Uruguay

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

Uruguay has ratified the American Convention on Human Rights and the International Covenant on Civil and Political Rights. Both treaties are international obligations assumed by the State and are applicable in domestic law. Both treaties expressly recognize the right to privacy.

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

- Article 212 of Uruguay’s Criminal Procedure’s Code (Interception of Correspondence and Other Communications)
- Article 5 of Law 18,494 Control and Prevention Laundered Assets and Funding Terrorism (electronic surveillance) - “The investigation of any offense may use all technological means available to facilitate clarification.”
- Article 25 of Law 18,331 of Personal Data Protection and “Habeas Data” Action: Database corresponding to the Armed Forces, law enforcement or intelligence agencies.
- Article 75 of Law 19.1

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

Article 5 of Law 18,494 on the Control and Prevention of Laundered Assets and Funding Terrorism establishes that electronic surveillance may be used when investigating certain crimes provided for by law. The State may use “all technological means available” in order to conduct electronic surveillance during an investigation provided the prosecutor receives permission from a competent judge via an issued order. The surveillance and subsequent collection must be overseen by the judge. The court is then responsible for selecting the particular collected material that will be used in the case and what material shall be considered unrelated and thus discarded. However, other agencies have surveillance capacities that are not regulated by law and could thus operate without legitimate aims. This is particularly worrisome when we think about the deregulation of the intelligence sector.¹

¹ Authorities involved would be the DINACIE (National Directorate of State Intelligence), the National Coordinator of Intelligence and some...
Can the Uruguayan State legally hack into our computers? Under what circumstances and legal authority?

The situation is unclear. Article 5, on electronic surveillance, allows for the State to use “all technological means available” to investigate any crime. A broad interpretation of Article 5 could mean that this provision authorizes various types of surveillance techniques and technologies such as the use of malware or IMSI-catchers. However, due to the age of the norm, we must consider that its creators did not take into account the level of intrusion new surveillance techniques and technologies have when drafting the law. What is needed is an explicit, clear, and precise legal authority to authorize such excessively invasive surveillance.

In encryption legal in Uruguay?

Encryption is legal in Uruguay. There is no legislation nor practices that prohibit the use of encryption in Uruguay.

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

In Uruguay, there exists no obligation for prior notification when a subject is the target of surveillance.

A person should have a right to know if they have been subjected to surveillance so it is necessary for Uruguay to incorporate a prior notification obligation into its law. This notification should only be deferred if and only if the judge responsible for granting authorization determines that notification could jeopardize the legitimate aim of the investigation. In any case, the law should establish deadlines for the deferral of notification. In Uruguayan legislation, the accused will learn that his or her communications have been intercepted at the time of the hearing.

How many communications have been wiretapped by the Uruguayan State?

The Supreme Court revealed that between January 2009 and March 2014, a total of 6,150 wiretaps were ordered by criminal judges. During that time, the criminal courts that authorized the most interceptions were the two that specialized in organized crime, authorizing 2,192 interceptions. There is no consolidated report on the use and scope of the surveillance laws, regulations, activities, powers, or guides. At the very least, the State should publish comprehensive information on the number of requests approved and rejected, a breakdown of applications by service provider, by investigating authorities, the type and purpose, and the specific number of people affected by each and according the type of research and their purposes. States should provide individuals with sufficient information to enable them to fully understand the scope, nature, and application of the laws permitting communications surveillance.

Has the Uruguayan government shown an interest in protecting the privacy of its citizens?

Considering the purchase of the electronic surveillance system “The Guardian” as well as the secret negotiations for the unmapped units within the structure of the various arms of the state (Land, Air and Sea).

---

purchase of malware it seems that the State cares more about obtaining invasive surveillance technology to spy on its citizens with greater scope and efficiency rather than protecting their privacy. Unfortunately the adoption of clear and precise limits that serve as strong guarantees against any potential abuse of power has not kept up with technological modernization.