Law on the Protection of Privacy (19,628) and give a new status to the use of personal information.


2 http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi/