PRIVACY INTERNATIONAL

Universal Periodic Review
Stakeholder Report: 24th Session, Paraguay

The Right to Privacy in Paraguay

Submitted by Privacy International and TEDIC

The Right to Privacy in Paraguay

Stakeholder Report
Universal Periodic Review
24th Session – Paraguay

Submitted by Privacy International and TEDIC
June 2015

Introduction

1. This stakeholder report is a submission by Privacy International (PI)[1] and TEDIC[2]. PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. TEDIC is a nonprofit organization in Paraguay. The mission is the defence and promotion of digital rights and the development of civil technology by influencing public policies toward a free culture.

2. PI and TEDIC wish to bring concerns about the protection and promotion of the right to privacy in Paraguay before the Human Rights Council for consideration in Paraguay's upcoming review.

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[3] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association. Activities that restrict the right to privacy can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursue.[4]

4. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data[5] A number of international instruments enshrine data protection principles,[6] and many domestic legislatures have incorporated such principles into national law.[7]

Follow up to the previous UPR

5. There was no mention of the right to privacy and data protection neither in the National Report submitted by Paraguay nor in the report of the Working Group.

---

1 For further information, please visit our website at: www.privacyinternational.org

2 For further information, please visit our website at: http://tedic.org/

3 Universal Declaration of Human Rights (Article 12), International Covenant on Civil and Political Rights (Article 17); regional treaties and standards including the African Charter on the Rights and Welfare of the Child (Article 10), the American Convention on Human Rights (Article 11), the African Union Principles on Freedom of Expression (Article 4), the American Declaration of the Rights and Duties of Man (Article 5), the Arab Charter on Human Rights (Article 21), and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8).

4 See Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17); see also report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014.

5 Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

6 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

7 As of December 2014, over 100 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (December 8, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

Domestic laws related to privacy

6. The Constitution of Paraguay protects the right to privacy under Article 33 reads:

> *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.*

7. Article 36 of the Constitution protects private communications against unlawful interference as follows:

> *The documental heritage of the persons 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 except by a judicial order for cases specifically specified 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 that prescribed above lacks validity in trial.*
>
> *In every case, strict reservation will be observed regarding that which would not be related to the [person] investigated.*

8. Furthermore, Article 135 upholds constitutional remedy of Habeas Data, and reads:

> *All persons may access the information and the data about themselves, or about their assets, that is contained in official or private registries of a public character, as well as to know the use made of these and for what purpose. All persons may request before the competent magistrate to update, rectify or destroy the data held on them, if they are wrong or illegitimately affect their rights.*

9. The Paraguayan Congress has adopted other laws with the purpose of protection personal data including, Law 1682/01 which was subsequently amended by the Law 1962/02.

10. In additional the Paraguayan Criminal Code[8] provides under Chapter VII on Punishable Acts against private life and the privacy of the person, other criminal sanctions for various violations including:
    - Violation of the home (Article 141)
    - Trespassing (Article 142)
    - Harm to the privacy of a person (Article 143)
    - Harm to the right to communication and image (Article 144).
    - Breach of confidentiality (Article 145)
    - Violation of the secrecy of communication (Article 146)
    - Exposing a secret of person nature (Article 147)
    - Disclosure of private secrets by a person with a special obligation to maintain the secret due to its profession (Article 148)
    - Disclosure of private secrets for economic purpose (Article 149)

International obligations relating to privacy

11. Paraguay is a founding member of the United Nations in 1945 and it has ratified the International Covenant on Civil and Political Rights ('ICCPR'), which under Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "*no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation".*

12. The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to *"adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."*

13. Paraguay has also ratified the American Convention on Human Rights which upholds the right to privacy under Article 11 and by virtue of the enactment of Decree No. 16,078 of 8 January 1993, the government of Paraguay recognised the competence of the Inter-American Court of Human Rights.

Areas of concern

14. Following decades of dictatorship under Alfredo Stroessner from 1954 to 1989, Paraguay entered a transitional period toward democracy which is still ongoing.

15. The debate on right to privacy and freedom of expression in the digital sphere is becoming more relevant in Paraguay as an increasing number of individuals are engaging online, and using it as a tool to express and share their political views, despite risks of being unfairly prosecuted or intimidated.

16. Also, a government campaign aimed at silencing, repressing, and surveilling of everyone in the country, in the name of tackling drug trafficking, has been reported..[9]

---

[8] Criminal Code of the Republic of Paraguay, Law 1160/97. Available at http://www.mre.gov.py/v1/Adjuntos/Privacidad/Ley1160.pdf

[9] Polischuk, S., Otro periodista asesinado en Paraguay mientras aumenta la vigilancia estatal, Resumer Latinamericano, 9 March 2015. Available at: http://www.resumenlatinoamericano.org/2015/03/09/otro-periodista-asesinado-en-paraguay-mientras-aumenta-la-vigilancia-estatal/

Communication surveillance

17. Like many countries in the region, Paraguayan suffered immensely during the dictatorship from the surveillance mechanisms put in place by its dictator. Archive documentation of what became known as the "Archive of Terror" documenting the operations of Stroessner's secret police for decades including information sharing with neighbouring Latin American dictatorship particular Chile and Argentina, showed that Stroessner's surveillance mechanisms were still in place after he had been ousted in 1989.[10]

Unlawful communication surveillance

18. The Penal Procedural Code[11] outlines the mechanisms and rules necessary to intercept and prevent a recipient (secuestro) from receiving correspondence which includes a judicial order with the aim of finding the truth under Article 198 and Article 199 allows with a judicial order, the interception and seizure of correspondence, telegraph or any other kind of correspondence.

19. Article 200 of the same text upholds that communication surveillance is exceptional, and that a judge may order the interception of communication of a person accused of an offence, and may use whatever technical means to obtain information (cualquiera sea el medio técnico utilizado para conocerlas).

20. Under Article 89 of the Telecommunication Law 642/95 the inviolability of correspondence conducted through telecommunication service is protected, except if authorised by a judicial order. Article 90 further defines further what the inviolability means, as *opening, abstracting, interfering, changing text, rerouting, publish, use, trying to know or facilitate that a person, beyond the recipient, has knowledge of the existence or content of the communication entrusted to the service provider and to provide an opportunity to commit such acts.*

21. Despite the provisions highlighted above, we are concerned by reports that suggest that surveillance is being conducted outside the legal framework. For example, it was reported that the Paraguayan intelligence services use surveillance for political purposes, as revealed in a cable[12], which was sent in February 2010 from the US Embassy in Paraguay to the US Government. The cable revealed that eavesdropping equipment intended for US-Paraguayan partnership to combat drug trafficking was requested to be used for political spying of the Paraguayan People's Army.[13]

22. International human rights standards require that any interference with the right to privacy, such as communication surveillance, must be prescribed by laws, which are accessible, and meets standards of clarity and precision to

---

[10] Ceaser, M., Paraguay's archive of terror, 11 March 2002. BBC News, http://news.bbc.co.uk/1/hi/world/americas/1866517.stm

[11] Law 1286/98. Available at: http://www.bacn.gov.py/MjAz&ley-n-1286

[12] Available at:https://wikileaks.ch/cable/2010/02/10ASUNCION97.html

[13] See: Rodriguez, K., *How the US fuels Latin America's surveillance technology*, Al Jazeera, Opinion, 21 May 2012. http://www.aljazeera.com/indepth/opinion/2012/05/201251413563152746 4.html and Rodriguez, K., *Surveillance Camp I: Mapping Strategies to Counteract Online Spying in Latin America*, Global Voices, 30 January 2013. Available at: https://advocacy.globalvoicesonline.org/2013/01/31/surveillance-camp-i-mapping-strategies-to-counteract-online-spying-in-latin-america/

allow individuals to foresee the scope of their applications. Secret or unaccessible laws do not meet the standards of legality required under international human rights standards.

Data retention

23. On 4 June 2015, the Senate defeated a draft data retention bill,[14] renamed "Pyrawebs"[15] by civil society campaigners[16]. Amongst others, the main concerns around the bill was the retention of communications and locations data of all users for a period of 12 months, access for any type of offence and failure to specify a level of evidentiary proof or justification that needed to be met to obtain access to the data.[17]

24. Whilst we welcome the defeat of this bill, we remain concerned by Article 10 of the Electronic Commerce law of 2013[18] which imposes an obligation on intermediary service providers, hosting service providers and data providers to store communications data for a duration of 6 months.

25. The interception, collection and use of communications data (metadata) interfere with the right to privacy, as it has been recognized by human rights experts, including the UN Special Rapporteur on freedom of expression, the UN Special Rapporteur on counter-terrorism and human rights and the High Commissioner for Human Rights.[19]

26. The European Court of Justice issued an important decision in April 2014 when it declared the EU Directive on Data Retention was invalid and noted that metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained" and concluded that the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right to privacy.[20]

Establishment of intelligence agency

27. With the Presidential Decree No. 2812 of 18 December 2014[21], the President of Paraguay, Horacion Cartes established regulations under Law No. 5241, of

---

14 EFF, *Turning the tide against online spying in Paraguay*, IFEX, 5 June 2015. Available at: http://www.ifex.org/paraguay/2015/06/05/pyrawebs_campaign_victory/

15 "Pyrawebs", which is a play on words on the terms "pyragues", which refers to the civil spy network that operated under the Stroessner.

16 Amnistia Internacional and TEDIC, *Comentarios Y Recomendaciones de Amnistia Internacional (AI) y la Organización Tecnología, Educación, Desarrollo, Investigación Y Comunicación (TEDIC) Sobre eEl Proyecto De Ley "QUE Establece La Obligación De Conservar Los Datos De Tráfico*", May 2015. Available at: http://amnesty.org.py/wp-content/uploads/2015/05/PARAGUAY_Pyto.-de-Ley-que-establece-la-obligaci%C3%B3n-de-conservar-los-datos-de-tr%C3%A1fico-Mayo-2015_FINAL.pdf

17 Rodriguez, K., Pyrawebs, Paraguyans Rise Against Mandatory Data Retention, EFF, 12 March 2015. Available at: https://www.eff.org/deeplinks/2014/12/pyrawebs-paraguayans-rise-against-mandatory-data-retention

18 LawNo. 4868/13. Available at: http://www.eljurista.com.py/admin/publics/upload/archivos/ea41b40fb8ce27bd7ec64237fd75ef89.pdf

19 See report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

20 See: Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CA0293 .

21 Presidential Decree No. 2812 for the regulation of Law No. 5241/2014, which creates the national intelligence system. Available at: http://www.presidencia.gov.py/archivos/documentos/DECRETO2812_uegnk41y.pdf

22 August 2014, creating the National Intelligence System[22] (Sinai, Sistema Nacional de Inteligencia)[23].[24] It is unclear what the intelligence apparatus was prior to the establishment of the Sinai

28. According to Law No. 5241/2014[25] and the the Presidential Decree No. 2812/2014[26], only the National Secretary of Intelligence (SIN, Secretaria Nacion de Inteligencia) has the authority to "collect and process" information with the aim of producing intelligence. But Article 24 of the Presidential Decree No. 2812/2014[27] also mentions General Directorate of Intelligence as being responsible for the collection and processing of information to produce intelligence. However, this body is not included nor its activities and powers outlines in Law No. 5241/2014.

29. Whilst the law provides that communications surveillance will only be conducted in exceptional circumstances if it cannot be obtained elsewhere (Article 24), and only following judicial authorisation (Article 26), the following areas are of concern with regards to ensuring the application of human rights standards to the application of communication surveillance by intelligence agencies.

30. The National Secretary of Intelligence (SIN), the body of the SINAI which is authorised to conduct surveillance, is administratively and functionally autonomous, but it is still dependent on the Executive (article 13.) This raises concerns as to the independence of the SIN from the Executive who will be submitting to in request to conduct surveillance.

31. The law allows intelligence gathered by the Sinai to be used to prevent, warn and inform of *any* threat or risk which will affect national interests[28]. This is a very broad and vague definition which fails to limit the purpose and aim of communication surveillance, and opens the door to abuse.

32. Article 3(4) outlines the principles by which the Sinai, including the organisms and individuals that make it up, will have to request judicial authorisation in order to obtain personal information from a competent judicial authority. However the article also reads that in cases "*serious"* threats to collective security of individuals, authorities and institutions, or public security and the rule of law, this judicial authorisation can be bypassed. By failing to define what constitutes "serious", the law introduces a broad opportunity to lawfully bypass the requirement for judicial authorisation.

33. Furthermore, we are concerned the lack of a robust oversight of intelligence activities and the law imposes blanket secrecy to those involved in intelligence operations, the confidential classification of documents, records and archives related to intelligence and counter-intelligence activities will

---

22 The Sinai consists of the The National Council of Intelligence (CNI), the Ministry of Interior, the Ministry of National Defence, and the Armed Forces of the Nation, the Permanent Secretary of the Council of National Defence, the National Anti-Drugs Secretary (SENAD), and the Money Laundering Prevention Secretariat (SEPRELAD).

23 Law No. 5241/2014. Available at: http://www.gacetaoficial.gov.py/uploads/pdf/2014/2014-08-22/gaceta_2399_GEDAIDIJADKDHBJAJCAEHEACFGGJHBECFICCBKBC.pdf

24 La Información, *Horacio Cartes crea la primera agencia nacional de inteligencia de Paraguay*, 24 December 2015. Available at: http://noticias.lainformacion.com/politica/defensa/horacio-cartes-crea-la-primera-agencia-nacional-de-inteligencia-de-paraguay_SIU44zEY8cXhCL7DuLTeN3/

25 Article 14 (1) of Law No. 5241/2014

26 Article 12 (a) of Presidential Decree No. 2812/2014

27 Presidential Decree No. 2812 for the regulation of Law No. 5241/2014, which creates the national intelligence system. Available at: http://www.presidencia.gov.py/archivos/documentos/DECRETO2812_uegnk41y.pdf

28 Article 2 (a) of Presidential Decree No. 2812/2014

reserved for a period of 20 years and also, the law does not provide for notification of individuals subject to surveillance.

Data protection

34. In 2001[29], Paraguay enacted a data protection law which was modified in 2002, by Law No. 1969[30]. As amended in 2002, the law regulates the collection, storage, distribution, publication, modification, destruction, and duration, and in general, the treatment of personal data contained in public and private databases.

35. However the law failed to created a data protection authority. This means that individual must file complaints with the courts.[31] Data protection rules need to be enforced by an independent data protection authority which is given the resources and mandate to investigate, act on complaints, and impose fines in case of breaches of the law.

Health data

36. Whilst there is not specific laws for the protection of personal health information, Law No. 1682/2001 includes the protection "medical condition" under its provision on the protection of sensitive data under Article 4.

37. However this still concerns as the Law No. 1682/2001 does not impose any penalties for violations of personal health information, it only applies sanctions for violations of financial and economic solvency data.[32]

Abortion

38. Several UN treaty bodies such as the Committee on the Elimination of Discrimination against Women (CEDAW) expressed concern regarding the lack of a confidentiality code/policy in medical centres violates the patients' privacy rights, in particularly women who are admitted in hospital for complications of abortion.[33]

39. Furthermore, Paraguayan NGOs and INGOs, such as Amnesty International, have expressed concerns that lack of confidentiality and respect for the right to privacy is an obstacle which is preventing women and girls from seeking medical assistant for post-abortion care after unsafe, clandestine abortion.[34]

40. There is an urgent need for relevant stake-holders including law enforcement and particularly health care professionals to be aware of the their legal obligations to safeguard the privacy of their patients and to respect their professional oath to provide emergency care to those who need it.

---

29 Law No. 1682/2001 http://www.bacn.gov.py/MjUzOQ==&ley-n-1969

30 Ibid

31 Leiva, A. M., *Data Protection Law in Spain and Latin America: Survey of Legal Approaches*, International Law News, Fall 2012, Volume 41. No. 4. Available at: http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html

32 LexiMundi, Data Privacy, Global Practice Guide, pp 102-103. Available: http://www.lexmundi.com/Document.asp?DocID=6349

33 Concluding observations of the Committee on the Elimination of Discrimination against Women (CEDAW) on Paraguay, UN Doc. CEDAW/C/PRY/CO/6, 8 November 2011, para. 31

34 Amnesty International, Submission to the UN Committee on Economic, Social and Cultural Rights, 54th Session (23 February-6 March 2015), pp 15-18. Available at: http://tbinternet.ohchr.org/Treaties/CESCR/Shared%20Documents/PRY/INT_CESCR_CSS_PRY_19059_E.pdf

On-going legislative processes

41. Paraguay is also in the process of drafting various new bills, which will have privacy implications.

42. In 2013, a project law, No. 1881 amending the law No. 1340 of 22 November 1988 which suppressed the illicit traffic in narcotic drugs and dangerous drugs and related crimes and establishes other measures of prevention and recovery of drug addicts.[35] One of the provisions which raises concern is Article 8 which reads that judicial authorisation for activities described as 'special investigations' in the bill such as electronic surveillance, will not have to be recorded in the case file until the preliminary hearing.[36]

43. Paraguay opened a consultation with the view of reforming the Telecommunications Act with the aim of modernising and encouraging the advancement of telecommunication in Paraguay.[37] One of the main concerning provisions being discussed in this reform process is the lack of net neutrality provisions. Net neutrality is essential to ensure that internet providers treat all data that travels over its networks equally, without discrimination, rather than adding a layer of control over what data can be accessed on its network. Net neutrality is argued as a guiding principle to ensure the internet remains free and open but also it provides a framework to protect privacy.[38]

44. In November 2014, the Organisation of America States (OAS) and the National Secretariat for Information and Communication Technologies (SENATICS) of Paraguay, announced they OAS would be supporting Paraguay in the development of a National Cybersecurity Plan.[39] A draft plan is yet to be produced but a working group has been created which includes civil society representatives.

45. In these various legislative processes, it is essential that Paraguay takes on an open and transparent consultation process for stakeholders to engage in the process, particularly civil society organisations, as well as takes the necessary steps to ensure that new legislation respects its international human rights law and standards on the right to privacy, and other fundamental rights and freedoms.

Recommendations

46. We recommend that the government of Paraguay:

---

35 Available at: http://www.ipasecpy.net/preguntas-frecuentes/marco-legal-de-la-seguridad-ciudadana/normativa-interna/

36 Ferreira, M., *Proyecto de ley contra el crimen organizado*, ABC, 28 April 2014. Available at:http://www.abc.com.py/edicion-impresa/suplementos/judicial/proyecto-de-ley-contra-el-crimen-organizado-1238930.html

37 Agenda Legislativo, *Harán audiencia pública sobre proyecto de reforma de ley de telecomunicaciones*, 12 march 2015. Available at:http://www.agendalegislativa.com.py/paraguay/8759-haran-audiencia-publica-sobre-proyecto-de-reforma-de-ley-de-telecomunicaciones

38 Masse, E. and MacDonald, R., *Human Rights Day: Network neutrality key to preserving online privacy*, Access, Blog, 10 December 2013. Available at: https://www.accessnow.org/blog/2013/12/10/human-rights-day-network-neutrality-key-to-preserving-online-privacy

39 OAS, *OEA apoyará a Paraguay en el desarrollo de su Plan Nacional de Seguridad Cibernética*, Press release, C-476/14, 3 November 2014. Available at: http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-476/14

- Recognise and take steps towards compliance with international human rights law and standards by ensuring the application of the following principles to communication surveillance namely, legality, legitimacy, necessity, adequacy, proportionality and respecting process of authorisation from a competent judicial authority, with due process, user notification, transparency, public oversight and respect for the integrity of communications and systems as well as ensuring safeguards against illegitimate access and right to effective remedy;
- Ensure it takes the necessary measures to ensure that the function and operations of intelligence agencies fall within an independent oversight mechanism to ensure transparency and accountability;
- Ensure that the state surveillance of online and offline activities is lawful and does not infringe on citizen's fundamental rights and freedoms, including through use of the information communication technologies;
- Review the data retention framework in order to ensure its compliance with international standards;
- Review data protection legal framework in order to include access to redress and reparation in case of violations, particularly in relations to personal health information;
- Establish an independent data protection authority with the necessary resources, staffing and other powers to investigate and sanction cases of data protection breaches.
- Take the necessary steps to ensure an open and transparent legislative process of draft legislation processes initiated and ensure the bills are in compliance with Paraguay's international human rights law and standards on the right to privacy, and other fundamental rights and freedoms.