What is the legal framework that protects people's privacy in Peru? Are my rights protected against State communications surveillance?

Peru is subject to the various international human rights treaties it has ratified. These treaties, such as the American Convention on Human Rights and the International Covenant on Civil and Political Rights, recognize the right to privacy and other fundamental freedoms. They are binding and applicable directly in Peruvian jurisdiction.

Article 2 of the Political Constitution of Peru of 1993 outlines the rights guaranteed to all persons, including: (i) the assurance that information services, whether computerized or not, or public or private, will not provide information affecting personal and family privacy, (ii) the right to personal and family privacy, (iii) the inviolability of the home, and (iv) the secrecy and inviolability of private communications and documents. In that vein, the Peruvian Constitutional Court has repeatedly recognized the scope of this case law, understood as:

"[...] The personal sphere on which a human being has the ability to develop and enhance their own personality freely. Therefore, it is considered that [this right] is formed by the data, facts or personal circumstances, that being true, are strictly reserved for the knowledge of the subject themselves and a small group of people, and their disclosure or knowledge by others causes some damage."

Article 2, paragraph 10 of the Constitution also protects the inviolability of private communications:

10. Secrecy and the inviolability of private communications and documents. Communications, telecommunications, or any private correspondence may only be opened, seized, intercepted or wiretapped by an authority with a warrant issued by a judge and with all the guarantees provided in the law. Any matter unrelated to the circumstances under examination shall be kept secret.

There are also some legal regulations that protect the right to privacy and the protection of personal data. These include:

• Article 13 of Personal Data Protection law

---

1 Constitutional Court, on the proceedings N. 6712-2005-HC / TC. October 17, 2005.
“Communications, telecommunications, computer systems or their instruments, when they are private or for private use, may only be opened, seized, intercepted or audited by a motivated order of the judge or with the authorization of their subject, with the guarantees provided in the law. Secrecy is kept concerning the matters unrelated to the fact that motivates their examination. The personal data obtained in violation of this rule has no legal effect.”

- Article 4 of the Single Revised Text of the Telecommunications Law states that the inviolability and secrecy of telecommunications is protected by law.

- Article 13 of the Telecommunications Regulation establishes that a violation of this right occurs when someone who it is neither the sender nor receiver deliberately steals, intercepts, interferes, alters or changes the text of the communication, publishes or uses it in any way, or directs it away from its intended destination.

**What is the legal framework that authorizes the surveillance of communications in Peru?**

The process for which an authority may intervene on communications is described in Law 27,697 and detailed in the Penal and Criminal Procedure Codes, as well as in the Protocol of Joint Action for Intervention or Record Keeping Telephone Communications or Other Forms of Communication, approved by Ministerial Resolution No. 0243-2014-JUS.

According to this legal framework, only a judge may authorize a prosecutor to listen and control the communications of an accused person who is the subject of a preliminary or judicial investigation corresponding to a particular list of offenses including:


**Who has the authority to access stored information and intercept communications in Peru and by what means?**

Criminal prosecutors (*Fiscales Penales*), public prosecutors (*Procuradores Públicos*), and the Attorney General (*Fiscal de la Nación*), in certain cases, may issue a request for the interception of communications. The communications surveillance is carried out by authorized personnel of the Public Ministry (*Ministerio Público*) and/or the National Police under the supervision of the prosecutor in charge of the investigation. The law allows for the assistance of the telecommunications companies to carry out surveillance in real time and, if the characteristics of the communications require it, authorities can also request assistance from individuals or legal experts in monitoring activities. The interception request that the prosecutor sends to the judge must contain all the necessary information and specify all the factors and circumstantial evidence that may allow the judge to issue a well-informed authorization. If the request is denied, the prosecutor may appeal to a superior judge the day after they are notified. The prosecutor’s request and the judicial authorization must contain specific information that differentiates it from other kinds of collections and

---

2 Law No. 29733, Personal Data Protection Law, available at: [https://eff.org/r.beoh](https://eff.org/r.beoh)
controls the aim to be carried out, including:

1. Whether the communication is clearly determined, whether it is likely to occur within an indeterminate group of communications, or whether it will occur in certain circumstances.

2. Whether the communication will occur in the future or has already happened.

3. Whether the communication is accessible to any person who will perceive it, or if it is private or encrypted.

4. Whether there has been an attempt to conceal the identity of the sender or receiver of the communication, or any other person, event or circumstance mentioned in the communication; as well as describing any difficulties designed to prevent accessing or identifying the communication, its parts, or information mentioned therein.

The National Intelligence System also contemplates scenarios in which government authorities can use communications surveillance, authorized by Legislative Decree 1141 on the Strengthening and Modernization of National Intelligence System (SINA) and the National Intelligence Directorate (DINI) as well as its regulations.

Are the telecommunications companies required to retain my communications data? Under what conditions may authorities access my communications data?

• Yes, Legislative Decree No. 1182, which has been in force since July 2015, requires telecommunications companies and public entities related to these services to retain telecommunications data for twelve (12) months on a computer system and must allow authorities to consult and access the data online in real time with prior judicial authorization. After 12 months, telecommunication companies must keep the data for an additional twenty-four (24) months in an electronic storage system.

• The data that has been stored for more than twelve months must be delivered within seven (7) days of the judicial authorization.

• The decree authorizes the police to require any telecommunications operator access to the location data of mobile phones or electronic devices. Further information on the Peruvian campaign against Legislative Decree 1182, here: http://www.hiperderecho.org/dl1182/

• According to law, telecommunications companies such as Movistar or Claro are required to provide real-time access to their data after the police request it. Meaning, prior judicial authorization is not required. This rule applies when three requirements are fulfilled simultaneously: (i) there is a flagrant crime;\(^4\) (ii) the investigated crime is punishable by over four years in prison, and (iii) accessing this information is necessary for the investigation. By the time the police assess whether these three requirements have been fulfilled, they will have already had access to the data. So, the unit in charge of the police investigation will have twenty-four (24) hours to send a report to the prosecutor that supports their request and the prosecutor will have twenty-four (24) hours to ask a judge to authorize the measure. In turn, the judge who receives the order will have twenty-four (24) hours to rule on the legality of the request and set the period of validity.

---

\(^3\) In early February 2015, the Peruvian government announced its intention to completely restructure the National Intelligence System. The results of such restructuring may involve partial or total renewal of the aforementioned laws.

\(^4\) There is flagrante delicto when a crime is being committed, has just been committed, or up to 24 hours after it has been committed (Criminal Procedure Code, Article 259).
In October 2015, by Ministerial Resolution No. 0631-2015-IN, the Home Office approved the “Access Protocol of Geolocation Data from Mobile Phones or Electronic Devices of a Similar Nature,” which establishes the process for accessing geolocation information created by Legislative Decree No. 1182. However, invoking the national security exception of the Law of Transparency and access to Public information, the Ministry has classified the text of the Protocol as “Confidential.”

Is my geolocation information protected under the Constitution and Peruvian legislation?

Yes, the Constitution recognizes that everyone has the right to privacy and the inviolability of communications. In particular, it states that communications, telecommunications and any private correspondence may only be opened, seized, intercepted or wiretapped by a warrant issued by a judge and with all the guarantees provided in the law. Similarly, since 2009 Peru has had a special rule that was approved by the Department of Transport and Communications that establishes safeguards for the right to the inviolability and secrecy of telecommunications. The rule expressly outlines the scope of the protection of the right to privacy and inviolability of telecommunications to include “the source, destination, conduct, course or duration of a communication.”

In encryption legal in Peru?

Yes, there is no legislation or practice that bans the use of encryption.

Is the State authorized to use malware to spy on my communications?

No. In the context of a criminal investigation, it is possible to order the interception of telephone communications or any other form of communication (including electronic communications). Furthermore, it is also permissible to intercept communications for the purpose of obtaining copies or backups of e-mail addressed to or sent by the accused with a court order. A prosecutor may also request the seizure of goods—such as computers—and request the disclosure of private documents with a judicial order. All of these activities are carried out by the Public Ministry in collaboration with the National Police. However, the Criminal Procedure Code does not mention using tools to compromise computer systems to obtain information in the form of “hacking.” There is no knowledge of the systematic use of these mechanisms.

How can I find out if the State is surveilling my communications?

A person who has been subjected to communications surveillance can request the judge, up to three days after the initial notification, to conduct judicial review. However, the intelligence system keeps the proceedings confidential, classifying the information as secret work.

We do know that a user will not be notified when authorities gain access to their geolocation data. Authorities even prohibit companies from disclosing their involvement in providing geolocation data to them.

How many communications have been intercepted by the Peruvian State?

The Peruvian State is not required to release transparency reports about its monitoring activities; it is not subject to public oversight. Apart from the notifications a person gets whose communications were surveilled as part of a criminal
investigation, there is no mechanism or law that requires the authorities who carry out these measures to report on the number of interventions that have been made, the type, nor the scope.

In the intelligence system, the only public oversight mechanism that exists is the Congressional Intelligence Committee, but all of the information that the Committee receives is classified and secret.

Recently, the lack of control over the intelligence system’s activities has led to a political crisis that resulted with the deactivation of the system and its upcoming reorganization.5

**Has the Peruvian State shown an interest in protecting the privacy of its citizens?**

The Peruvian government has formally demonstrated their commitment to privacy, but in recent years privacy protections in the country have been eroding this right thanks to the introduction of various legal instruments. Specifically, some of the rules related to public security, drug trafficking, and intelligence reform have eroded legal guarantees that protect private information and personal data.

Once Legislative Decree No. 1182 entered into force, the police no longer needed to get explicit judicial authorization to obtain private information. Now they can obtain data directly from the telecommunications companies with a single request if they consider themselves within the criminal conduct established by the Legislative Decree.

---

5 “Gobierno cerrará la DINI por 180 días para su reestructuración,” *El Comercio*. Feb 9, 2015, available at: [https://eff.org/r.v79d](https://eff.org/r.v79d)