State Communications Surveillance and the Protection of Fundamental Rights in Paraguay

By Jorge Rolón Luna and Maricarmen Sequera Buzarquis
in collaboration with Katitza Rodríguez and David Bogado

March 2016

ELECTRONIC FRONTIER FOUNDATION

TEDIC

Jorge Rolón Luna is a lawyer who studied international human rights law at Oxford University and the University of Rome Tor Vergata. He is currently a professor in the College of Communication Sciences at the Catholic University of Asunción. Previously he worked as the commissioner of the National Prevention Mechanism against Torture in Paraguay (2012-2015) and was a judge from 1996-2002.

Maricarmen Sequera Buzarquis is the executive director of TEDIC, a non-profit organization based in Paraguay that develops civic technology and works to protect human rights on the Internet. She is a lawyer who graduated from the National University of Asunción with a focus in intellectual property. She worked for the Department of International Relations at Paraguay's Executive Office (2009-2011) and has conducted research on politics and law in Beijing. She previously lived in Paris where she expanded her knowledge on human rights in the digital age.

This report was drafted in partnership with the Electronic Frontier Foundation (EFF). We would like to thank Katitza Rodríguez, International Rights Director at EFF, and David Bogado, Latin American Community Development Coordinator at EFF, for leading a substantial revision of this report; and Kim Carlson, EFF, for her editing and formatting work.

This report is part of EFF's "Surveillance and Human Rights" project carried out in eight countries in Latin America by the Electronic Frontier Foundation, an international non-profit organization that, since 1990, has been defending freedom of expression and privacy in the digital world.

Table of Contents

Introduction....4

I. Constitutional Framework....6
1.1 Normative Power of International Human Rights Treaties in the Constitution....6
1.2 Constitutional Framework....8

II. Legal Framework....12
2.1 State Communications Surveillance in the Criminal and Criminal Procedure Legislation....12
2.2 State Communications Surveillance in Telecommunications Legislation....15
2.3 State Communications Surveillance in Intelligence and Counterintelligence Legislation....16
2.4 Further Provisions related to State Communications Surveillance....18
2.5 Bills that Jeopardize Internet Communications....20

III. Case Law on Communications Surveillance....23

IV. Communications Surveillance Technology....25

V. Institutional Framework....27

VI. International Principles on the Application of Human Rights to Communications Surveillance....30

VII. Conclusions and Challenges....34

Introduction

From 1954-1989, Paraguay was a dictatorship—the longest-lasting to ever occur in South America, unceasing for 35 years.[1] During that time, communications were intercepted and recorded systematically and illegally by the State and stored in the databases of intel agencies. One such example are the "Terror Files," a database belonging to the police that was discovered in 1992[2]

Twenty-seven years after the fall of the authoritarian regime, the country is finally a democracy. However, the democratic institutions that have been in place since the 1992 Magna Carta are still weak.

In this context, over the past few years emergency bills have been introduced through legal exceptions that have resulted in a criminal system that protects against real or alleged criminal acts. These types of regulations are legal tools used to relieve a society that has been shaken by violence, crime, terrorism or any kind or political turmoil.

These real or alleged criminal acts, or "critical" situations, provoke a type of legal inflation—often due to the belief that violence, crime, terrorism of any kind, and political turmoil can only be solved through penalty increases, the criminalization of new behaviors, restrictions on the right to defense, dismissal of judicial guarantees, or invasions on people's private lives.

The result is a punitively-minded State; one that makes regulatory changes that violate constitutional rules, criminal law, and criminal procedure principles and undermines international human rights law in addition to redefining the role of law when dealing with social conflicts.

There are many laws already in force in the country, as well as laws that have been rejected and others that are under review in Congress that are heading in this direction. At the time of this report's publication—March 2016—a Parliamentary Commission for Penal Reform has the task of reviewing the country's penal and criminal procedural law.[3] Paraguay's justification for advocating for such punitive and security-based legislation—to protect the safety of all citizens, even if it conflicts with individual rights—was based on a misconception: crime is a phenomenon that is solved (or not) using four branches of the penal system: criminal law, police work, the courts, and the penitentiary system. The same criteria used for analyzing the irrational use of pretrial detention in criminal policy can also be used to, for example, analyze the uncontrolled intrusion, or surveillance, into peoples' private lives as a tool to investigate certain crimes.

Globally, we see these fundamental rights threatened by laws and bills that often ignore constitutional rights and guarantees that are otherwise recognized by State constitutions and international treaties.[4] This usually happens in cases where public safety or the democratic system is at stake. Still, little is known about Paraguay's alleged acquisition of advanced surveillance technology, its technical capabilities, and the level of which it interferes with fundamental freedoms.[5]

This report analyzes Paraguay's normative framework (constitutional, international, and legal) for the protection of fundamental rights against government surveillance. It also studies the main laws—specifically, rules from the criminal investigation system and the intelligence service—which empower authorities to carry out communications surveillance in the digital age. Based on this analysis, we then examine whether Paraguay's national legislation complies with the international human rights standards, using the International Principles on the Application of Human Rights to Communications Surveillance as a guide.[6] Given the technical and legal complexity of this report, the terms "communications surveillance" and "communications" will be used as they appear in the International Principles on the Application of Human Rights to Communications Surveillance:[7]

- Communications surveillance: to monitor, intercept, collect, analyze, use, preserve, save, interfere or obtain information that includes or reflects the past, present or future communications of a person.

- Communications: The activities, interactions and transactions transmitted by electronic means, such as content, identity, location tracking information—including IP address, time and duration of communications, and identifiers of the equipment used.

I.
Constitutional Framework

1.1 Normative Power of International Human Rights Treaties in the Constitution

The preamble to Paraguay's constitution (hereinafter, PYC), recognizes the validity of international human rights law:

> *Reaffirming the principles of republican, representative, participative and pluralistic democracy, ratifying the national sovereignty and independence, and integrating the international community.*

The PYC frequently reference the international system and the validity of a supranational legal order in its articles. The most significant provisions are:

Article 137: Of the Supremacy of the Constitution

> *The supreme law of the Republic is the Constitution. [La Constitución], the treaties, conventions and international agreements approved and ratified, the laws dictated by the Congress and other juridical provisions of inferior hierarchy, sanctioned in consequence, integrate the positive national law [derecho positivo] in the formulated order of preference [prelación]. (...)*

Article 141: Of International Treaties

> *International treaties validly celebrated, approved by [a] law of the Congress, and whose instruments of ratification were exchanged or deposited, are part of the internal legal order with the hierarchy determined in Article 137 (...)*

Article 145: Of the Supranational Juridical Order

> *The Republic of Paraguay, in conditions of equality with other States, admits a supranational juridical order which guarantees the enforcement of human rights (...)*

Article 143: Of International Relations

> *The Republic of Paraguay, in its international relations, accepts international law and adjusts itself to the following principles: (...) 5. the*

international protection of human rights;

Other provisions related to the international treaties in question include:

Article 122: Of the Matters That May Not Be the Object of [a] Referendum

> *[The following] may not be the object of [a] referendum: 1. international relations, treaties, international conventions or agreements;*

Article 142: Of the Denunciation of the Treaties

> *The international treaties relative to human rights may only be denounced by the procedures that govern for the amendment of this Constitution.*

Article 215: Of the Delegated Commission

> *Each Chamber, with the vote of the absolute majority, may delegate to commissions the treatment of bills of laws, of resolutions and of declarations. By a simple majority, it may withdraw them in any state prior to the approval, rejection or sanction by the commission.*
>
> *The General Budget of the Nation (...), the codes, the international treaties may not be the object of delegation.*

Article 224: Of the Exclusive Attributions of the Chamber of Senators

> *[The following] are exclusive attributions by the Chamber of Senators: 1. to initiate the consideration of bills related to the approval of international treaties and agreements:*

Article 238: Of the Duties and of the Attributions of the President of the Republic

> *[The following] are duties and attributions of whomever exercises the presidency of the Republic:*
>
> *(...) 7. (...) to negotiate and to sign international treaties;*

After carefully examining these articles, we conclude that: Paraguay accepts supranational legal order, meaning international treaties and agreements are recognized as part of Paraguay's legal system and enjoy a higher hierarchical order than national laws. Such international agreements cannot be repealed by referendums—any denunciation of human rights treaties must follow the same procedure as constitutional amendments.

Recent case law developed by the Inter-American Court of Human Rights (hereinafter IACHR) compels judges to conduct adequacy tests.[8] This obligation goes hand in hand with other important considerations outlined by the IACHR, such as a list of non-

derogable human rights. Even if a law is endorsed by the will of the people, that doesn't necessarily grant it legitimacy under international law.[9] The IACHR has compelled officials from all State sectors to conduct adequacy tests on their acts and legislation.[10]

1.2 Constitutional Framework

1.2.1 Right to Privacy[11]

There are many ways to define the right to privacy. Some definitions emphasize the impassable space of a person's individual freedom, which cannot be invaded, trespassed or intruded upon by third parties—be they individuals or the State. From this perspective, the right to privacy is considered the sovereignty of private life. Privacy also involves a person's right to control his or her personal information. Privacy is a fundamental right, and it is critical for a functioning democracy and human dignity. The right to privacy in the PYC Constitution encompasses the inviolability of the home and correspondence, rights related to the reproduction of images, intimacy (*intimidad*), and the protection of personal data.

Regarding the right to privacy, Article 33 of the PYC outlines:

Article 33: Of the Right to Privacy

> *Personal and family intimacy, as well as the respect of private life, is inviolable. The behavior of persons, that does not affect the public order established by the law or the rights of third parties[,] is exempted from the public authority. The right to the protection of intimacy, of dignity, and of the private image of persons is guaranteed.*

The right to privacy reinforces other rights such as: freedom of speech and press, the right to fair and balanced information and the right to assembly, which are all protected in the PYC.[12] In turn, Article 36 of the PYC states:

Article 36: Of the Right to the Inviolability of Documental Patrimony [Patrimonio Documental] and Private Communication

> *The documental patrimony of individuals is inviolable. The records, regardless of the technique used, the printed matter, the correspondence, the writings, the telephonic, telegraphic, cable graphic or any other kind of communication, the collections or the reproductions, the testimonies and the objects of testimonial value, as well as their respective copies, may not be examined, reproduced, intercepted, or seized [secuestrados] except by a judicial order for cases specifically provided for in the law, and when they would be indispensable for [the] clearing up of matters of the competence*

> *of the corresponding authorities. The law will determine the special modalities for the examination of commercial accounting and of obligatory legal records. The documental evidence obtained in violation of what has been prescribed above lacks validity in trial. In every case, strict reservation will be observed regarding every thing that is not related to the [person] investigated.*

1.2.2 The Protection of Personal Data

Article 135 of the PYC enshrines the right to data protection:

> *All persons may access the information and the data about themselves, or about their assets, [that] is [obren] in official or private registries of a public character, as well as to know the use made of the same and of their end. [All persons] may request before the competent magistrate the updating, the rectification or the destruction of such information, if it were wrong or illegitimately affected their rights.*

Additionally, Law 1682/01,[13] amended by Law 1969/02 regulates the treatment of private data.

According to Article 1:

> *This law is designed to regulate the collection, storage, distribution, publication, modification, destruction, duration and overall, the processing of personal data in files, registers, data banks or other technical means of treatment of public or private data intended to provide reports, in order to ensure the full exercise of the rights of the owners. This Act shall not apply in any case to databases or to sources of journalistic information nor freedoms to express opinions and to inform.*

The dissemination or disclosure of "sensitive" personal data is prohibited.[14] However, it is legal to collect, store, process, and publish personal data or characteristics in the context of scientific or statistical investigations, polls and surveys about public opinion, or market studies. Personal data revealing, describing or judging an individual's private property, financial solvency, or compliance with commercial obligations may only be published if explicit authorization is given by the data subject, or if the data are taken from public sources, or when State or private entities are required to disclose such information in accordance with specific legal provisions.[15]

Alternatively, the law authorizes the publication and dissemination of personal data that is considered public, such as an individual's name, ID number, address, age, date and place of birth, marital status, occupation or profession, work place, and work phone number.[16] At

the time of this report's publication, modifications to the law are being debated in Congress,[17] but any changes that will be implemented are unknown.

The Martín Almada[18] case of 1992 was the most iconic case of habeas data the country had ever seen.[19] Almada, a victim of Alfredo Stroessner's military dictatorship, was able to unveil the secret *stronista* police database called "the Terror Files" by requesting personal data about himself through a habeas data constitutional remedy. These files have been recognized by UNESCO as part of the Intangible Heritage of Mankind. While these files include thousands of documents that reveal police practices, it should be noted that other important files such as the military files or those belonging to the Ministry of Foreign Affairs have not been published yet.

> Nowadays, if an individual wants to file a writ of habeas data, they need to do so before a trial judge. However, if the sought-after information could be contained in the "Terror Files," they simply need to submit a request. Such request must be submitted to the Documentation and Archives Center [Centro de Documentación y Archivo] which relies on the Supreme Court of Justice—where the aforementioned files can be found. In that case, the citizen needs only to complete a form, attach a copy of their identification documents, and include a brief summary about the section of the file in which the requested document is located. No competent judge may deny the writs or remedies provided for in the previous articles; were a judge to do so with no justification, he or she would be prosecuted and, when appropriate, removed from his or her position, pursuant to Article 136 of the constitution.

1.2.3 Communications Surveillance

As stated above, the right to privacy is protected in Paraguay's constitution. Article 30 of the CR further establishes that:

Of Electromagnetic Communications Signals

> *The emission and propagation of electromagnetic communication signals are in the State's public domain, which, in the exercise of its national sovereignty, shall promote their implementation according to the rights of the Republic and pursuant to the international conventions ratified on this subject. The law shall guarantee, on a level playing field, full access to the use of the electromagnetic spectrum, as well as to the electronic tools for the collection and processing of public information, with no further limits than those imposed by international regulations and technical norms. The authorities shall make sure that these elements are not used to infringe upon personal or family privacy and the other rights established in this Constitution.*

As stated in the last part of this article, the State must ensure that the electronic tools for the collection and processing of information are not used to violate the privacy and other rights of its citizens established in the constitution. Thus, the State is clearly obligated to respect the privacy of individuals. Moreover, this article recognizes that these electronic tools pose risks and threaten human rights.

II.

Legal Framework

2.1 State Communications Surveillance in the Criminal and Criminal Procedure Legislation

When analyzing criminal legislation in Paraguay, we bear in mind the following considerations:

First, the job of criminal law is not to take action in all cases involving dangerous behavior or to protect all legal rights. It is solely meant to protect only the most important rights so not to trivialize them or burden the courts and prosecution offices.

Next, criminal law must not protect legal rights from all aggressions, but only from the most important ones, due to the piecemeal character of criminal law.[20]

Lastly, criminal law must only be applied when all other effective remedies have been exhausted in preventing misconduct. The principle of criminal subsidiarity, or *ultima ratio*, provides that criminal law shall only be employed if society as a whole cannot be, with equal effectiveness, sufficiently protected with less harmful controls.[21]

The same principles apply for authorizing State surveillance. Disproportionate intrusions based on the possibility that an infinitesimal part of the population might eventually commit a crime clashes with the principle of minimum intervention desired by the State.

> *Along with this problem comes the long-discussed—utilitarian and rights-based—function of Criminal Law as the protection of citizens against the restrictions on subjective rights and fundamental interests, be they individual or collective. The notion of the legal right that refers to the principle of the seriousness of crimes as a necessary condition for the justification of criminal prohibitions is seen as the external axiological limit (with reference to the rights deemed as politically primary) or the internal axiological limit (with reference to rights protected by the constitution) to Criminal Law. On the other hand, the policies on Criminal Law seem to be oriented nowadays in the exact opposite direction. In fact, the unchained criminal intervention is continuously expanding, and has come to be, (...) the main instrument for legal regulation and social control...*[22]

Finally, international standards on the topic of analysis must be applied; in this case, everything related to communications surveillance, which as we mentioned earlier, includes 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."[23]

2.1.1 Criminal Code

The Criminal Code (hereinafter CP), Law N° 1160/97[24] regulates infringements upon the right to communications and to self image. In particular, it indicates that those who, without the subject's consent: (i) listen using technical instruments; (ii) record or store communications; or (iii) make, through technical means, an individual's communications that were not said publicly immediately available to a third party, shall face imprisonment of up to two years or be fined.

The same regulation is applied to those who, without the consent of the affected, produce or transmit images: (i) of another person on his or her private property; (ii) of another person's private property; (iii) of another person outside his or her property, in violation of the right to private life. The same punishment shall apply to those who share a recording, as described above, with third parties.

Article 146: Violation of the Secrecy of Communications

> *1°) Those who, without the consent of the subject: open a closed letter not addressed to them;*
>
> - *Those who open a letter, as described in article 14, point 3, that is closed or inside a closed package or specially destined not to be opened by them, or those who learn or communicate to a third party the content of a letter; or those who through technical means and managing to keep it closed learn its content or communicate it to third parties,*
> - *shall be punished with imprisonment for up to one year or with a fine.*
>
> *2°) Criminal prosecution shall depend on the basis of the charges brought by the victim. The provisions set out in article 144, subsection 5, last section shall be applied.*

2.1.2 Criminal Procedure Code

Law N° 1286 of July 8, 1998 establishes the following:

Article 198 – Interception and seizure of correspondence: Whenever it is useful in order to find out the truth, the judge shall order, by a sustained judicial order, and under penalty of invalidity, the interception and seizure of postal, telegraphic or any other kind of correspondence, sent by or to the accused, even when the accused went by a false name or alias. The limitations to the seizure of documents and objects shall apply also in this case.

Article 199 – Opening and inspection of correspondence: Once correspondence or objects are intercepted, the judge shall open them, placing the procedures on record. The judge shall examine the objects and read the contents of such correspondence to himself. If they are related to the procedure, he shall order the seizure of the elements; otherwise, he shall keep the confidentiality of their content and order their delivery to the addressee.

Article 200 – Communications Interception: The judge shall order, by a sustained judicial order, and under penalty of invalidity, the interception of the communications of the accused, irrespective of the technical means used to learn them. The result may only be delivered to the judged that ordered the interception, who shall proceed according to the provisions of the previous article; he shall order the written version of recordings or of those parts he deems useful, and order the destruction of the recording or the parts of it that do not relate to the procedure, with the prior access to it of the Public Ministry, the accused and his or her defense counsel. Communications interception shall be exceptional. (...)

Article 228 – Reports: The Judge and the Public Ministry may request reports from any person or public or private entities. Such reports shall be requested orally or in written, and they shall indicate the procedure to be followed, the name of the accused, the place where the report must be handed over, the deadline for submission and the consequences provided for when failing to report.

From this, we gather four rules:

- When it comes to the interception of any type of correspondence, including e-mails, it is only the judge who may order the interception;
- A lack of judicial authorization would make the procedure invalid;
- The judge is in charge of the content of the intercepted information, communicating it to the Public Ministry, and subsequently destroying the evidence;

- The interception of private communications is exceptional.

In short, neither criminal procedural law nor criminal law allow for, in criminal investigations, violations to the right to privacy by the body of the criminal prosecution (Public Ministry).

2.2 State Communications Surveillance in Telecommunications Legislation

2.2.1 Law N° 642/95 on Telecommunications

This law from 1995 that created the National Commission on Telecommunications (Conatel, in Spanish)—the country's regulatory body of telecommunications—explicitly protects the inviolability of communications:

> *Article 89 – The correspondence sent through telecommunications and documental patrimony services is inviolable, except by a judicial order. This provision is applicable to the staff of telecommunications services, as well as to any individual or user with knowledge about the existence of such correspondence or about its content.*
>
> *Article 90 – The inviolability of the secrecy of correspondence transmitted via telecommunications encompasses the prohibition of opening, subtracting, interfering, altering, diverting, publishing, using, learning or facilitating to third parties the existence or content of communications entrusted to service providers and the prohibition of setting the conditions to commit such actions.*

2.2.2. Executive Decree 14135/96[25] (Annex)

> *Article 9: The inviolability and secrecy of communications are attacked when a person who is not the issuer nor the addressee of a communication deliberately takes, intercepts, interferes with, changes or alters the text, diverts, publishes, uses, learns or facilitates to third parties the existence or content of any communication. The individuals who, due to their responsibilities, have access to the content of a communication held via telecommunications services, are obliged to preserve and guarantee the inviolability and secrecy of such communication. Telecommunications service providers are compelled to adopt the most adequate measure to guarantee the inviolability and secrecy of communications held via such services.*

This reinforces what is established in procedural legislation:

- Communications are inviolable;
- Public or private service providers or individuals with access to the content of a communication are compelled to preserve and guarantee the inviolability and secrecy of such communication and refrain from making it available to third parties;
- Judicial authorization is needed in each case.

2.2.3 Resolution of the regulatory body

Conatel's Resolution 1350/2002[26] goes against Law 642/95 on Telecommunications. This resolution gives telephone service providers the power to store a detailed call log of all Paraguayan users for a period of six months:

> *Article. 1. – A time period of six (6) months shall be established as the obligatory duration for the preservation of call logs—either incoming or outgoing—to all the lines that make up the client list of different mobile phone service providers (STMC, in Spanish) and/or the System of Personal Communication (PCS).*

Call logs, text messages, and location data are now stored for six months as established by Conatel's Resolution, a resolution that was crafted during the same year in which there were several kidnappings for ransom that shocked the Paraguayan society.[27]

This pre-investigation measure for any type of offense is disproportionate in relation to the pursued aim. It clearly ignores the State's ideal of minimal intervention when it comes to criminal law, characteristic of "minimum criminal law."[28]

2.3 State Communications Surveillance in Intelligence and Counterintelligence Legislation

2.3.1 National Intelligence System

Articles 6, 24, 25, 26, and 27 of Law Nº 5241/14, which creates the National Intelligence System (SINAI, in Spanish) set out the right to the inviolability of documentary heritage by stating that:

> *Article 6. – Inviolability of Documental Patrimony. Telephone, postal, fax or any other system of communication to deliver objects or transmit images, audio, data packets or any other type of information, file, and/or private documents, or documents that are not meant to be read or accessed by the public shall not be examined, reproduced, intercepted or seized, except with a judicial order, as long as they are indispensable for the specific objectives*

defined by this law (...)

Title III – Procedures for the Collection of Information

Article 24. – Exceptionality. The procedures to obtain information established in this Title are only applicable when the bodies or institutions of the National Intelligence System (SINAI) are not able to obtain such information from open sources. The information to be obtained must be strictly necessary for the achievement of the State's objectives to protect peace, national security, institutional stability and prevent terrorist threats, organized crime and drug trafficking while defending the constitutional and democratic system.

Article 25. – Classification. The procedures described in the previous article are the following:

1. *Interception of telephone, computer, radio communications and of any kind of correspondence;*
2. *Interception of computer systems and networks;*
3. *Wiretaps and electronic audiovisual recording; and,*
4. *Interception of any other technology system for the transmission, storage or processing of communications and information.*

Article 26. – Judicial Authorization. It is the Secretary of National Intelligence who requests the judicial authorization in order to conduct the proceedings described in the previous article. The request shall be submitted to the Supervisory Criminal Judge on duty in the place in which the proceedings are to be conducted.

The judge may order, by a sustained decision and under penalty of invalidity, to conduct the procedures referred to in the article above, within 24 (twenty-four) hours, without further proceedings. The resolution ordering this must specify the means to be used, the individualization of the person(s) to which the measures apply and their duration, which may not be longer than 90 (ninety) days, which might be extended for 90 days more.

Article 27. – Examination. The Secretary of National Intelligence must hand over the result of the procedure to the judge that ordered it, who shall listen to the content by himself. He may also ask for a written version of the recording or of parts of it that he deems useful, and order the destruction of the recording or a part of it when they do not relate to the procedure, having previously accessed them.

The interception of communications and the intrusion on privacy by intelligence institutions have five specific features to take into account:

1. *The interception of the communications in question must be exceptional and indispensable;*
2. *Interception is only conducted in cases related to legal rights or State interests established by the law;*
3. *A judicial authorization is required, otherwise the procedures are invalid;*
4. *The investigated individual(s) must be specified. (Massive or unidentified interception is prohibited);*
5. *Intelligence investigations have limited duration.*

2.4 Further Provisions related to State Communications Surveillance

2.4.1 Special Law on Combating Drug Trafficking[29]

The National Anti-drug Department (SENAD, in Spanish) is an institution that falls under the executive power.[30] According to the law that established it, "it will coordinate the actions or government agencies that work on programs against drug trafficking and drug addiction." But without constitutional and legal provisions, it essentially acts as a security agency. The law provides the agency with the following responsibilities:

> *Article 88. – The judge may order—when appropriate and for a limited period of time—upon the request of the SENAD or the prosecutor, that they or their duly identified agents take pictures or videotape the suspects and their actions and intercept, record, tape or reproduce their verbal, cable or electronic communications. The request shall contain the types of situations that are supposed to be photographed or filmed or the types of communications that are supposed to be intercepted, recorded, taped or reproduced, together with the technical means that are going to be used, and the aims pursued by the implementation of such procedures. The judge may demand that the requester hand over additional elements supporting the request. Only the collected documents that are related to the investigated acts shall be placed on record or preserved.*
>
> *Article 89. – The judge authorizing the measure and the Public Ministry shall follow up and supervise each operation and investigation, thus being able to give instructions when they are in progress.*

The judge and the Public Ministry shall constantly be informed about the course of the operations and investigations, and the evidence obtained shall be made available for them.(...)

Article 91. – Those who authorize, control or intervene in undercover operations or controlled deliveries must strictly keep the confidentiality of such operations and are compelled to respect the personal and family privacy of individuals.

Communications interceptions established by law can be found in the chapters related to "Controlled Deliveries" and "Undercover Operations."

From these articles we conclude that:

1. A judicial authorization must be granted in each case;
2. The interception of communications and correspondence is exceptional;
3. There should be specific instructions about the type of communication to be intercepted;
4. Interception must be appropriate (relative to the pursued aims);
5. The judge may request further reasons to order the measure, when he considers it is necessary;
6. The interception must be conducted during a limited time period;
7. The judge and the corresponding prosecutor must supervise and follow-up on each operation and investigation;
8. Those participating in the operations ("Controlled Deliveries" or "Undercover Operations") are compelled to respect the privacy of the individual and keep any information strictly confidential.

2.4.2 Law on Electronic Commerce

Law 4868/13 on Electronic Commerce also poses a risk to the privacy of communications in Paraguay. Article 10[31] compels Paraguayan Internet service providers and data brokers to store traffic data or data "relative to electronic communications" for at least six months.

This law does not include minimum safeguards that would protect private information, nor does it include criteria to justify company data collection. This article limits judicial power and the police by only giving them access to data stored by companies.

2.4.3 Further Provisions related to Mandatory Data Retention

Paraguay does not have a specific law compelling telephone or Internet service providers to retain the communications data of its entire population for criminal prosecution purposes.[32] However, it *does* provide for voluntary data retention for commercial purposes.

In 2014, a bill, dubbed "Pyrawebs," (an allusion to the police espionage that was conducted during the military dictatorship) that would have compelled Internet service providers to store their users' metadata for 12 months for alleged criminal investigation purposes was nearly approved in by congress. After a grassroots campaign against the bill, it was rejected in the senate.

2.5 Bills that Jeopardize Internet Communications

2.5.1 Bill against Organized Crime

Pursuant to Article 1 of the draft bill, its objective is to "... define the rules and procedures for the use of special investigation techniques in the investigations related to Organized Crime."[33]

As any other special law, its rules and procedures are exceptional and give unusual powers to state agents involved in such investigations. According to its description, the bill aims to adequately combat criminal organizations, which, in our globalized world, use the technology that is available and the large financial resources that result from the illegal activities they carry out to their advantage. To that end, the State must provide for adequate laws and procedures to deal with these types of crimes—special investigation tools seem to be the most useful remedies as described below:

> *Techniques or tools that allow the collection of elements or means of proof that help obtain useful information in order to combat organized crime, as established by both the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988, (Vienna Convention of 1988), and the United Nations Convention against Transnational Organized Crime (Palermo Convention). In view of the provisions established in these international documents and of the experiences in the practice, the most efficient special investigation techniques against organized crime are: communications interceptions, controlled deliveries, the use of undercover agents, whistleblowers and developer agents, the existence of safeguards in the process for the protection of witnesses, the confidentiality of identities where appropriate and any other techniques guaranteeing the celerity and success of the investigations conducted to that end, among others.*

In the case of this bill, the offenses to which these special techniques apply are clearly specified. The list is quite long, it includes 17 criminal offenses of the Criminal Code, special laws against drug trafficking,[34] the special law adopting the provisions of the Customs Code on human trafficking;[35] the law on Firearms;[36] the anti-terrorism law,[37] and other criminal laws.[38]

The bill establishes that, as part of the investigation of these crimes, "electronic surveillance" may be conducted, which is defined as follows:

> *...electronic surveillance is the special investigation technique that allows for the use of all technological and/or electronic means—present or future—which allow to obtain information and means of proof with respect to the commission of a punishable act or to identify the perpetrators and accomplices.*

According to this bill, such surveillance may be:[39]

- Adequate, necessary, and indispensable for the clarification of the investigated punishable acts;
- Authorized when the situation requires it;
- Conducted whenever there is a justified suspicion about the commission of one or more punishable acts that are included in organized crime;
- Always necessary, reasonable, and proportional;
- Requested by the Public Ministry; A judicial authorization shall always be needed pursuant to the provisions set out in Article 125 of the Criminal Procedure Code;
- Monitored and supervised by the Public Ministry; regardless of the supervision that higher authorities will exercise over the agents involved.

2.5.2 Bill for the Protection of Children and Adolescents against Harmful Content on the Internet[40]

At the time of this report's publication, a bill is being discussed in the first constitutional instance of the National Congress. The bill aims to regulate Internet content filtering on public Wi-Fi networks and even among Internet Service Providers (ISP).

> *Article 3: Of Active Protection. "Internet Service Providers (ISP) must provide and install, obligatorily and for free, in the benefit of their users and clients, who shall declare at the moment of subscription or subsequently, whether girls, boys or adolescents are going to have access to the Internet, or in the benefit of anyone that requests it, a specific software with systems of*

detection, filter, classification, elimination or blocking of inappropriate contents, pursuant to article 2, handing over the corresponding manuals and indications for use.

The National Commission on Telecommunications (CONATEL), through its competent technical unit, shall establish using technical norms the requisites and minimum conditions that the software must meet, as well as its implementation and availability.

This law initiative neglects the principle of net neutrality[41] as an essential aspect of users' freedom of expression and privacy. This bill gives too much power to third parties, in this case to Internet Service Providers, to act as guardians of the Internet who control their users' Internet browsing.

III.

Case Law on Communications Surveillance

There is an emblematic case from the highest court involving communications surveillance in Paraguay. In ruling N° 674/10,[42] the Supreme Court rejected an extraordinary appeal in a case involving Cecilia Cubas, the daughter of former President Raúl Cubas Grau (August 1998 – March 1999) who was kidnapped on September 21, 2004 when a criminal group encircled her car meters away from her house on the outskirts of Asunción. Cecilia Cubas was found dead on February 16, 2005.[43]

The Supreme Court stated that all the procedural guarantees were met and that the Public Prosecutor's Office did not violate the suspects' communications privacy by requesting and obtaining—without a judicial order—the metadata of phone calls made by the kidnapping and murder suspects.

> *The response given by the Court of Appeals was specific and satisfactory. Pursuant to article 228 of the CPP, the Public Ministry may request reports from any person or public o private entity. Article 316 of the CPP, in relation to the powers of the Public Ministry, reaffirms that "it may demand information from any official or government employee, in accordance with the circumstances of the case. All public authorities are obliged to collaborate with the investigation, depending on their respective competences, and to comply with the requests for reports made in conformity with the law." Moreover, the fact that the Public Ministry has had access to the reports and subsequently processed them did not represent any violation, neither constitutional nor legal. As shown, the information provided data about the subjects as regards phone line, date, time, phone numbers of incoming and outgoing calls, and the geolocation from where they were made. It had access to the details on the cross-referencing of calls, but not to their content, in which case the legal right being violated would have been the inviolability of communications and the right to privacy.*[44]

In short, the Supreme Court's stance on the inviolability of communications is as follows:

- Article 36 of the National Constitution on the right to the inviolability of documental heritage and private communications protects communications *per se* —the words that may have been said by the accused on a phone, but not the data

associated to these communications (with whom, when, the frequency, among others).

- In the expert opinion on cross-referencing calls, it makes clear that the data in question is the telephone companies' records that consist of the investigated telephone number, the incoming and outgoing calls of such number, the date and time such calls were made; none of these represents the content of a telephone communication—what a person says and what the other person hears by using a telephone.

- In the expert opinion on cross-referencing calls, the examination is based on the data of phone calls that remain after the communication has ceased, and not on the communications that such data generated; the communication is protected by our constitution, but the object of examination is not.

- In the expert evaluation in which the communication data (also known as metadata) was subject to examination, a judicial order was not obligatory, since the witness expert's work did not affect the constitutional protection of metadata, and because there was an actual judicial order as per the Public Ministry's job.

The fact that the Court has taken these considerations into account without evaluating the criteria on metadata being discussed internationally nowadays is troublesome and demands attention. From the perspective of the application of human rights to communications surveillance, the Public Ministry does not have the power to request such reports, much less without a judicial order, since it violates privacy.

Neither does the Court take into account the Inter-American Court of Human Rights' decision in the case where Brazil was sentenced for illegal wiretaps in a criminal process.[45] The Court itself believes the right to privacy protects both the content of the electronic communication and any other data associated with the technical process of a communication, such as metadata or traffic data. This is understood as "the destination of outgoing calls and the origin of the incoming ones, the identity of the interlocutors, the frequency, time and duration of the calls, which are aspects that may be observed without the need to register the content of the call through the recording of conversations."

IV.

Communications Surveillance Technology

Through the Ministry of Interior, the State has recently started the process of public tender for the purchase of technology to equip institutional security.[46] The tender document does not describe the details of the software for reasons involving confidentiality. The National Congress has requested reports on the software, but it is unknown whether or not they've gotten a response.[47]

In addition, Wikileaks[48] exposed a series of diplomatic cables which revealed that during Fernando Lugo's presidency (2008 – 2012), then-Minister of Interior, Rafael Filizzola, held conversations with the U.S. embassy in order to learn about a new cell phone interception program. By the end of 2014, the National Police Commander admitted, on television, that the police resort to using wiretaps with no judicial authorization only to prevent and persecute punishable acts related to kidnapping and extortion.[49]

Paraguay was involved in the Hacking Team leaks scandal as well. The prosecutor of the Computer Crimes Unit of the Public Ministry, Ariel Martínez, is believed to have held conversations in 2014 about the purchase of spy software from the Italian company, Hacking Team,[50] according to e-mails released by Wikileaks.[51] Hacking Team's flagship product is a system used to intercept computers, video calls, e-mails, instant messages, and passwords: the Remote Control System (RCS). According to an investigation carried out by Privacy International,[52] this software is capable of dodging the encryption of computer programs, monitoring communications and call logs, viewing browsing history, files and pictures that have been deleted from a device. In addition, it is able to take control of a computer or cellphone's microphone and camera and use them to spy. According to an official declaration, Paraguay never purchased the system.[53]

Paraguay is connected to another case involving surveillance technology, this one, calledFinFisher. Citizen Lab,[54] a multidisciplinary laboratory at the University of Toronto, published a report on the characteristics and uses of the FinFisher system,[55] and lists Paraguay as one of the countries that acquired its software (whose functioning is similar to that of Hacking Team's). The report highlights that the institution that controls it is unknown.

It is clear that the Paraguayan State—if it has not done so already—is in the process of expanding (or at least planning to expand) its advanced systems of communications surveillance technology. And all without the appropriate safeguards. Paraguay has no

regulations that compel accountability, public oversight regarding the use and scope, or transparency reports in the criminal process and/or in intelligence activities.

There is no independent body that supervises those who authorize surveillance requests nor those who make the requests. There are no mechanisms for user notification in neither the criminal process nor the intelligence process, so that citizens may exercise a democratic control on the implementation of the powers of the State.

V.

Institutional Framework

Below is a list that outlines the bodies involved in the criminal prosecution system in Paraguay (including the National Police). Following that is an outline of the criminal process for communications surveillance.

Figure 1: Organizational chart of the bodies involved in communications surveillance

1. Judicial Branch—Supervisory Judge (Authorizing Judge)
2. Public Ministry (Prosecutors)
3. National Police / SENAD (National Anti-Drug Department)

Figure 2: Procedure for communications interception

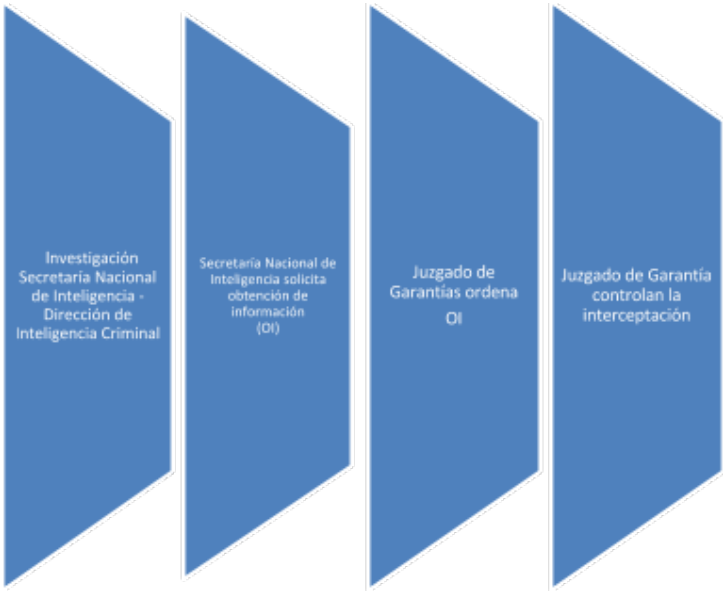
1. Prosecutor's Investigation, Police Investigation and Criminal Report
2. Interception is Requested by the Public Prosecutor's Office
3. Interception is Ordered by the Supervisory Judicial Authority
4. The National Police and the SENAD conduct the interception
5. Supervisory Judge and Public Prosecutor's Office examine the interception

Figure 3: Intelligence system in Paraguay

Figure 3 is an organizational chart of Paraguay's intelligence system and its functioning. Then, a diagram of the steps that intelligence bodies need to follow to obtain information.[56]

Judicial Branch (Supervisory Judge)
//
Secretary of National Intelligence
//
Department of Criminal Intelligence
//
Military Intelligence – SENAD (National Anti-drug Department) – Police Intelligence

Figure 4: Procedures that intelligence bodies follow to conduct communications surveillance



1. Investigation. Secretary of National Intelligence – Department of Criminal Intelligence
2. Secretary of National Intelligence Submits Request to Obtain Information
3. Supervisory Judicial Authority Orders to Obtain Information
4. Supervisory Judicial Authority Oversees the Interception

VI.

International Principles on the Application of Human Rights to Communications Surveillance

In this section, we analyze whether Paraguayan legislation complies with the standards set by the International Principles on the Application of Human Rights to Communications Surveillance.[57] These Principles are deeply rooted in international human rights law and compliance with such standards is imperative to the human rights framework which can now be found in Paraguay's domestic constitutional norms, as well as in the international human rights documents signed and subscribed by the country. The compliance with such principles is, consequently, equivalent to the supralegal norms in force. Therefore, States must comply with its international rights obligations.

Now we shall analyze some provisions in the national legislation authorizing communications surveillance activities and their compliance with the International Principles:[58]

- 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. Given the rate of technological changes, laws that limit human rights should be subject to periodic review by means of a participatory legislative or regulatory process.*

Citizen Lab's revelations about the State's alleged purchase of malicious software has sparked serious concerns. Its use in the country is not explicitly authorized by domestic legislation, let alone is its implementation or scope specifically regulated. In some cases, the laws, like Article 200 of the CPP, are so vague that they leave the door open for the future use of any type of tool, including those that could be malicious. These types of imprecise laws can be used to authorize more intrusive surveillance than just the mere interception of communications. This requires a public debate in Congress and other spheres about the need for additional safeguards, including transparency, public oversight, prior judicial authorization, among others.

- PROPORTIONALITY: *Decisions about communications surveillance must be made taking into account the benefit that is pursued and the harm it would cause to*

individuals' rights and to other interests in conflict, and it should include an assessment of the sensitiveness of the information and the seriousness of the restriction on the right to privacy. Moreover, the information will be accessed only by the specified authority and used only for the purpose and duration for which authorization was given. (...) Any excess information collected will not be retained, but instead will be promptly destroyed or returned. (...) That the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

Domestic laws establish that communications surveillance shall be exceptional. However, mass and *a priori* communications surveillance for criminal investigations, like the Resolution of Conatel, which compels mobile phone companies to store cellphone metadata and text messages for six months goes against this Principle.

- COMPETENT JUDICIAL AUTHORITY: *Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent.*

When it comes to the interception of communications, the laws and resolutions previously analyzed in this report establish the obligation, by a sustained decision and under penalty of invalidity, to make the request through the order of a competent judge. Pursuant to Articles 166, 168, and 169 of the Criminal Procedure Code, situations like these are the cause of absolute invalidity, and cannot be restored nor validated. In Paraguay, no entities are authorized to intercept private communications without a judicial order, according to the legal order in force. It is not possible for evidence obtained illegally, such as the illegal communications surveillance, to be corrected *a posteriori* by a judge.

- 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:

1. *Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorized, or there is an imminent risk of danger to human life; and*

2. *Authorization to delay notification is granted by a Competent Judicial Authority; and*

3. *The User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.*

In neither the criminal process nor the legal framework governing the activities of the intelligence agencies are there mechanisms in place for deferred user notification for any type of intrusion into private life.

- 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.*

The laws that regulate communications surveillance do require the State to submit transparency reports in neither the criminal process nor over the activities of the intelligence agencies. The National Police, the Public Ministry, and SENAD's annual reports do not contain the number of requests approved and rejected, nor a disaggregation of the requests by service provider, authority, type or purpose.

- PUBLIC OVERSIGHT: *States must establish independent oversight mechanisms in order to guarantee transparency and accountability in Communications Surveillance.*

Paraguay does not have a mechanism for effective remedy, nor does it have any other independent body that oversees surveillance requests during the criminal process or over the activities of the intelligence agencies. It does not have a law on the protection of personal data *per se* to provide safeguards against human rights abuses from public and private actors. Today, the only legal institution used is *Habeas Data*, which is a constitutional guarantee.

- INTEGRITY OF COMMUNICATIONS AND SYSTEMS: *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.*

It should be noted that Articles 9 and 10 of the Bill on the preservation of traffic data ("Pyrawebs") imposed sanctions on Internet service providers that fail to comply with the obligation to retain traffic data. To that end, the corresponding administrative entity (CONATEL) is empowered to set rules and impose administrative sanctions, in accordance with Law N° 642 on Telecommunications.

However, there are no provisions that establish the necessary guarantees to protect users from information confidentiality abuses or violations in accordance with the State's human rights obligations. Those affected by the illegal use of their personal data or by the violation

of their private communications are exposed to a situation of legal defenselessness, which is incompatible with the obligations of the Republic of Paraguay.

Fortunately, it should be noted, there are no laws or regulations regarding the use of encryption tools or other tools that protect the identity and security of individuals that threaten anonymity.

VII.
Conclusions and Challenges

The surveillance debate in the digital age is becoming more and more important in Paraguay. So is the increasing need for individuals feel as though they can participate and express their views online without feeling threatened or surveilled unfairly. Any type of control of activities on the Internet must be accompanied by public policies and balanced laws that interfere with individuals' private lives so that these occasional invasions are legitimate, proportional, adequate, and necessary.

The framework for the protection of human rights provides strong protection. However, such framework is not specific enough to cover new situations that these evolving technologies present.

On the basis of what has been analyzed and elaborated on in these sections, it can be seen that the Paraguayan legal framework must raise its communications privacy protection standards, strengthen the legal institutions that provide safeguards for such rights, and support a democracy that, although still weak, has been standing for 35 years after a relentless dictatorship.

In the light of the International Principles on the Application of Human Rights to Communications Surveillance, we must express the following:

- It is imperative to strengthen criminal institutions for an improved interpretation of domestic and international laws on communications surveillance given the advance in surveillance techniques and technologies. The jurisprudence of the Supreme Court analyzed in this research shows that there is a need for more knowledge about surveillance techniques and the restriction on the right to private life. The contributions made by international rapporteurs for human rights and the international case law are part of the *acquis communautaire* indispensable for communicating with judges and prosecution officials.

- It is necessary to strengthen the controls conducted on the functioning of intelligence and counterintelligence activities. It is important to begin working side by side with the Human Rights Commissions of the National Congress, the Public Defender's Office, and the Court of Auditors of the Republic—public institutions that have to prioritize their commitments to transparency, access to public information, and defending human rights with the purpose of pointing out their scope in order to conduct adequate and effective control over criminal investigation

activities that involve any type of intrusion into people's privacy lives.

- As for transparency, the State should make public the use and scope of the laws on communications surveillance. 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 investigation authority (security agencies, prosecutors, and judges respectively), type, purpose, and the specific number of individuals affected by each. The Paraguayan State should provide the public with sufficient information to enable citizens to fully comprehend the scope, nature, and application of the laws permitting communications surveillance.

- Article 10 of the law on Electronic Commerce, on the retention of metadata via the Internet with commercial purposes should be modified, as well as the Resolution of CONATEL about the storage of phone calls data, since they do not comply with the principles of proportionality, necessity, adequacy, and due process.

- The National Congress needs to discuss and debate about the international standards on communications surveillance. This discussion should involve citizens and civil society organizations in order to avoid passing bills like the one on mandatory data retention ("Pyrawebs"). Legal frameworks for Safe Internet browsing for the Defense of Children and Adolescents are also needed—ones that exclude disproportionate measures and avoid the unnecessary creation of new crimes that have little capacity to do harm.

- It is essential to protect whistleblowers: The law must recognize the immunity of those who, in good faith, report the law and human rights violations and acts of corruption by those under orders of strict confidentiality. Such immunity should be explicitly recognized in legislation imposing criminal or administrative sanctions on those who fail to comply with their duties of secrecy.

- Those whose communications are being surveilled should be notified—in cases where the law does not require otherwise—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. This shall enable those affected to have knowledge of the content and scope of the invasion of their privacy and, thus, they may be able to exercise their right to access to justice to seek remedies against abuses.

- Technology that has been, or is allegedly being, acquired by the State should ensure adequate protection of personal data. It is also imperative to establish mechanisms for the control, protection, and preservation of the data collected as a result of

legitimate and authorized surveillance measures. Such mechanisms should be under the State's control and responsibility. Moreover, the requisite of proportionality is not fully met, since the legal framework does not impose an obligation to destruct all the material collected by communications interceptions that is not relevant for the investigation.

- The authorities have made no declarations through any of their agencies on the procedures and protocols for employing systems like FinFisher, thus it is important to know the reasons and motives for operating such electronic surveillance systems in the country. The existence of the aforementioned system has neither been officially confirmed nor officially and emphatically denied.

- Due Process: It is crucial to guarantee that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, when debating about the rights of a person, this person is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law.

- It is essential to respect constitutional guarantees but also to publish investigation files in the future, providing for the principle of transparency after having conducted all surveillance procedures.

- Debate and discussion for a new law on personal data: A law on personal data safeguarding individuals' privacy should establish guarantees for the effective protection of personal data, allowing those affected by an abusive surveillance measure to be compensated for their rights that have been violated and to have access to an adequate remedy. It is also necessary to create an independent body for the protection of such guarantees.

- Public Oversight: The Paraguayan State should establish independent oversight mechanisms in order to guarantee transparency and accountability in communications surveillance. Oversight mechanisms should have the authority: to access all potentially relevant information about State actions, including, when appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been comprehensively and accurately publishing information about the use and scope of communications surveillance techniques and powers in accordance with its transparency obligations; to publish periodic reports and other information relevant to communications surveillance; and also to make public statements on the lawfulness of those actions, including the extent to which they comply with these Principles. Independent oversight mechanisms should be established in addition to any oversight already provided within the State.

1 Cortés, Martín. "Paraguay tuvo la dictadura más larga y silenciosa de América Latina" [Paraguay Suffered the Longest, most Muted Dictatorship in Latin America]. Infojus Noticias. March 22, 2014. Available at: http://www.infojusnoticias.gov.ar/entrevistas/paraguay-tuvo-la-dictadura-mas-larga-y-silenciosa-de-america-latina-82.html [Accessed on: July 22, 2015].

2 Jacinto Flecha, Víctor. El descubrimiento del Archivo del Terror en 1992. [The Finding of the Terror Files] Ministry of Culture. May 28, 2011. "Database: records of detainees and individuals held in custody; statements; reports about individuals, social, student and union activities, inspection of people, entry/exit points in borders, collection of pictures of detainees, meetings, fingerprints, etc. Available at: http://www.cultura.gov.py/lang/es-es/2011/05/el-descubrimiento-del-archivo-del-terror-en-1992/ [Accessed on: December 2, 2015].

3 Law N° 5,140/13. Modifying articles 1, 2 and 3 of Law Nº 2,403 "Which creates the National Commission for the Study of the Reform of the Criminal and Penitentiary System."

4 For example, USA Patriot Act of September 26, or the "Law on the Organization of Public Safety," also known as the "Ley Mordaza" [gag rule] in Spain.

5 Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," [No prestes atención al servidor detrás del proxy: continúa proliferación de Mapeo de FinFisher], CitizenLab. October15, 2015. Available at: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/ [Accessed on: December 2, 2015]. Cáceres, Víctor. Los drones llegan a Paraguay. [Drones Enter Paraguay] ABC Color, September 27, 2013. Available a t : http://www.abc.com.py/especiales/fin-de-semana/los-drones-llegan-a-paraguay-622049.html [Accessed on: December 2, 2015]. El Gobierno de Brasil empleará tres UAV para el monitoreo de la triple frontera del Sur [Brazil to Implement Three UAVs to Monitor the tri-border Area]. Infodefensa, November 17, 2011. Available at: http://www.infodefensa.com/es/2011/11/17/noticia-el-gobierno-de-brasil-empleara-tres-uav-para-el-monitoreo-ininterrumpido-de-la-triple-frontera-del-sur-2.html [Accessed on: December 2, 2015]. WikiLeaks, The HackingTeam Archives. Paraguay, Uruguay Report

6 International Principles on the Application of Human Rights to Communications Surveillance. Available at: https://es.necessaryandproportionate.org/text Background and Supporting Legal Analysis https://es.necessaryandproportionate.org/analisislegal Universal Implementation Guide for the International Principles on the Application of Human Rights To Communications Surveillance, https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf [Accessed on: December 2, 2015].

7 *International Principles on the Application of Human Rights to Communications Surveillance* (2014). Available at: https://es.necessaryandproportionate.org/text [Accessed on: December 2, 2015]. See also La Rue Frank, Report of the Special Rapporteur for the promotion and protection of the right to freedom of expression and of opinion, A/HRC/23/40, April 17, 2013, p. 3.

8 The "adequacy test" established by the Inter-American Court of Human Rights in the case of "Almonacid Arellano," which was completed by others, specially by the "Trabajadores cesados del Congreso," demands that national judges deem domestic laws (including the constitution) that are opposed to the American Convention on Human Rights, and to its interpretation by the Inter-American Court) invalid. This is a useful document to build an inter-American *ius commune* for personal and constitutional rights. Its success shall depend on the wisdom of the sentences of the Inter-American Court, and on the national court's will to follow them. (See the Special Report, N° 5/2014, National Mechanism for the Prevention of Torture in Paraguay, available online at: http://:www.mnp.gov.py) The two *leading cases* as regards the adequacy test of the Inter-American Court are the case of "Almonacid Arellano et al. v. Chile," paragraph 124; Case of Gomes Lund et al. (Guerrilha do Araguaia) v. Brazil, paragraph 176, and Case of Furlan and family v. Argentina. Preliminary Exceptions, Merits, Reparations and Costs. Sentence of August 31, 2012. Series C Nº 246, paragraph 302.

9 "The fact that [Uruguay's] Expiry Law of the State has been approved in a democratic regime and yet ratified or supported by the public, on two occasions, namely, through the exercise of direct democracy, does not automatically or by itself grant legitimacy under International Law…". Inter-American Court of Human Rights. Case of Gelman v. Uruguay, Sentence of February 24, 2011, paragraph 238.

10 Thus, in several sentences the Court has established that it is aware that domestic authorities are bound to the sovereignty of the law and that is why they are compelled to apply the provisions in force in the legal order. However, when a State is part of an international treaty like the American Convention, all of its organs, including its judges and the bodies linked to the enforcement of the law at all levels are also subjected to the treaty, which compels them to ensure that the effects of such provisions are not undermined by the application of norms opposed to their objective and aim, so that legal or administrative decisions do not make the full or partial compliance with international obligations illusory. In other words, all State authorities are obliged to conduct on their own initiative an "adequacy test" between domestic law and the American Convention, in the context of their respective competences and the pertaining procedural regulations. In doing so, they should take into account not only the treat but also the interpretation given to it by the Inter-American Court, final interpreter of the American Convention. (Case of Gelman v. Uruguay. Resolution of the Inter-American Court of Human Rights of March 20, 2013. Monitoring compliance with judgment, paragraph 66.)

11 In this investigation, we consider that the right to privacy covers the right to private life and the right to intimacy, the secrecy or inviolability of communications and the protection of personal data, together with the inviolability of the home.

12 See articles 26 and 28 of the Constitution of the Republic of Paraguay.

13 "That regulates private information." Updated on the 1969/02 law. "That modifies, broadens, and repeals various articles of the 1682/2001 law, "which regulates private information."

14 This law defines sensitive data as information relative to race or ethnicity, political preferences, health status, religious, philosophical or moral beliefs, sexual privacy and, in general, all information that might trigger judgmental or discriminatory situations, or that may affect the dignity, privacy, family intimacy and reputation of individuals.

15 See articles 3, 4 and 5 of Law Nº 1682/01.

16 See article 6 of Law Nº 1682/01.

17 "Today, the Senate passed a modified version regulating the disseminations and the treatment of private information (Informconf). The draft goes again to the House of Representatives. The Senate's commission on Legislation modified the bill approved by the House of Representatives and ordered that only those who owe the equivalent of three minimum salaries or more be included in the Informconf system. Moreover, the Senate also approved that people who pay their debt be taken out of such system within the following 24 hours (…) The draft was sent back to the Representatives, who must ratify or approve the Senate's version in order to be adopted in Congress. See: ABC Color Newspaper, May 19, 2015, p. 8.

18 File N: 561, page 174, year 1992: writ of *habeas data* in favor of Martín Almada, Criminal Court 3, Judge José Agustín Fernández.

19 "On September 14 of 1992, at 8:10, PhD. Martín Almada has submitted before this trial court nº 3 a request for *habeas data*, under the aegis of Attorney Pedro Darío Portillo and Attorney Rodolfo Aseretto." Justice Museum – Judicial Branch. Available at: http://www.pj.gov.py/contenido/132-museo-de-la-justicia/132 [Accessed on: December 3, 2015].

20 Mir Puig, Santiago. General Criminal Law [Derecho Penal Parte General], Barcelona Publishing House Tecfoto, 1996, p. 90: "A second principle deriving from the limitation of criminal law to what is strictly necessary is the premise of the «piecemeal character of Criminal law». This means that Criminal law must not criminalize all misdemeanors in relation to the rights it protects, but only the attacks that are more dangerous to them."

21 Mir Puig, Santiago. *Op. Cit.* P. 89: "In order to protect social interests, the State must first exhaust all less harmful means before turning to criminal law, which, in this sense, is a subsidiary weapon, an *ultima ratio*." García Ramírez, Sergio. Op. Cit. "...criminal law must be the *ultima ratio legis*." Milanese, Pablo. Modern Criminal Law and the Collapse of the Principle of Minimum Intervention. [El Moderno Derecho Penal y la Quiebra del Principio de Intervención Mínima.] www.derechopenalonline.com/febrero2004/milaneseintervencion.htm: "Subsidiarity consists in resorting to criminal law as a way of social control, only in the cases in which other less harmful controls are insufficient, that is to say, «when the other barriers protecting legal rights given by other branches of law fail.»

22 Ferrajoli, Luigi. Minimum Criminal Law and Fundamental Legal Rights [Derecho Penal Mínimo y Bienes Jurídicos Fundamentales]. http://www.corteidh.or.cr/tablas/r16993.pdf [Accessed on: December 2, 2015].

23 Human Rights Council. Ibid., paragraph 81.

24 See article 144.

25 By which the regulations of Law № 642/95 "Of Telecommunications" were passed.

26 National Commission on Telecommunications (CONATEL). RESOLUTION № 1350/2002.- Which establishes the obligation to register the details of calls for six months. Available at: http://www.buscoley.com/pdfs/r_1350_2002.pdf [Accessed on: December 3, 2015].

27 Última Hora. Cases of Kidnapping in Paraguay [Los casos de secuestros en Paraguay]. Available at: http://www.ultimahora.com/los-casos-secuestros-paraguay-n460811.html [Accessed on: December 28, 2015].

28 "The minimum criminal law represents the reduction to a minimum of criminal circumstances and their general regulation through the legalization of all behaviors that do not affect fundamental rights and overfill the judicial area with useless and innocuous punishment, which is a scarce and expensive resource, and have the threefold effect related to the general weakening of safeguards, the inefficiency of the judicial machinery, and the devaluation of the legal rights worthy of criminal protection." Ferrajoli, Luigi. Crises in the Political System and Jurisdiction: the Nature of the Italian Crisis and the Role of the Judiciary [Crisis del sistema político y jurisdicción: la naturaleza de la crisis italiana y el rol de la magistratura]. Magazine Punishment and State [Pena y Estado] year 1 issue 1–Argentina 1995: Publishing House: Editores del Puerto s.r.l. p. 113.

29 Law № 1881 modifying Law № 1340 of November 22, 1988 "which combats the illegal trafficking of narcotics and dangerous drugs and similar crimes, and establishes preventive and rehabilitation measure for addicts."

30 In this regard, it must be taken into account article 172 of the Constitution: "Public Force is exclusively made up of military and police forces".

31 Law 4868/13 on Electronic Commerce. Available at: http://www.eljurista.com.py/admin/publics/upload/archivos/ea41b40fb8ce27bd7ec64237fd75ef89.pdf [Accessed on: December 2, 2015].

32 Pyrawebs, Tedic. Available at: http://pyrawebs.tedic.org/ [Accessed on: December 2, 2015].

33 Bill presented by senators Fernando Silva Facetti, Enrique Bacchetta and Roberto Acevedo on October 2, 2013.

34 Law 1340 of November 22, 1988 "which combats the illegal trafficking of narcotics and dangerous drugs and similar crimes, and establishes preventive and rehabilitation measure for addicts" and its modifications.

35 Law 2,422/04, Customs Code.

36 Law 4036/10 on Firearms, their parts, ammunitions, explosives, accessories and the like.

37 The provisions in Law 4024/10, which criminalizes punishable acts of terrorism, terrorist associations and the financing of terrorism.

38 The provisions in Law 4439/11, which modifies and expands several articles of Law 1160/97 of the Criminal Code and Law 3440/08, which modifies several provisions in Law N° 1160/97, Criminal Code.

39 Article 6.

40 SILpy - System of Legislative Information. Bill: OF THE PROTECTION OF CHILDREN AND ADOLESCENTS AGAINST HARMFUL CONTENT ON THE INTERNET. Available at: http://sil2py.senado.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F103933 [Accessed on: December 3, 2015].

41 National Commission on Telecommunications (CONATEL). RESOLUTION FOLDER W 190/2009 WHICH ESTABLISHES THE REGULATIONS OF INTERNET ACCESS SERVICES, DATA TRANSMISSION. Available at: http://www.conatel.gov.py/files/marcoregulatorio/resoluciones/RD_190_2009_-_INTERNET_RES_DIR_CON_ANEXO.pdf [Accessed on: December 3, 2015].

42 Agreement and Sentence Nº 674/10 "Extraordinary Petition of Cassation Filed by Ombudsman Sandra Rodríguez Samudio in the Case of Anastacio Mieres Burgos et al." File N° 773, page 245.

43 ABC Color. Special Case of Cecilia Cubas. Available at: http://www.abc.com.py/multimedia/caso-cecilia-cubas/ [Accessed on: December 2, 2015].

44 Supreme Court of Justice. Criminal Court: Criminal Matters. Inviolability of Private Communications. Evidence. Means of Proof. Evidence of Legal Experts. Cross-Referencing of Calls. Agreement and Sentence N° 711 Del 20/08/14.

45 https://web.archive.org/web/20140527113509/http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

46 Public Tender of Purchase of Equipment and Peripherals for the Internal Security of the Ministry of Interior (National Police) Page 10 https://www.contrataciones.gov.py/sicp/download/getFile?cid=45685&fileName=OAwkXiYNi6QOh%2BTIKqR3782C1d%2Fp2D6FjIiEs6npdi%2F1ZqqfT7VKyeTQxatNaWt5IxSb9jusPNXO1wj6SydKziVsfoYTRYq%2BBaCsYn4it67q6WhpQnEfFfcXrCqQvEbOmkkgUBngwr4ij3Ea4EbM7A%3D%3D [Accessed on: December 2, 2015].

47 http://www.agendalegislativa.com.py/senado/5922-senado-pide-informe-al-ministerio-del-interior-sobre-equipos-de-escuchas-telefonicas [Accessed on: December 2, 2015].

48 Wikileaks https://wikileaks.org/plusd/cables/10ASUNCION97_a.html [Accessed on: December 2, 2015].

49 Report by Channel 4 Telefuturo: Wiretaps with no Judicial Authorization will Take Place in Cases of Extortion and Kidnapping [Escuchas telefónicas sin orden judicial se darán en caso de extorsión y secuestro] – November 26, 2014 https://www.youtube.com/watch?v=3Bkdspxhae8 [Accessed on: December 2, 2015].

50 The Hacking Suite for Governmental Interception. Available at: http://www.hackingteam.it/ [Accessed on: December 3, 2015].

51 WikiLeaks - The Hacking Team Archives. Paraguay - Uruguay Report. Available at: https://wikileaks.org/hackingteam/emails/emailid/249535 [Accessed on: December 3, 2015].

52 Privacy International. Briefing for the Italian Government on Hacking Team's surveillance [Informe para el Gobierno italiano sobre la vigilancia de Hacking Team]. Available at: https://www.privacyinternational.org/sites/default/files/Briefing%20for%20the%20Italian%20Government%20on%20Hacking%20Team's%20surveillance%20exports.pdf [Accessed on: December 3, 2015].

53 Government Negotiated Espionage [Gobierno negoció espionaje]. ABC Color. July 9, 2015. Available at: http://www.abc.com.py/nacionales/estado-negocio-espionaje-1385872.html [Accessed on: December 2, 2015].

54 https://citizenlab.org/ [Accessed on: December 2, 2015].

55 Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," [No prestes atención al servidor detrás del proxy: continúa proliferación de Mapeo de FinFisher], Citizen Lab. October 15, 2015. Available at: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

56 Information may be obtained through the following means: "1) The interception of telephone, computer and radio communications and of correspondence in any of its forms; 2) The interception of computer systems and networks; 3) Wiretaps and audiovisual electronic recordings; and, 4) The interception of any technological system for the transmission, storage or processing of communications and information." Article 25 of Law N° 5241/14, which creates the SINAI.

57 International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/text [Accessed on: December 2, 2015]. EFF, ARTICLE19, Background and Supporting Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/AnalisisLegal; [Accessed on: December 2, 2015], Access, Universal Implementation Guide on the International Principles on the Application of Human Rights to Communications Surveillance, available at: https://eff.org/r.4gac [Accessed on: July 20, 2015].

58 International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/text [Accessed on: December 2, 2015].; EFF, ARTICLE19, Background and Supporting Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/AnalisisLegal; [Accessed on: December 2, 2015], Access, Universal Implementation Guide on the International Principles on the Application of Human Rights to Communications Surveillance, available at: https://eff.org/r.4gac [Accessed on: July 20, 2015].