Paraguay

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

Paraguay is subject to international treaties on human rights. 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. These treaties are international obligations adopted by the State and they apply to domestic law.

At the national level, Article 33 of the Constitution also recognizes the right to privacy. Article 36 protects the right to private communications and the integrity of communications. Personal data is protected in Article 135 of the Constitution.

Are my rights protected against State surveillance of communications?

In addition to constitutional protections, Law No. 1160/97 of the Criminal Code establishes penalties for intercepting, recording, storing, or facilitating the interception of communications that belong to a third party. The same penalties exist for those who violate a third party's privacy by disseminating private images of that person.

Regarding the confidentiality of communications, Article 146 states that anyone who violates someone’s right to communications privacy is subject to a penalty of up to one year in prison or a fine. Unfortunately, Paraguay does not have a truly comprehensive law on personal data protection.
What is the legal framework that allows for the surveillance of communications in Paraguay?

Articles 25, 26, and 27 of the Penal Code define the legal procedures for communications interception. In particular, Article 26 states:

Article 26 - “Judicial authorization. The Secretary of National Intelligence is responsible for seeking judicial authorization to use the procedures outlined in the previous article. The application must be filed with the Criminal Court of Guarantees in the location where the respective procedure will be performed.

The judge has 24 hours to authorize the interception according to the preceding article by a reasoned decision, under penalty of nullity, without further ado. The judicial authorization should specify the means to be used, the identification of the person or persons to whom the measure will apply, and the deadline, which may not exceed 90 (ninety) days, renewable once up to an additional period.”

Article 27 - "Review. The National Intelligence Secretary must deliver the results of the measure to the judge who ordered it, who shall review the content and, if necessary, order a written transcription of the recording, or the parts considered useful, and order the destruction of any intercepted content that is unrelated to the procedure, prior to accessing it."

In short, the Penal Code makes clear that in order for intelligence agencies to suspend the right to private communications and conduct surveillance:

1. the interception in question must be exceptional in nature and there must not be a less onerous means of obtaining such information;
2. the interception measure must be related to State assets and interests established by law;
3. the measure must be approved by judicial authorization;
4. the identification of the person(s) being investigated must be precisely defined (banning mass or indiscriminate surveillance);
5. the surveillance measure must be carried out within a certain, limited period of time.

There are other regulations that reference surveillance, including the special law on drug trafficking (Articles 88, 89, and 91).

The law’s chapters on “controlled deliveries” and “covert operations” establish communications interception. The law states that in order for interception to be considered lawful:

1. the measure must be approved by judicial authorization;
2. the interception in question must be exceptional in nature and there must not be a less onerous means of obtaining such information;
3. the specific type of communications to be intercepted must been specified;
4. the relevance of the interception must be defined;
5. the judge has the ability to request additional justification for the issuance of the measure, if necessary;
6. there must be a deadline for the interception;
7. the judge and the prosecutor shall be responsible for monitoring each interception;
8. those involved in the interception process shall maintain confidentiality and respect the privacy of individuals.

In addition, Article 10 of the Electronic Commerce Act (Law 4868/13) states that the companies that provide Internet in Paraguay, and those that provide data hosting, should store data traffic for at least six months. The law does not include any legal safeguards. This article limits judicial and police power to access stored company data.

Who has the authority to monitor communications in Paraguay and by what means?

The graphic below explains the procedure for communications surveillance in criminal matters:

What's the process to intercept communications during a criminal investigation?

1. Attorney General prosecution
2. Police examination
3. Complaint
4. Attorney General requests authorization for intercepting communications
5. Judge of Guarantees authorizes the interception
6. The Drug Enforcement Agency (SENAD) and National Police carry out the interception
7. Judge of Guarantees and Attorney General oversee the interception to ensure no rights are violated

In addition, intelligence agencies can intercept communications through a process that begins with an investigation by the National Criminal Intelligence Secretariat and a request to obtain information from the same institution. The Court of Guarantees may authorize such interception, and if it does, it is responsible for monitoring the interception.

Are telcos forced to keep my communications? Under what conditions may the police access my communications data?

No, the bill on mandatory data retention was rejected in Congress. However, Article 10' of the Electronic Commerce Law 4868/13. Available at: [http://www.eljurista.com.py/admin/publics/upload/archivos/ea41b40fb8ce27bd7ec64237fd75ef80.pdf](http://www.eljurista.com.py/admin/publics/upload/archivos/ea41b40fb8ce27bd7ec64237fd75ef80.pdf) Date Accessed: Dec. 2, 2015.
Law 4868/13 requires telecommunications companies to store at least six months of data “relating to electronic communications.” This article prevents the judicial power and law enforcement from accessing this retained data retained for criminal investigations.

**Can the state legally hack into my computer to monitor my communications?**

The legal scenario is uncertain. There is no specific regulation that allows authorities to use malware to monitor a person’s communications. However, Article 200 of the Code of Criminal Procedure provides that a judge may order the interception of communications of an accused “regardless of the technical means used to achieve it.” This is a dangerously broad power considering the many ways that new technology can be used to spy on citizens. In all cases, judicial authorization is required to carry out such measures.

We believe the law should require specific authorization to employ such practices (and it should be clear that such measures shall only be authorized when they are the least burdensome way to obtain the necessary information).

**Is encryption legal in Paraguay**

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

**How can I find out if my communications have been or are being monitored?**

Notifying a person who has been the subject of surveillance is not mandatory in Paraguay so it is very difficult for a person to know whether their communications have been surveilled. Incorporating user notification into law is necessary so a person can exercise their right to defense. Such notification should only be deferred if the judge responsible for granting the authorization determines that the notification could jeopardize the investigation. In any case, the law should set deadlines for the deferral of notification.

The notification should detail all of the materials that were obtained through the surveillance measure so that the affected person may know the content and scope of the invasion of privacy and exercise their right to remedy.

**How many communications have been intercepted by the Paraguayan State?**

The rules governing communications surveillance in both criminal proceedings and intelligence work do not require the publication of transparency reports. The annual reports of the National Police, the Public Ministry, and SENAD do not disclose the number of surveillance requests that have been approved or rejected, nor a breakdown of requests by service provider, authority, type, and purpose.

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

In Paraguay “there is insufficient information” about the use of surveillance tools by the State. Paraguayan law does not compel the State to issue transparency reports about the number of surveillance requests the police and intelligence
agencies have submitted. Nor does it have an agency that specifically oversees surveillance activities. Paraguay does not have a law on personal data protection just as there is nothing that protects users from abuse or violation of their communications privacy, in accordance with State obligations on human rights guarantees. The only mechanism available is Habeas Data, which is insufficient.

However, we must emphasize that there are no rules or regulations that prohibit anonymous speech or the use of encryption tools, which help to protect the privacy and security of communications.