Examining Internet Freedom in Latin America (EXLILA)

Country report: Paraguay

Maricarmen Sequera Buzarquis

TEDIC

Association for Progressive Communications (APC)
March 2016

This report was produced as part of the APC project Examining Internet Freedom in Latin America (EXLILA). The project is funded by the Open Society Institute (OSI) and APC and coordinated by Derechos Digitales.

Table of contents

1. Executive summary

Paraguay experienced state and private surveillance during the military dictatorship of Alfredo Stroessner (1954-1989).[1] However, the democratic period is not exempt from similar practices or new forms of abusive intrusion into the lives of citizens.

This report analyses surveillance and violations of basic rights that continue in this democratic period in Paraguay, in other forms including surveillance using the internet. It also documents the heightening of some processes such as tougher penalties, penalisation of new behaviours, restrictions on the right to a defence, lack of effective judicial guarantees, massive intrusion into people's private lives, and increased powers for the main actors in the criminal system. This is part of a global trend that may be called "neopunitivism" to mitigate unsustainable situations.[2] Neopunitivism in turn leads to legislative changes that violate constitutional and international law principles and regulations of human rights and criminal and procedural rights.

Technology is expanding in Paraguay. Thirty percent of the population has some form of connection to the internet. But the expansion and connectivity plans of private companies are not matched by national telecommunications policies, which are backward in terms of regulations and the application of policies on the internet that do not take human rights into account.

On the other hand, basic rights are strengthened by constitutional laws, ratifications of international treaties and administrative regulations on human rights that fulfil an important role for the foundations of a democratic system. There is no doubt that Paraguay meets the minimum standards for the defence of basic rights. But there are vacuums or failures in compliance with due process, notification of the parties, and understanding that the same limits on invading people's privacy must be transferred to the internet. Today, as throughout the region, citizens run a high risk of infringement of their rights to freedom of expression on the internet and to privacy, resulting in the weakening of the democratic system.

2. Introduction

The rights to privacy, freedom of expression and access to information and knowledge are essential for human dignity and for a democratic society. However, these rights are under threat from public and private actors who seek to take advantage of the possibilities of interfering in people's private lives, blocking content and censorship by means of technological advances.

At present, high speed (broadband) internet reaches Paraguayan municipalities by means of mobile networks, whereas wired technologies in the home have very low coverage. In terms of internet use, the penetration rate, understood as "the number of persons with access within a country," is approximately 30%.[3] Only 5% of households have a fixed internet connection.[4] However, 25% have access through mobile phones.[5] Internet over mobile phones has wide coverage with 2G/3G/4G networks, although 4G is

[1] https://en.wikipedia.org/wiki/Alfredo_Stroessner

[2] For example, guerrillas in Paraguay. Paraguayan People's Army (EPP - Ejército del Pueblo Paraguayo). https://en.wikipedia.org/wiki/Paraguayan_People%27s_Army

[3] World Bank. World Development Indicators (2009-2013).

[4] World Bank. Fixed broadband subscriptions (per 100 people), 2013. http://data.worldbank.org/indicator/IT.NET.BBND.P2

[5] World Bank. Mobile cellular subscriptions (per 100 people), 2014. http://data.worldbank.org/indicator/IT.CEL.SETS.P2

still very limited. According to the National Telecommunications Commission (CONATEL), at the end of 2014 there were 252,118 subscribers to mobile internet and 185,125 subscribers to fixed internet in Paraguay, totalling 437,243 subscribers in a population of 6,802,295.[6]

More and more countries in the world have increasing technological capabilities to carry out simultaneous, invasive, focused and large-scale surveillance and interception of communications.[7] Ever since Edward Snowden revealed the existence of national and international programmes directed by the National Security Agency (NSA) of the United States, devoted to the mass surveillance of the private communications of millions of internet users, there has been public debate about the context and limits of valid systematic monitoring by states. In some cases this surveillance has been incited by the discourse of the doctrine of national security, clashing with the international human rights system.[8] An example of this is Paraguayan government campaigns that ultimately silence, repress and surveil everybody, in the name of the fight against drug trafficking or terrorism.[9]

Another threat to the rights of access to information and knowledge is the latest amendment of law 1328/98 on copyright in Paraguay.[10] The amendment increased the private monopoly of related rights over a work from 50 to 70 years after they become due.[11] These protectionist policies in the cultural industry are deeply harmful, limiting people's creative capacities and infringing their right of access to knowledge and culture.[12]

While the prosecution of punishable offences and national security are legitimate aims, it is important that they be limited to what is established in the constitution, which is the social compact par excellence and the democratic guarantee that limits the interference of the state into the private lives of individuals. In addition, the international human rights system provides standards and principles to prevent risks and abuses of these fundamental rights.

Paraguay has constitutional protections and ratifications of international human rights conventions. However, this does not guarantee adequate safeguards when the state expands the technology of its communications surveillance. Absence of regulations in this area does not constitute an attack on human rights *per se*, but it hampers accountability and social control of state surveillance through telecommunications. Some of the laws that reinforce the doctrine of national security and violate the human rights system are already in force, while others are being considered in the National Congress.

---

[6]CONATEL. Suscriptores de internet móvil y fijo (2010-2014). www.conatel.gov.py/images/2015-2/PNT/DESARROLLO/midt%202014.pdf

[7]La Rue, F. (2013, 17 abril). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations, A/HRC/23/40, para. 33. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[8]For example, the USA Patriot Act of October 26, 2001, or the Citizens Security Law in Spain, better known as the "gag law", to give only two examples.

[9]Polischuk, S. (2015, 9 March). Otro periodista asesinado en Paraguay mientras aumenta la vigilancia estatal. *Resumen Latinoamericano.* www.resumenlatinoamericano.org/2015/03/09/otro-periodista-asesinado-en-paraguay-mientras-aumenta-la-vigilancia-estatal

[10]sil2py.senado.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F1406

[11]Sequera Buzarquis, M. (2013, 5 December). ¿70 años de derechos conexos? No, gracias. *Tedic*. www.tedic.org/70-anos-de-derechos-conexos-no-gracias

[12]The main harm caused by increasing related rights by a further 20 years is the loss of access to countless books, periodicals, leaflets, photographs, films, recordings and other works that are "property" and are generally no longer commercialised. They thus become forgotten and possibly lost forever. Extended terms are also expensive for consumers and performers, while the beneficiaries are the owners of companies holding the related rights, who very probably had nothing to do with the original creation of the work.

In spite of the above, there are important examples of resistance to human rights violations and strengthening of constitutional guarantees in Paraguay. One example was the rejection and shelving in July 2015 of a bill to establish the obligation to retain traffic data[13] on the part of internet providers. This was a political victory for the country's citizens[14] who analysed, discussed and pressured the authorities to reject a bill that endangered the right to privacy of the entire population.

The Law on Access to Public Information[15] has also entered into force through its regulatory decree.[16] This is an opportunity for citizens to demand accountability on the government's activities – especially those that violate fundamental rights – and the free exercise of communications, democratic guarantees that are supported by the constitution.

3. General regulatory framework and most important internet regulations in the country

The highest law in the Paraguayan legal system is the Constitution. Article 137 defines the following ranking order for laws: "international treaties, conventions and agreements that have been approved and ratified, laws enacted by Congress and other legal provisions of a lower order, in the stated order of precedence." This means that human rights treaties and conventions are above national laws that may be less favourable for citizens.

3.1. National Constitution

Article 33 of the Constitution, on the right to intimacy, says:

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

The same article reinforces the other human rights enshrined in the Constitution: freedom of expression and of the press, the right of access to public information, and freedom of assembly and manifestation.[17]

The privacy of communications is protected by Article 36 of the Constitution on the right to the inviolability of documentary assets and of private communication:

> The documentary assets of persons are inviolable. Records, regardless of the technique used, printed matter, correspondence, writings, telephonic, telegraphic or any other kind of communications, collections or reproductions, testimonies and objects of testimonial value, as well as their respective copies, may not be examined, reproduced, intercepted or seized

[13]Sistema de Información Legislativa: Proyecto de ley de retención de datos de tráfico. sil2py.senado.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F102821

[14]Campaña Pyrawebs: www.pyrawebs.tedic.org

[15]Ley No. 5282 de libre acceso ciudadano a la información pública y transparencia gubernamental (2014). www.hacienda.gov.py/web-hacienda/archivos_de_disenho/imagenes/images/ley%205282.pdf

[16]Decreto No. 4064 por el cual se reglamenta la Ley No. 5282/2014 "de libre acceso ciudadano a la información pública y transparencia gubernamental" (2015). www.idea.org.py/v1/wp-content/uploads/2015/09/DECRETO-4064-14.pdf

[17]National Constitution, Articles 26, 28, 29, 32. jme.gov.py/transito/leyes/1992.html

except by a judicial order for cases specifically specified in the law, and when they would be indispensable for clearing up 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. Documentary evidence obtained in violation of that prescribed above lacks validity in trial. In every case, strict confidentiality will be observed regarding that which is not related to the subject of investigation.

In this way the Constitution determines that state intervention can only occur by means of a judicial order.[18]

The first right to be compromised by surveillance of internet communications by the authorities is the right to privacy. This includes the right of all persons to the protection of personal information, which must not be accessed, searched or altered by third parties without authorisation. Therefore, when an authority carries out activities intended to search, interfere with or access a person's communications, it must be an exceptional event and have previous judicial authorisation.

3.2. International laws

Article 12 of the Universal Declaration of Human Rights says that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, and that everyone has the right to the protection of the law against such interference or attacks.[19]

Correspondingly, the right to privacy is also recognised in Article 11 of the American Convention on Human Rights[20] and Article 17 of the International Covenant on Civil and Political Rights.[21]

3.3. National laws

The Paraguayan Congress has adopted other laws to protect personal data, including Law 1682/01, which was later modified by Law 1962/02.[22] This law on personal data has serious shortcomings that include vague and imprecise concepts about the definition of sensitive data. Its scope is also unsatisfactory, as it does not apply to public and/or private data banks. Neither does it create an authority responsible for data protection. All this means that every individual must present a unilateral action of *habeas data* for

[18]See, for example, the action for unconstitutionality in the trial of Juan Claudio Gaona Cáceres and Ruben Melgarejo Lanzoni on bribery, intent to extort, aggravated passive bribery. Year 2008-No.799-Constitutional Chamber of the Supreme Court. "In regard to interception of communications authorised by a judicial resolution, there should be no confusion between the different scope of violation of constitutional rights and the offence; without prejudice to the possible purpose of proving a charge as a source of investigation, it may violate constitutional legality thus becoming inadmissible with all the subsequent effects."
www.csj.gov.py/jurisprudencia/cache/25c136e078225ec4be3ff3ec67d4b407.htm

[19]Universal Declaration of Human Rights. www.un.org/en/universal-declaration-human-rights

[20]American Convention on Human Rights. www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm

[21]International Covenant on Civil and Political Rights. www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[22]The first article says: "The purpose of this law is to regulate the collection, storage, publication, alteration, destruction, duration and in general the processing of personal data contained in files, records, databanks or any other technical means of processing public or private data intended to be reported, in order to guarantee the full exercise of the rights of its owners. This Law will not in any case be applied to journalistic databases or information sources nor to the freedom of opinion and information." In other words, publication or dissemination of "sensitive" personal data is prohibited, while it is lawful to collect, store, process and publish personal data or characteristics for scientific, statistical, surveying, polling or market research purposes. A bill to modify articles 5 and 9 is being debated in the National Congress. La Nación. (2015, 18 August). Diputados ratifican sanción a Ley de Informconf. *La Nación.* www.lanacion.com.py/2015/08/18/diputados-ratifican-sancion-a-ley-de-informconf

every case of violation of the law. There are also flaws in the protection of sensitive data like "medical conditions," as there is no penalty whatsoever for violations in handling information on personal health. Penalties are only provided for cases of violations of data on economic and financial solvency.

A recent example of flagrant violation of confidentiality and patient privacy was the case of the pregnancy of a 10-year-old girl in Paraguay in May 2015.[23] Her health status was public knowledge from the time the case became known until her delivery. In addition, several United Nations treaty organisations, such as the Committee for the Elimination of Discrimination against Women (CEDAW) have shown concern about cases of women admitted to hospital with complications of abortion.[24] In these cases the personal data of the women having the abortions have been made public.

Habeas data is one of the constitutional guarantees (Article 133 of the Constitution). The most emblematic case of *habeas data* was the lawsuit brought in 1992 by Martín Almada,[25] who under *habeas data* was able to unearth the secret archives of the police during the military dictatorship of Alfredo Stroessner (1954-1989), known as the "Archives of Terror".[26] At present, recourse may be had to *habeas data* before the judge of first instance.

Furthermore, Chapter VII of the Criminal Code on punishable offences against the private life and intimacy of individuals establishes other penalties for various offences including: violation of the home (Article 141), trespassing (Article 142), infringement of a person's privacy (Article 143), infringement of the right to communication and image (Article 144), violation of confidentiality (Article 145), violation of the secrecy of communications (Article 146), disclosure of the private secrets of a person with a special duty to maintain secrecy due to his profession (Articles 147 and 148), and disclosure of private secrets for economic gain (Article 149).

The Code of Criminal Procedure describes the mechanisms and rules required to prosecute offences. Articles 198 and 199 grant permission, with a judicial order, to intercept and seize correspondence, telegraphic or any other kind of correspondence. Article 200 provides for the possibility of surveillance of communications under exceptional circumstances, and establishes that a judge may order the interception of communications of persons accused of offences, using any technical means necessary to obtain the information required for the investigation. But the limits of what kind of technology should be used, or how excessive its use may be, are not clear, disproportionately affecting a number of fundamental rights of the suspected individual.

The Specialised Unit for Cyber Crime – which tried to purchase surveillance software from the Italian firm Hacking Team – according to Resolutions No. 3459/10 and 4408/11 has the power to ask a judge for interception of communications in the investigation of certain specific crimes, such as unlawful access to

[23]ABC. (2015, 18 August). Niña dará a luz mañana. *ABC.* www.abc.com.py/nacionales/nina-dara-a-luz-manana-1396977.html

[24]Committee on the Elimination of Discrimination against Women (2011, 8 November). Concluding observations of the Committee on the Elimination of Discrimination against Women – Paraguay. CEDAW/C/PRY/CO/6. http://www.refworld.org/publisher,CEDAW,CONCOBSERVATIONS,,4eea26a42,0.html

[25]On 14 September 1992, at 08:10 hours, at the Criminal Court of First Instance, an application of *habeas data* was presented by Dr. Martín Almada, sponsored by lawyers Pedro Darío Portillo and Rodolfo Aseretto. www.pj.gov.py/contenido/132-museo-de-la-justicia/132

[26]The "Archives of Terror" of Operation Condor record the operations of Stroessner's secret police over decades. They contain information about the coordination of operations with neighbouring dictatorships, especially Chile and Argentina. This discovery showed that Stroessner's surveillance methods were still in use even after his overthrow in 1989.

data, interception, preparation for unlawful access to data, modification of data or computer systems, sabotage of computer systems, card forgery, and others.

The Public Ministry, in general, may have access to the intercepted communications once the judge has given the relevant authorisation. Article 89 of the Telecommunications Law 642/95 establishes the protection and inviolability of telecommunications services except when there is a judicial order from the competent judge.[27] Article 90 reinforces the meaning of inviolability, which is broken when a person who is not the original recipient of the communication has knowledge of the existence or content of the communication and has the opportunity of extracting, interfering, altering the content or itinerary, publishing or using this information. Executive Decree 14135/96 complements this law through its Article 9 on inviolability and secrecy of telecommunications.[28]

The principle of "net neutrality" is a relevant component in exercising freedom of expression and privacy on the internet. Resolution 190/2009[29] of Paraguay's National Telecommunications Commission (CONATEL) establishes the protection of this principle in Article 26: "The provider supplying the service shall abide by the principle of network neutrality; it shall not be entitled to interfere with or degrade traffic received or generated by the user, nor change the contracted capacity according to the user's choice of type of content, application, origin or destination." However, punitive and administrative sanctions in the event of non-compliance are not envisaged. Increased awareness of this principle among citizens has led to complaints being raised against providers not complying with this principle and the relevant article in the resolution. An emblematic case of infringement of the neutrality principle was the blocking of the satirical site ABC.me by an internet service provider for private reasons,[30] showing that abusive behaviour is not only perpetrated by states. Whereas the regulations are established in a resolution, the current proposal for amending the Law of Telecommunications seeks for it to be passed as a law. Unfortunately, the proposal does not include restriction or exclusion penalties providing for imprisonment or fines in the event of infringement of this principle.

It is worth noting that not all CONATEL regulations comply with human rights standards, and that in some cases they contradict the Constitution or international treaties. For example, CONATEL regulation 1350/2002[31] poses a risk to personal communications as it stipulates in Article 1 "the term of six (6) months, as the compulsory period for retaining records of details of all inward and outward calls for all lines comprising the client portfolio of different operators of the cellular mobile telephony service and/or

[27]See Article 89 of the Law on Telecommunications 642/95.

[28]Article 9 says: "The inviolability and the secrecy of telecommunications are breached when a person who is not the originator or the recipient of the communication deliberately extracts, intercepts, interferes with, changes or alters the text, changes the itinerary, publishes, uses, tries to know or enables another person to know the existence or content of any communication. Persons who by reason of their official role have knowledge or access to the content of a communication sent through the telecommunications services, are obliged to preserve and guarantee its inviolability and secrecy. Concessionaires or licensees and those authorised to provide or use telecommunications services, are obliged to adopt appropriate measures to guarantee the inviolability and secrecy of communications made through these services."

[29]Comisión Nacional de Telecomunicaciones. (2011). Resolución Directorio W 190/2009, Reglamento de los servicios de acceso a internet, transmisión de datos. https://webcache.googleusercontent.com/search?q=cache:q5EXMXB7Lp8J:docs.paraguay.justia.com/nacionales/leyes/resolucion-n-190-del-11-de-marzo-de-2009-por-la-cual-se-establece-el-reglamento-de-los-servicios-de-acceso-a-internet-transmision.doc+&cd=5&hl=es&

[30]Satirical webcsite ABC.me parodied the media outlet ABC, which led to the blocking of the website for four hours by local ISPs. Another notorious protest was that against the blocking of Whatsapp calls. Both cases obliged CONATEL to take a position. For more information, see: www.tedic.org/las-continuas-violaciones-a-la-neutralidad-de-la-red-en-paraguay

[31]Comisión Nacional de Telecomunicaciones (CONATEL). (2002, 6 November). Resolución No. 1350/2002. www.buscoley.com/pdfs/r_1350_2002.pdf

personal communication service". It does not envision any administrative or restrictive penalties or fines in the event of public or private disclosure of the content of these signals.

Another regulation posing a risk to communications privacy and clashing with the Constitution is Law 4868/13 on Electronic Commerce; Article 10[32] binds internet service providers and web hosting service providers in Paraguay to store traffic data or "electronic communications" data for a period of six months. This law does not meet minimum requirements for safeguarding user information privacy, nor does it provide clear criteria to enable the distinction between data that can and cannot be stored. It may be noted that Article 10 prohibits the judicial branch and the National Police from accessing the data stored by the companies.

Since 2014 Paraguay has had a National Intelligence System, created by President Horacio Cartes by Presidential Decree No. 2812 of 18 December 2014,[33] which regulates Law No. 5241 dated 22 August. In Article 14 of this law and Article 12 of the decree only the National Intelligence System (SINAI) is empowered to "collect and process" data with the aim of safeguarding national security.

However, Article 24 of the same decree provides that the General Intelligence Directorate is also responsible for the collection and handling of data for the generation of intelligence. It is rather striking that no mention is made in Law 5241/2014 of any such Directorate, nor of its activities and powers.

Although the law provides that communications surveillance will only be carried out under exceptional circumstances – i.e., if it cannot be obtained elsewhere by virtue of Article 24, and under judicial authorisation by virtue of Article 26 – the following areas are causes for concern due to the need to guarantee the application of human rights regulations to the communications surveillance carried out by these intelligence agencies. In any case, it is not legitimate to justify communications surveillance as "collection of intelligence" since the wording of the regulation does not define what is meant by "intelligence" or how disproportionate this surveillance can be, in such a way that it can affect those who make things difficult for the current government, such as its opponents, journalists and activists, among others.[34]

The law provides that intelligence will be comprised within the SINAI and used to prevent, warn about and inform of any threats or risks that affect national interests (Article 2a). This is a very broad definition that does not restrict the purpose and objective of communications surveillance and opens the door to different types of abuse.

Article 4 describes the principles according to which SINAI, including its component bodies and individuals, must request judicial authorisation to collect personal data. However, the article also stipulates those cases in which such judicial authorisation will not be necessary, namely: cases of "serious" threat, or those that jeopardise collective security, or the safety of authorities and institutions, or those that damage public security and the rule of law. Since no definition is provided as to what is meant by "serious", this paves the way for legally eluding the requirement of a judicial authorisation.

---

[32] www.eljurista.com.py/admin/publics/upload/archivos/ea41b40fb8ce27bd7ec64237fd75ef89.pdf

[33] www.presidencia.gov.py/archivos/documentos/DECRETO2812_uegnk41y.pdf

[34] United Nations General Assembly. (2014, 21 January). Resolution adopted by the General Assembly on 18 December 2013 [on the report of the Third Committee (A/68/456/Add.2)] 68/167. The right to privacy in the digital age. A/RES/68/167. www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=http://www.un.org/depts/dhl/resguide/r68_resolutions_table_en.htm&Lang=E

Another opportunity for the violation of communications is provided by Law 1881, which modifies Law No. 1340 of 22 November 1988 "which represses illicit traffic of narcotics and dangerous drugs, and related crimes, and provides measures for the prevention and rehabilitation of drug-dependent individuals." This law entitles the National Anti-Drug Secretariat (SENAD) to intercept, search and record oral, cable or electronic communications at the request of a judge, which the judge will be able to authorise in each case and for a certain period.

There are also problems related to intellectual property. Article 184 of the Criminal Code, Law No. 1160/97,[35] states that copyright violation will be punishable by up to three years imprisonment or a fine for persons who without authorisation of the owner disclose, promote, reproduce or publicly perform a work protected by copyright. This law is applied in the online environment with all the complexity implied, such as the method of obtaining information through prior surveillance: the IP of the unlawful download or seizure of the computer or mobile phone, which disproportionately violates fundamental rights.

3.4. Draft bills that may affect fundamental rights on the internet

There are two draft bills that may affect fundamental rights on the internet that are currently being studied by the National Congress. The Bill on Protection of Children and Adolescents against Harmful Content on the Internet[36] is intended to regulate filtering of internet content on public wireless networks and also at the level of internet service providers.[37]

For its part, the Bill on Organised Crime provides unusual powers to state agencies in charge of this sort of investigation. According to jurist Jorge Rolón Luna,[38] who analysed this bill, the offences to which these special investigative techniques will be applied are clearly established: there is a fairly long list including 17 criminal offences in the Criminal Code. It will be applied in conjunction with other "special" laws, such as: the fight against drug trafficking,[39] human trafficking as provided in the Customs Code,[40] the Law on Firearms,[41] the Anti-Terrorist Law[42] and other criminal laws. [43]

As part of the investigation of these offences, "electronic surveillance" may be carried out, defined as follows:

> Electronic surveillance is a special investigative technique that allows utilisation of all technological and/or electronic means known or to be discovered, that lead to obtaining

[35] www.mre.gov.py/v1/Adjuntos/Privacidad/Ley1160.pdf

[36] sil2py.senado.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F103933

[37] Article 3, on active protection: "Internet service providers (ISPs) must provide and install compulsorily and free of charge to their clients and users, who must at the time of contracting the service or at any later time declare whether children or adolescents will have access to the internet, or to anyone requesting it, specific software with systems of detection, filtering, classification, elimination and blocking of harmful contents in compliance with Article 2, with the corresponding manuals and instructions for use."

[38] Jorge Rolón Luna, jurist, former judge (1996-2002) and former commissioner of the National Preventive Mechanism against Torture in Paraguay (2012-2015).

[39] Law 1340 of 22 November 1988

[40] Law 2422/04.

[41] Law 4036/10.

[42] Provisions in Law 4024/10 that punish offences of terrorism, terrorist association and financing of terrorism.

[43] Law 4439/11 modifying and amplifying various articles of Law 1160/97, Criminal Code, and Law 3440/08 modifying several provisions of Law 1160/97, Criminal Code.

information and evidence regarding the committing of the offence under investigation or that lead to identification of the perpetrators and participants.

4. Problematic cases

At present there is no jurisprudence covering fundamental rights in the online environment such as explicit prohibition of the use of encryption or anonymisation that directly affects free expression. However, there is information about the purchase of different technologies for the interception of communications, including networks and the internet. This affects not only privacy, but also the right to freedom of opinion and freedom of association, generating an indirect intrusion into a person's individuality. One of the cases mentioned above that undermined the principle of internet neutrality was that of two service provider companies – Personal and Tigo – that arbitrarily blocked access to the satirical site ABColor.me in 2012. Corporate censorship can be as pernicious as state censorship, and in some cases more powerful. In this case there was no pronouncement or penalty imposed by CONATEL, the telecommunications regulator. However, the citizens voiced their protest and the blocking was reversed within a few hours.[44]

Another attack on net neutrality has been carried out since 2013 by the ISP Tigo, which offers its users free access to the social network Facebook.[45] This fact has been positively highlighted by Mark Zuckerberg in various public declarations in the context of the project Internet.org.[46] Although the alliance between Tigo and Facebook undermines net neutrality and has the same disadvantages as the Internet.org project itself, CONATEL has made no declaration about it, although it did so in the case of the blocking of WhatsApp calls.[47]

The purchase of security software by the state is another problematic case. The Ministry of the Interior's public call to tender for the purchase[48] did not describe the special characteristics of the software in the procurement documents for reasons of confidentiality. The National Congress has requested information about it but the reply is not yet known.[49] Telephone tapping without a judicial order also occurs in the country, although, according to a representative of the Ministry of the Interior, it will be used only and exclusively for cases of extortion and kidnapping. [50]

---

[44] www.tedic.org/roben-este-post-neutralidad-en-la-red

[45] ABC. (2013, 4 December). Facebook móvil gratis para clients de Tigo. *ABC.* www.abc.com.py/abc-tv/locales/facebook-movil-gratis-para-clientes-de-tigo-646280.html

[46] ABC. (2014, 25 February). Zuckerberg destaca ejemplo de Paraguay. *ABC.* www.abc.com.py/ciencia/zuckerberg-destaca-ejemplo-de-paraguay-1218676.html

[47] Sequera Buzarquis, M. (2014, 21 January). ¿Tigo y Personal atentan la Neutralidad en la Red? [Derechos Digitales]. *Tedic.* www.tedic.org/tigo-y-personal-atentan-la-neutralidad-en-la-red-derechos-digitales

[48] Licitación pública nacional No. 17/2013 "Adquisición de equipamientos y periféricos para la seguridad interna plurianual" (Policía Nacional). *Página 10.* www.contrataciones.gov.py/sicp/download/getFile?cid=45685&fileName=OAwkXiYNi6QOh%2BTIKqR3782C1d%2Fp2D6FjIiEs6npdi%2F1ZqqfT7VKyeTQxatNaWt5IxSb9jusPNXO1wj6SydKziVsfoYTRYq%2BBaCsYn4it67q6WhpQnEfFfcXrCqQvEbOmkkgUBngwr4ij3Ea4EbM7A%3D%3D

[49] www.agendalegislativa.com.py/senado/5922-senado-pide-informe-al-ministerio-del-interior-sobre-equipos-de-escuchas-telefonicas

[50] Telefuturo Paraguay, Informe Canal 4. (2014, 26 November). Escuchas telefónicas sin orden judicial se darán en caso de extorsión y secuestro. www.youtube.com/watch?v=3Bkdspxhae8

A series of publications about the Ministry of the Interior have been leaked by WikiLeaks.[51] They show that during the administration of Fernando Lugo, then Minister Rafael Filizolla held talks with the United States Embassy to explain the government's new interception programme, including mobile phones. The nature of this system is unknown, as is its actual use in the prosecution of punishable offences.

Telephone tapping has been denounced many times to the institutions of criminal prosecution. However, the results of these investigations are also unknown and are all covered in a blanket of silence. The National Congress has been affected by this sort of abuse and is debating the situation in the current term.[52]

The debate on this matter has intensified due to articles in the international press about Paraguayan purchases of technology for mass surveillance through the internet. Conversations held by the cyber crime prosecutor Ariel Martínez with the firm Hacking Team[53] were leaked by WikiLeaks[54] and drew media attention. Hacking Team's star product is software that allows interception of computers, Skype calls, emails, instant messages and passwords, known as called Remote Control System. According to research by Privacy International,[55] the software is capable of breaking encryption of communication programmes and recording calls, and viewing web browser history as well as deleted files and photos. It is also able to take control of microphones and cameras and use them for spying. Fortunately, the purchase did not go through.[56]

Another case of purchase of surveillance technology was that of FinFisher.[57] This case was made public by The Citizen Lab – a multidisciplinary laboratory at the University of Toronto – which identified FinFisher users.[58] The report cites Paraguay as one of the countries that have purchased this software, and explains that it works like the Hacking Team product. The investigation did not discover which institution is handling this surveillance tool. However, the Cyber Incident Response Centre of the National Secretariat of Information and Communication Technologies (CERT-SENATICs) posted an official statement online[59] explaining that it has contacted The Citizen Lab and that the activity of FinFisher is being observed because its use is considered a crime in Paraguay.[60]

---

[51]WikiLeaks. (2010, 18 February). GoP seeks to implement new cell phone intercept system, but promises to keep SIU program intact. https://wikileaks.org/plusd/cables/10ASUNCION97_a.html

[52]EFE. (2014, 25 November). Convocan a ministros y a fiscal general por escuchas telefónicas a legisladores. Última Hora. www.ultimahora.com/convocan-ministros-y-fiscal-general-escuchas-telefonicas-legisladores-n850778.html; Escuchas telefónicas fiscales. (2003, 10 November). *ABC.* www.abc.com.py/edicion-impresa/policiales/escuchas-telefonicas-a-fiscales-729970.html

[53]www.hackingteam.it

[54]WikiLeaks. (2015, 8 July). Hacking Team. Paraguay-Uruguay Report. https://wikileaks.org/hackingteam/emails/emailid/249535

[55]Privacy International. (n/d). Briefing for the Italian Government on Hacking Team's surveillance exports. www.privacyinternational.org/sites/default/files/Briefing%20for%20the%20Italian%20Government%20on%20Hacking%20Team's%20surveillance%20exports.pdf

[56]ABC. (2015, 9 July). Gobierno negoció espionaje. *ABC.* www.abc.com.py/nacionales/estado-negocio-espionaje-1385872.html

[57]WikiLeaks Spyfile – FinFisher. https://wikileaks.org/spyfiles4/customers.html

[58]The Citizen Lab. (2015, 15 October). Pay no attention to the server behind the proxy: Mapping FinFisher's continuing proliferation. https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation

[59]CERT-PY. (n/d). Finfisher y su relación con Paraguay. www.cert.gov.py/index.php/noticias/finfisher-y-su-relacion-con-paraguay

[60]Tuit oficial del CERT-SENATICs: https://twitter.com/CERTpy/status/697104856352428033

Another element is the National Cyber Security Plan which was completed in June 2015 as a proposal of work to be implemented by CERT-SENATICs with the support of the OAS technical team.[61] Canada, Estonia, the United Kingdom and the United States contribute to this programme. Moreover, Paraguay currently presides the Inter-American Committee against Terrorism, and has been invited to join the Budapest Convention.[62] More public debate and discussion are required on drafting and implementation from the point of view of basic rights.

In terms of copyright as applied to the internet, there have been no cases of violations brought to courts in Paraguay. One of the projects that might have had an impact in this area was a failed bill on data retention[63] – the Pyrawebs bill – which planned to retain all internet traffic data in order to prosecute any punishable offence. The unauthorised downloading of copyrighted material might have come within the scope of the enforcement of this law. Thanks to strong civil society pressure, the bill was not approved.

5. Conclusions and recommendations

The debate on the right to privacy and freedom of expression in the digital environment is increasingly relevant in Paraguay, as in the rest of the region. This is due to increased connectivity which leads to more participation by people in the online environment, expressing and sharing their points of view and exercising their rights. This also implies risks of being unjustly persecuted or intimidated, or even crushed by the state apparatus, private companies or criminal groups. Therefore public policies are needed to provide greater balance and further protect the rights enshrined in the Constitution against laws and bills seeking to invade people's private lives on the pretext of combating the "horsemen of the Apocalypse."

The increasing regulations and penalties are unable to resolve the tensions generated between the right of access to culture and copyright and related rights. There are new ways of producing and consuming intangible goods promoted by the speed of access and copying provided by networks and in particular the internet. The laws must seek new mechanisms of protecting and encouraging creativity without becoming "steel cages" that hamper access to culture.

We believe there is a need for new criteria that recognise these new forms and this new tool called the "internet", that include the new ways of creating culture through information and communication technologies and that protect users from abuses by corporations and states, such as disproportionate and unnecessary surveillance, in order to safeguard the intangible heritage that is culture.

Another interesting thing about Paraguay is that there are no agencies authorised to intercept private communications without a judicial order under the current legal system. It is not possible for illegally obtained evidence, such as illegal interception of a communication, to be made admissible later on by a judge. According to Articles 166, 168 and 169 of the Code of Criminal Procedure, situations such as these are absolutely invalid and cannot be accepted or validated.

[61]Paraguay recibe apoyo de la OEA para su Plan Nacional de Ciberseguridad. www.senatics.gov.py/noticias/-/asset_publisher/T0yoqne5nEay/content/paraguay-recibe-apoyo-de-la-oea-para-su-plan-nacional-de-ciberseguridad;jsessionid=818E970B5A4E7DC1209E014893EA278C

[62]Voz de América. (2015, 7 May). OEA apoya plan de ciberseguridad de Paraguay. *Voz de América.* www.voanoticias.com/content/oea-ciberseguridad-paraguay/2753821.html

[63]Pyrawebs bill. See the campaign waged against the bill at: www.pyrawebs.tedic.org

We need wider debate on the enforcement of any plan or programme that does not include a human rights perspective, such as the Cyber Security Plan. This mechanism should also be used for the draft bill to amend the Law on Telecommunications where it lacks penalties of imprisonment or fines; penalties increase if there is public or private dissemination of telecommunications content.

As for the imperative need to amend the Law on Personal Data, in my opinion this should be urgently treated in the National Congress and discussed at a deeper level. On the one hand, a genuine law is needed that includes the minimum elements pointed out in this report, and on the other, it must be generated by a public agenda of debate. The result of all this should be a robust and efficient regulation that will be a cornerstone in the defence of fundamental rights, and so avoid the creation of laws that do not include standards for the protection of human rights, such as the "Pyrawebs" bill.

Other key regulations to strengthen freedom of expression in Paraguay are the Media Law to protect journalists and opinion leaders and a civil rights framework for the internet to reinforce mechanisms of protection of human rights on the internet.

Paraguay is undergoing technological expansion with advanced systems of communications surveillance, without proper safeguards: there is a lack of regulations enforcing accountability; a lack of transparency with regard to the use and scope of powers and techniques of communications surveillance; a lack of transparent reporting in the criminal and intelligence processes. Furthermore, there is no independent supervisory body to authorise cases of surveillance in criminal and intelligence processes. Neither are there mechanisms for deferred notification of users in the criminal or intelligence processes, so that civil society may exercise democratic control over how the authorities use their powers.