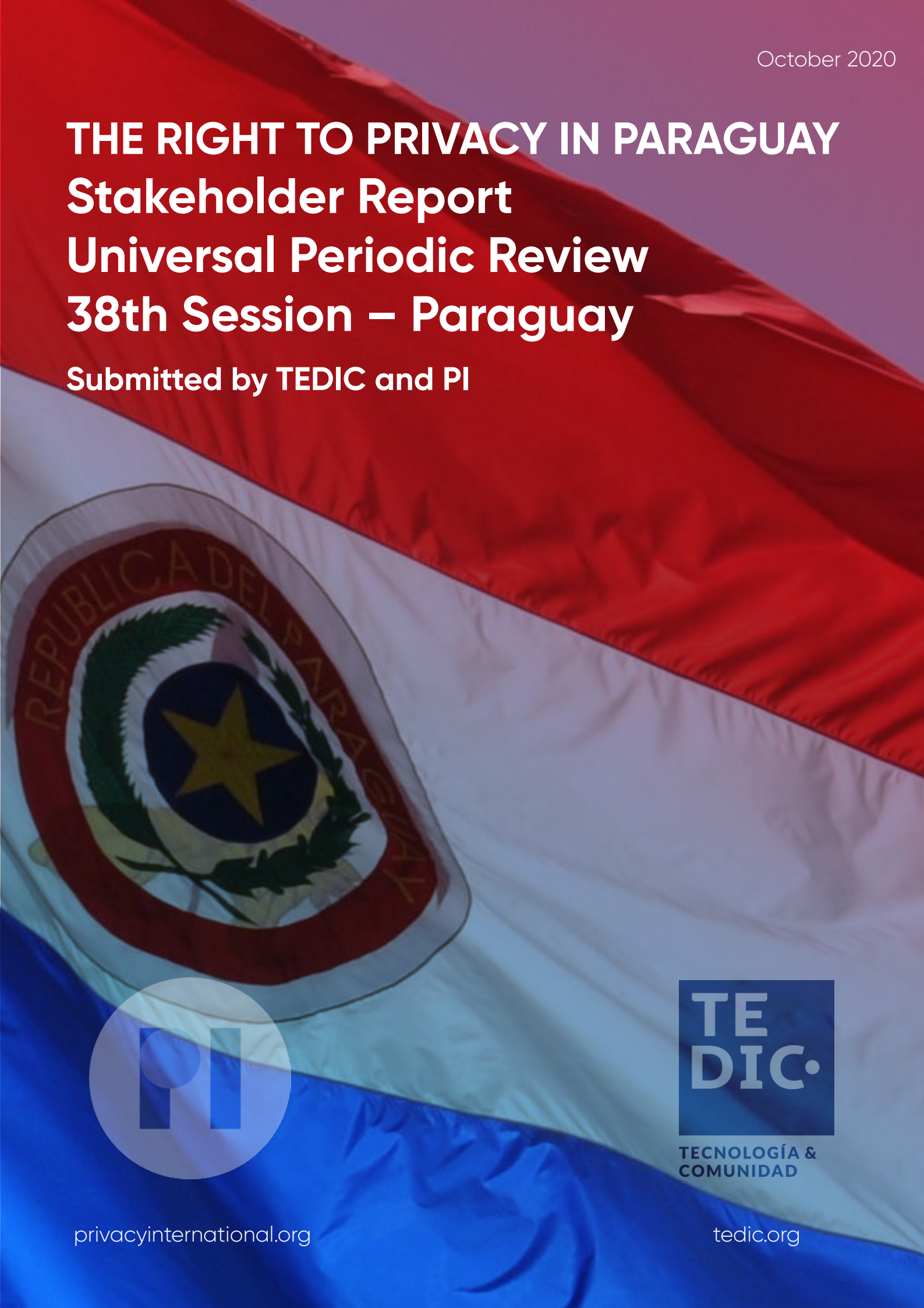
October 2020

THE RIGHT TO PRIVACY IN PARAGUAY
Stakeholder Report
Universal Periodic Review
38th Session – Paraguay

Submitted by TEDIC and PI



TECNOLOGÍA & COMUNIDAD

privacyinternational.org

tedic.org

Introduction

1. This report is presented by TEDIC[1] (Technology and Community Association) and Privacy International[2] (PI). TEDIC is a non-governmental, non-profit organization, based in Asunción, that promotes and defends human rights on the Internet and extends its networking to Latin America. PI is a London based human rights organization that works globally at the intersection of modern technologies and rights.

2. TEDIC and PI wish to express some concerns about the protection and promotion of the right to privacy, to be considered in the next review of Paraguay, in the 38th session of the Working Group of the Universal Periodic Review.

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 and it also supports and reinforces other rights and freedoms.[4]

4. 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 pursued. [5]

5. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data[6], the right to privacy has evolved to encapsulate State obligations related to the protection of personal data. A number of international instruments enshrine data protection principles[7], and many domestic legislatures have incorporated such principles into national law[8].

---

1 TEDIC's website: https://www.tedic.org
2 Privacy International's website: https://www.privacyinternational.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 Privacy International, Privacy Matters: https://privacyinternational.org/learning-resources/privacy-matters
5 See Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honor 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.
6 Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honor and reputation (art. 17)
7 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)
8 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

Follow up to the previous UPR

6. In the second cycle of the UPR in 2016, the UPR Working Group report made express mention of the observations presented by TEDIC and PI on the need for the government of Paraguay to take active measures to protect, respect and promote the right to privacy.

7. For its part, the Paraguayan State accepted[9] recommendations submitted by the Principality of Liechtenstein on monitoring activities[10]:

   - 102.62: ensure that all State surveillance activities are in line with international human rights law and do not infringe on the fundamental rights and freedoms of citizens.

   - 102.63: adopt the necessary measures to ensure that the operations of intelligence agencies are supervised by an independent oversight mechanism in order to ensure transparency and accountability.

Domestic laws related to privacy

8. The Constitution of Paraguay protects the right to privacy under Article 33, which 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*".

9. 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. […]".*

10. Furthermore, Article 135 upholds the 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 know the use made of these and for what purpose. All persons may request before the*

---

9 Ministry of Foreign Affairs of Paraguay. SIMORE system: https://www.mre.gov.py/SimorePlus (Surveillance label). Rights involved in the recommendations: Liberty and security of the person, Nonviolence, Civil and political rights, Scope of international obligations. Institution involved in the fulfillment and follow-up of these recommendations: National Telecommunications Commission, Ministry of the Interior, National Secretariat for Information and Communication Technologies (currently Ministry of Information and Communication Technology) and Ministry of National Defense. The SDG that it affects: 16 - Promote peaceful and inclusive societies for sustainable development, facilitate access to justice for all and build effective and inclusive institutions that are accountable at all levels. General remarks:
- Universal Periodic Review General Comment No. 16: Right to Privacy (Article 17)
- Universal Periodic Review General Comment No. 35: Liberty and security of person

10 A/HRC/32/9/Add.1, para. 34

competent magistrate to update, rectify or destroy the data held on them, if they are wrong or illegitimately affect their rights".

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

12. The Paraguayan Criminal Code[11] provides under Chapter VII on 'Punishable Acts against private life and the privacy of the person' and 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 personal nature (Article 147)
    - Disclosure of private secrets by a person with a special obligation to maintain the secret due to their profession (Article 148)
    - Disclosure of private secrets for economic purposes (Article 149)

International obligations relating to privacy

13. Paraguay was a founding member of the United Nations in 1945 and it has ratified the International Covenant on Civil and Political Rights (ICCPR), which under its Article 17 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 honor and reputation*".

14. 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]*".[12]

15. 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 recognized the competence of the Inter-American Court of Human Rights.

UN Human Rights Committee, ICCPR: Concluding observations on the fourth

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

12 UN HRC, General Comment No. 16: Article 17 (Right to Privacy), 8 April 1988, para. 1

periodic report of Paraguay

16. At its 126th session, the Human Rights Committee urged the Paraguayan State to intensify its efforts to deepen the promotion and protection of some specific rights.[13] In line with what TEDIC had reported[14], the Committee noted that:

    36. (…) the existence of a bill on the protection of journalists and human rights defenders that provides for the establishment of a national protection mechanism. However, it is concerned about reports of attacks, reprisals and assaults against journalists and human rights defenders, as well as the few convictions in that regard, and about the inadequate measures for ensuring their effective protection. The Committee is also concerned about allegations of the State's monitoring of private communications, including those of journalists. The Committee notes the information provided about the implementation of Act No. 5282/14 on free access by citizens to public information and government transparency, but regrets that there is no independent regulatory body to monitor the Act's implementation (arts. 6, 7, 9, 17, 19 and 22).

    37. (c) [Paraguay should] avoid State surveillance of any form, including of journalists and human rights defenders, except in the rare cases in which it is compatible with the Covenant, and establish a mechanism to oversee investigations of private communications carried out by the State.

Areas of concern

17. Following from the recommendations made to Paraguay during the second cycle of the UPR[15], TEDIC submitted a request for public information to the Paraguayan Ministry of Foreign Affairs and the Permanent Secretary of the Council of National Defense, the National Anti-Drugs Secretary (SENAD).

18. The Ministry of Interior[16] and SENAD[17] responded to the request by sharing the regulations that enable it to monitor communications. However, we deem that they are not sufficient to clarify the acquisitions and use of specific hardware and software for communication surveillance outlined and the regulation of surveillance activities undertaken by intelligence agencies as outlined in the following sections. The regulation shared only refers to telephone interception.

---

13 International Covenant on Civil and Political Rights. Concluding observations on the fourth periodic report of Paraguay. Year 2019. https://undocs.org/en/CCPR/C/PRY/CO/4

14 TEDIC presents the shadow report to the UN CCPR. Year 2019 https://www.tedic.org/tedic-presenta-reporte-ante-el-ccpr-de-la-onu/

15 See: see paragraph 7

16 Request #34610 United Nations Universal Periodic Review (UPR) - Ministry of Interior. September. 2020. https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/34610 [Accessed on September 13, 2020]

17 Request #34609 United Nations Universal Periodic Review (UPR) – SENAD. September. 2020 https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/34609 [Accessed on September 13, 2020]

19. Regarding the request for information about the accountability mechanisms, they only refer to administrative issues related to salaries, list of officials, acquisitions of goods, etc., but they do not provide the information requested to receive assurances about areas of concern outlined below including:
    - the measures and protocols that are being carried out in the operations of the intelligence agencies including the National Intelligence System, the Ministry of the Interior and SENAD,
    - the implementation, protocols and any type of personal data processing of individuals subject to surveillance by the intelligence agencies.
    - The measures and protocols to ensure transparency and accountability such as independent monitoring mechanisms.

Monitoring of communications

20. The Penal Procedural Code[18], under Articles 198 and 199, outlines the mechanisms and rules necessary to intercept and seize the correspondence sent by the accused or intended for them (epistolary, telegraphic or of any other kind), with the aim of finding the truth and including the requirement of a judicial order. Article 200 of the same text upholds that the interception of communications must be exceptional. A judge may order the interception of the communications of the accused, by whatever technical means.

21. Under Article 89 of the Telecommunications Law 642/95, the inviolability of correspondence conducted through telecommunication service providers is protected, except when authorized by a judicial order. Article 90 further defines inviolability as opening, abstracting, interfering, changing text, rerouting, publishing, using, trying to know or facilitating that any person beyond the recipient has knowledge of the existence or content of the communication entrusted to the service provider, or providing an opportunity to commit such acts.

22. With the Presidential Decree No. 2812 of 18 December 2014, the President of Paraguay, Horacio Cartes, established regulations under Law No. 5241 of 22 August 2014, creating the National Intelligence System (SINAI, 'Sistema Nacional de Inteligencia').[19] It is unclear what the intelligence apparatus was prior to the establishment of the SINAI.

23. According to Law No. 5241/2014 and the Presidential Decree No. 2812/2014, only the National Secretary of Intelligence (SIN, Secretaría de Inteligencia Nacional) has the authority to "collect and process" information with the aim of producing intelligence. But Article 24 of the Presidential Decree No. 2812/2014 also mentions the 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 outlined, in Law No. 5241/2014.

24. Whilst the law provides that the monitoring of communications will only be conducted in exceptional circumstances, when it cannot be obtained through other means (Article 24)

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

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

and only following a judicial authorization (Article 26), the following areas are of concern with regards to ensuring the compliance with human rights standards on the application of communication surveillance by intelligence agencies:

i. **Lack of independence from the executive:** The SIN, the body of the SINAI which is authorized 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 requests to conduct surveillance.

ii. **Lack of definition of 'national interest':** The law allows intelligence gathered by the SINAI to be used to prevent, warn and inform of any threat or risk which may affect national interests. 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.

iii. **Broad definitions of "serious threat" allows judicial authorization to be bypassed**: Article 3 (Law 5241/14) outlines the principles by which the SINAI, including the organisms and individuals that make it up, will have to request a judicial authorization in order to obtain personal information from a competent judicial authority. However, the article also reads that in cases of 'serious' threats to the collective security of individuals, authorities and institutions, or public security and the rule of law, this judicial authorization may be bypassed. By failing to define what constitutes a 'serious' threat, the law introduces a broad opportunity to lawfully bypass the requirement for judicial authorization.

iv. **Lack of robust oversight and transparency:** We are concerned about the lack of a robust oversight of intelligence activities and the law imposes a blanket of secrecy around those involved in intelligence operations. The confidential classification of documents, records and archives related to intelligence and counter-intelligence activities will be reserved for a period of 20 years. The SINAI, the SENAD, and the Armed Forces and the Ministry of the Interior do not have the obligation to publish reports on communications surveillance activities, so they operate with total autonomy and little effective oversight, or said otherwise, with total impunity.

v. **No notification requirement:** Finally, the law does not provide for the notification of individuals subject to surveillance. Those whose communications are being surveilled should be notified 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 authorisation. Only limited circumstances could allow for such notification to be postponed/delayed but those instances must be clear and regulated by law.[20]

Surveillance capabilities

25. As a result of the lack of transparency of surveillance policies and practices in Paraguay, it is not clear what kind of capacities the State possesses. However, several reports have appeared in recent years showing the existence of communications surveillance systems which differ substantially from what the surveillance activities permitted for the government to undertake by law, and there is evidence that over the last few years the Paraguayan State has obtained a series of tools to conduct surveillance without an appropriate legal framework in place to oversee their acquisition and use.

20 For examples for example if it would undermine the purpose of the activity or there is an imminent risk of danger to human life,

26. For example, there is evidence of the purchase of the Finfisher software, a highly invasive surveillance malware developed by the North American company Gamma.[21] It was reportedly acquired by the SENAD[22], as evidenced by publications of invoices, purchase receipts and a record of delivery published by the newspaper ABC Color and as outlined in research by the Citizen Lab of the University of Toronto, Canada in 2012.[23]

27. Finfisher is a highly intrusive software that once installed allows the authorities to follow the movements of each user of a cell phone or another selected device. Specifically, it gives access to the complete location history of a user, enables secretly recording audio and video from the microphones and cameras of a smartphone or a laptop, as well as allowing to retrieve the user's contact list or even remotely implanting incriminating evidence on a user's device.

28. There are also records of the acquisition by the State of software for wiretapping. Wikileaks has leaked diplomatic conversations of 2010 between the Ministry of the Interior and the Embassy of the United States, where they talk about the purchase of wiretapping software.[24]

29. Another similar case occurred during the government of ex-president Federico Franco, who also acquired wiretapping equipment worth 2.5 million dollars. According to a report from the General Audit Office of the Executive Branch, the wiretapping team had disappeared from the offices of the Ministry of the Interior by November 2013.

30. These activities of wiretapping were undertaken without a judicial order[25], and such activities continue to be carried out under the excuse that it is used only and exclusively for cases of extortion and kidnapping, as no judicial order is required in such instances, thus violating due process.

31. Wikileaks cables revealed that the Public Ministry, through the Office for the Control of Computer Crimes, had held conversations for the purchase of surveillance software, Galileo software – Remote Control System (RCS), from the Italian company Hacking Team.[26] To date, it has not been confirmed whether the purchase was completed.

32. The Joint Task Forces (FTC), made up of the Armed Forces, the Ministry of the Interior and the SENAD, is an institution created 7 years ago to mitigate terrorism in the northern part of the country, and receives 14 million dollars annually.[27] This Institution acquired

---

21 More questions and doubts about malicious software acquired by SENAD. Available at https://www.tedic.org/mas-preguntas-y-dudas-sobre-software-malicioso-adquirido-por-senad/ ; and Mapping Finfisher https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/ [Accessed on August 20, 2020]

22 Available at "Senad spent almost 200 million guaraníes just on «assemblage and setup»" http://www.abc.com.py/edicion-impresa/judiciales-y-policiales/senad-gasto-casi-g-200-millones-solo-en-montaje-y-configuracion-590062.html?fb_comment_id=419236824858112_2094744#f1c83727667f9fc ; and "Senad denies the purchase of the software" http://www.hoy.com.py/nacionales/senad-niega-negociado-en-compra-de-equipo-de-escuchas [Accessed on August 20, 2020]

23 Available at https://citizenlab.org/ [Accessed on August 20, 2020]

24 Available at https://wikileaks.org/plusd/cables/10ASUNCION97_a.html [Accessed on August 20, 2020]

25 Channel 4 Telefuturo Report: Wiretapping without a court order will occur in the event of extortion and kidnapping - 11/26/2014 https://www.youtube.com/watch?v=3Bkdspxhae8 [Accessed on August 20, 2020]

26 Available at https://wikileaks.org/hackingteam/emails/emailid/249535

27 Presidential Decree 103/2013 "which creates the Joint Task Forces (FTC)". [Accessed on August 20, 2020]

surveillance technology such as drones and surveillance software via 'exceptions' without a public tender.[28]

33. Such tools and technologies continue to be used without being subject to any accountability and oversight mechanisms with no reports published on their use including when and for what purpose.

Use of surveillance technology to tackle gender-based violence

34. The law 6558/20 modified the 'Law against Domestic Violence' and enabled the judge to impose surveillance measures such as the monitoring system by electronic control devices, which allows the recognition of the location of the aggressor, in order to monitor and control his movements. Whilst surveillance can be legitimate to investigate such crimes, if done in accordance with the principle of necessity and proportionality, there are concerns that this law puts the alleged victim reporting the crime at risk, since in order to identify the aggressor's proximity, the victim is also required to provide access to their own location to the National Police. [29]

35. The National Telecommunications Commission (CONATEL) issued resolution No. 583/20 by which "the telecommunications user protection regulation is modified" in order to prevent fraud and extortion by third parties. [30] It empowers the Ministry of the Interior to request the blocking of telephone lines without judicial authorization or compliance with due process. Telephone service operators in Paraguay were concerned about the new regulation and requested a review of the legal framework.[31] However, to date there are no responses from CONATEL authorities.

Facial recognition in Paraguay

36. The Ministry of the Interior was responsible for the purchase of national security face recognition software in 2018. The software was later used in the capital downtown[32] as well as in and around football stadiums.[33] The official argument is that they wanted to offer higher security in crowded areas.[34]

---

28 Contrataciones Públicas – FTC Https://www.contrataciones.gov.py/licitaciones/adjudicacion/352802-adquisicion-drone-desmalezadora-armada-paraguaya-1/resumen-adjudicacion.html [Accessed on September 15, 2020]

29 "Sanctioned use of electronic anklets for the prevention of domestic violence" https://www.ultimahora.com/sancionan-uso-tobilleras-electronicas-casos-violencia-domestica-n2890499.html

30 CONATEL Board Resolution N° 583/2020 https://www.conatel.gov.py/conatel/resolucion-directorio-n-24-2020-2/

31 Genera preocupación nueva resolución de CONATEL que otorga superpoderes a la policía. Junio 2020. https://www.abc.com.py/nacionales/2020/07/03/genera-preocupacion-nueva-resolucion-de-conatel-que-otorga-superpoderes-a-policia/

32 "Artificial intelligence as an ally in the anti-violence crusade" https://www.hoy.com.py/deportes/la-inteligencia-artificial-como-aliada-en-la-cruzada-antiviolencia [Accessed on August 20, 2020]

33 Biometrics and video surveillance in Paraguay. TEDIC https://www.tedic.org/biometria-y-video-vigilancia-parte1/ [Accessed on August 20, 2020]

34 Reconocimiento facial nueva forma de combatir la delicuencia. https://www.abc.com.py/nacionales/2019/07/11/reconocimiento-facial-nueva-estrategia-para-combatir-la-delincuencia/ [Accessed on August 20, 2020]

37. When TEDIC submitted a request for a transparency report through the Portal of the government for access to public information, the response of the ministry was to deny the information on its use, citing national security issues.[35]

38. The request focused on asking for a report on the details of the implementation, protocols and any type of treatment of personal data that are processed and used in the facial recognition system, as well as knowing what the purpose of the system is, if the error rates of the algorithm have been evaluated and whether an analysis has been carried out on its impact on human rights.

39. The Ministry of the Interior refused to respond to the request, alleging its reserved nature as well as its impact on national security. TEDIC presented an amparo action to the judicial authority, but access was denied both in the first and second instance. Their argument was that it puts national security at risk, since that information is considered 'sensitive material or information', and because it has been dealt with by the National Defense Council, "whose deliberations are confidential".

40. It should be noted that for certain information to be considered reserved for public access that those categories must be expressly established by law (Article 22 of Law 5282). This is not the case in Paraguay since there is no regulation that reserves the type of information that was requested. Among the information requested were: i) What is the purpose of these teams? ii) How does the software work? iii) Have the algorithm error rates been evaluated? and iv) Has a human rights impact analysis been carried out prior to its implementation?

41. The resolution in question violates the right to access information and the responsibility of State institutions to ensure transparency and regulations. Given this manifest arbitrariness, TEDIC initiated a judicial action to access public information through the amparo appeal. The basis for TEDIC's legal challenge was that denying them access to this information was contrary to Article 28 of the Constitution (Right to be informed) thus undermining the right of the whole society to know about the processing of their personal data by public institutions.

42. In September 2019, TEDIC filed an unconstitutionality action, but to date the Supreme Court has not taken any steps to issue a judgment.[36]

Government measures during the Covid-19 pandemic

43. As many countries in the world, the government of Paraguay has put in place various measures to help contain the spread of the Coronavirus. Some of these measures impose severe restrictions on people's freedoms, including to their privacy and other human rights. Unprecedented levels of surveillance, data exploitation, and misinformation are being tested across the world.

35 FOIA – TEDIC – Facial recognition cameras in Asunción - Ministry of the Interior http://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/19983

36 Who watches the watchman? Facial Recognition in Asunción. Year 2019. https://www.tedic.org/en/who-watches-the-watchman-facial-recognition-in-asuncion/ [Accessed on August 20, 2020]

44. Many of these measures are based on extraordinary powers, and like in many countries the duration of use in emergency situations have not been timebound, i.e. sunset clauses. Others use exemptions in data protection laws to share data. Some may be effective and based on advice from epidemiologists, others will not be. But all of them must be temporary, necessary, and proportionate.

45. Here we outline various measures taken by the government which require further scrutiny and accountability:

Drones in times of health emergency

46. The Ministry of the Interior acquired drones for surveillance in public spaces to enforce compliance with mandatory quarantine in times of pandemic. It is not the first time that this ministry has obtained this type of technology. In 2019 it had already acquired an unmanned vehicle capable of carrying a semi-automatic launcher of non-lethal projectiles (rubber bullets)[37]. The then Minister of the Interior, Juan Ernesto Villamayor, pointed out that the objective of that tender was to use the drone in demonstrations, evictions of buildings, raids and sporting events.[38]

47. Firstly, any measures taken in the name of public health must respond to the needs and guidance of health care professionals, and also the use of digital technologies to combat this pandemic cannot be excluded from an examination of necessity and proportionality in the event of possible effects on our fundamental rights. In line with this, all technology used in the context of this pandemic must meet this test and ensure the protection of our personal and sensitive data.

48. Furthermore, there must guarantee that such exceptional uses will be limited to the emergency we face and terminated as soon as they are no longer necessary, and they must enable access to accountability procedures. All these measures are key to avoiding a disproportionate impact leading to discrimination against the most vulnerable groups, as well as a possible impact on mental health and the stigmatization of people affected by COVID-19.

Social media monitoring and surveillance of peaceful demonstrations

49. Social media monitoring (SOCMINT) has become a tactic used by government agencies for law enforcement purposes which refers to the techniques and technologies that allow companies or governments to monitor social media networking sites such as Facebook or Twitter.[39]

---

37 Public Procurement - Ministry of the Interior - UAV Drones https://www.contrataciones.gov.py/licitaciones/adjudicacion/368495-adquisicion-vehiculo-aereo-no-tripulado-uav-dron-lanzador-semiautomatico-proyectiles-1/resumen-adjudicacion.html [Accessed on August 20, 2020] and Public Procurement - Ministry of the Interior - Drones https://www.contrataciones.gov.py/licitaciones/adjudicacion/357568-adquisicion-equipos-antidisturbios-chalecos-antibalas-drones-1/resumen-adjudicacion.html [Accessed on August 20, 2020]

38 Drone use: does it combat the pandemic or strengthen surveillance? https://www.tedic.org/en/drone-use-does-it-combat-the-pandemic-or-strengthen-surveillance/ [Accessed on August 20, 2020]

39 Privacy International, Social Media Intelligence https://privacyinternational.org/explainer/55/social-media-intelligence

50. As part of measures deployed during the pandemic, the government of Paraguay has been monitoring social media networks for compliance with mandatory confinement and other protocols established to tackle the pandemic.

51. The Cybercrime Prosecutor's Office charged a person for the alleged threat of infecting others with COVID19. The event took place on the social network Twitter, when the person published the following sentence: “We will send you the virus by delivery”. [40] Furthermore, measures deployed to tackle the pandemic interfering with other fundamental rights and freedoms such as the right to freedom of peaceful assembly and to freedom of association.

52. The Prosecutor’s Office also charged demonstrators who were peacefully protesting the murder of two girls at the hands of the Fuerzas de Tareas Conjuntas (FTC), a unit of the Paraguayan armed forces.[41] The alleged cause of the accusations was the lack of face masks.[42] They also used photographs published on social networks to identify and accuse people who were participating in a public demonstration against the government, basing the accusations on the damage inflicted to a National Monument, which had been painted over. [43]

53. Surveillance technologies are affecting the right to peaceful assembly in new and often unregulated ways, and in particular the unregulated use of SOCMINT negatively affects the exercise of the right to freedom of peaceful assembly. [44] It has a chilling effect on individuals wishing to demonstrate online, as well as using social media platforms to organise and promote peaceful assemblies.[45] The use of such tactics should only be permissible, if at all, as part of the investigation of crimes, and under strict guidelines.

54. The use of tactics raises questions about the regulations which oversee such tactics, if any exist, and also puts into question as to whether social media data is public for anyone to make use of, or whether as we would argue that this data is not public and has implications for privacy and other fundamental rights, and thus the use of such tactics must comply with the international principles of legality, necessity, and proportionality.

---

40 “Charged woman who spoke of ‘sending the virus by delivery’ on Twitter” https://www.abc.com.py/nacionales/2020/03/31/mujer-que-amenazo-con-contagiar-covid-19-se-expone-a-pena-de-tres-anos/ [Accessed on August 20, 2020]

41 “They Were Girls - Double Infanticide in Paraguay”. Página 12, Argentina https://www.pagina12.com.ar/291213-eran-ninas-el-doble-infanticidio-en-paraguay [Accessed on August 20, 2020]

42 The partiality of the prosecution leads to dangerous stronist practices https://www.ultimahora.com/la-parcialidad-la-fiscalia-lleva-peligrosas-practicas-stronistas-n2905243.html

43 “More accused for actions in front of pantheon and ask to have more prosecutors”. Última Hora https://www.ultimahora.com/mas-imputados-actos-frente-al-panteon-y-piden-tener-mas-fiscales-n2905031.html [Accessed on August 20, 2020]

44 PI, Submission on Article 21 of the International Covenant on Civil and Political Rights, February 2019, available at https://privacyinternational.org/sites/default/files/2019-03/Submission%20on%20Article%2021%20of%20ICCPR_0.pdf

45 General Comment 37 of ICCPR para. 62 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11

Biometrics in the voting system

55. The bill on the implementation of biometrics in the electronic voting system in Paraguay, "which modifies articles 98, 201 and 208 of Law 834/96", was presented in 2019. [46] In response to bill, TEDIC raised concerns about the fact that the collection of personal and sensitive identity data, including biometric information, unduly interferes with the anonymity of the persons authorized to vote. The creation of personal databases, potentially accessible to government authorities and third parties, interferes with the privacy zone.

56. The deployment of technology used to conduct elections needs to be scrutinised. Biometric voter registration, authentication and results transmissions systems are expensive to implement and often complex.[47] Procurement needs to be transparent and myths busted about how the technology actually works, what it can realistically do and what problem its use is trying to solve. Technology should reinforce trust in elections and the democratic process, not undermine it.

57. The processing of fingerprints of voters may be one more control mechanism that could aggravate surveillance practices and harassment of minorities and vulnerable groups. The deficiencies that the State already has when it comes to protecting the private information of citizens make these records even more problematic and with a high risk of being leaked.[48]

58. As noted by the Office of the High Commissioner for Human Rights (OHCHR) in its report on privacy in the digital age "*The creation of mass databases of biometric data raises significant human rights concerns. Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused*", and it concluded that: "*Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data*."[49] Furthermore, the OHCHR expressed concern that some states were proceeding with processing biometric data "*without having adequate legal and procedural safeguards in place*."[50]

59. Before proceeding with this bill, there was no evaluation of the impact of the use of the biometric data system, and there was also no previous impact analysis to assess the relevance of the implementation of such a data collection system. It is unclear why there was a need to integrate biometrics within the voting system. Any interference by the State in the private life of its citizens must be based on solid foundations and supported by serious and independent data and diagnoses, in order to meet the conditions of necessity and proportionality required for the legitimacy of any measure that seeks to limit fundamental rights.

---

46 "What is modified of articles 98, 201 and 208 of law 834/96", http://silpy.congreso.gov.py/expediente/118767 [Accessed on August 20, 2020]

47 Privacy International, Data and Elections, available at: https://privacyinternational.org/learn/data-and-elections

48 Biometric data in the electronic voting system in Paraguay https://www.tedic.org/huella-dactilar-iris-y-reconocimiento-facial-identidad-que-no-se-puede-reimprimir/ [Accessed on August 20, 2020]

49 A/HRC/39/29, para 14

50 Ibid

Personal data protection regime

60. In 2001, Paraguay enacted a data protection law which was modified in 2002 by Law No. 1969.[51] The amended law regulates the collection, storage, distribution, publication, modification, destruction, duration and in general terms the treatment of personal data contained in public and private databases. However, the law has various shortcomings which undermine its ability to effectively protect people and their data, and fails to meet the requirement to be recognized as a comprehensive data protection law in line with internationally recognised data protection standards and principles.

Absence of a data protection authority

61. The law failed to create a data protection authority. This means that the only legal form of protection is Habeas Data and there are no guarantees of protection by the State, it is only at the request of the victim. Accountability and enforcement are key components to ensure not only effective implementation of the law but also to build trust of the public. Data protection rules must be 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 is not sufficiently protected

62. Whilst there are no specific laws for the protection of personal health information, Law No. 1682/2001on data protection includes the protection of the 'medical condition', under its provision on the protection of sensitive data, under Article 4.

63. This still raises concerns, however, 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.

64. The Ministry of Health, in its resolution SG No. 146/2012[52], articles No. 4 and 6, affirms that there is an obligation to respect and protect the right to privacy, as well as the obligation for all health personnel to respect the confidentiality of the information and data of all people who receive health care or receive information and guidance through a health service provider. In other words, they must guarantee professional secrecy.

65. In this framework, the COVID19 pandemic unleashed a general fear in the population, and in the face of this crisis the responses have often been reactions of fear and discrimination. In this sense, there have been cases of harassment of people who suffered the disease, as well as their relatives. This sensitive health information was leaked by people who were

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

52 "By which the obligation is established to provide access to quality health services and care without discrimination, with effective compliance with the duty of confidentiality and guarantee of full validity of professional secrecy in care". Available at: https://clacaidigital.info/bitstream/handle/123456789/780/RES.SG.N%C2%BA%20146%20del%202012%20CON%20ANEXO.pdf?sequence=5&isAllowed [Accessed on August 20, 2020]

part of the information chain of the public and private health system, resulting in public persecution.[53]

66. The Ministry of Information and Communication Technology developed a mobile application for the registration of people with COVID19, as well as the monitoring of symptoms. According to the Ministry of Health, 5,473 people downloaded the app[54], while only people who are tested positive for the disease are registered in the system. To date, it is not possible to access the privacy and data policies of the application, nor is it planned to allow the application of the data subject rights to access, rectify, cancel and object in relations to one's profile once the critical stage of the pandemic has ended.

67. Furthermore, there have been discussion to create electronic medical records in Paraguay, through a legislative proposal that is being analysed in Congress. The proposal intends that the document registration be mandatory, chronological, individualized and complete in digital support, property of the patient. In turn, it is expected that each medical action from birth to death be stored in the form of writings, graphics, imaging or documents of any other nature.[55] To date, there is no prior analysis of the possible impact on human rights, and given that there is no comprehensive personal data protection law in Paraguay, there are no foreseeable guarantees of protection against possible abuse of this sensitive information.

68. Finally, the Social Security Institute (IPS) requests sensitive personal information, including the fingerprints of the person insured, for registration in the social system. This has caused companies to request unnecessary sensitive information from their employees, such as HIV test results, abortion history, among others.[56]

Ñandareko and Pytyvo social assistance systems

69. The State systems for economic aid and food kits for vulnerable groups in times of pandemic, called Ñandareko and Pytyvo, had several vulnerabilities in their implementation, resulting in the violation of sensitive information of the beneficiaries. Databases of individuals were leaked, and there were cases where third parties posing as beneficiaries had access to financial resources.[57] These databases are hosted on servers of private companies and their web pages do not respect minimum security criteria, such as https.
70. There are concerns that these databases could be used for political purposes, since there is no control or transparency in the collection of information. This was the case of an

53 "Family of COVID19 patient receives threats". Available at https://www.ultimahora.com/familia-paciente-covid-19-recibe-amenazas-n2875197.html [Accessed on August 20, 2020]

54 TEDIC consultation to the MSPyBs on July 30, 2020. Gender: F. 2484 M. 2989.

55 Legislators propose to create electronic medical records registry. June 2020. [Accessed on August 20, 2020] http://www.senado.gov.py/index.php/noticias/noticias-generales/5900-legisladores-proponen-crear-registro-de-historias-clinicas-electronicas-2020-06-16-22-55-57

56 Personal Data in the Social Security Institute. Exploratory analysis on some personal data protection practices in the social security system of the Paraguayan State. TEDIC 2018 https://www.tedic.org/en/investigacion/personal-data-in-the-social-security-institute-exploratory-analysis-on-some-personal-data-protection-practices-in-the-social-security-system-of-the-paraguayan-state/ [Accessed on September 15, 2020].

57 "Investigation into who leaked the Pytyvo database". June 2020. [Accessed on September 15, 2020] https://www.ultimahora.com/pytyvo-policia-descarta-hackeo-e-investiga-quienes-filtraron-datos-beneficiarios-n2888246.html

amateur soccer team that signed up for a tournament, then appeared on a roster for a Partido Colorado pro-presidential re-election campaign.[58]

Recommendations

We recommend the government of Paraguay to:

71. Adopt an adequate regulatory framework in line with internationally recognized principles and standards in order to guarantee the transparency and accountability in the acquisition of surveillance technology.

72. Adopt an adequate legislative framework in line with internationally recognized principles and standards to regulate the use of surveillance technology by the State, state bodies or other state authorized actors, which must protect people against potential abuses. Any legal framework should provide:

    a. Specific regulation on the use of intrusive surveillance tools and methods, including hacking, malware, drones as well as biometric technologies. The law needs to guarantee that any surveillance measure will respect the principles of necessity and proportionality;
    b. Independent judicial authorization;
    c. Appropriate audit mechanisms by oversight bodies for any use of private surveillance technology;
    d. Appropriate reporting procedures to ensure transparency regarding the general surveillance capabilities of the State and meaningful information regarding the scope and extent of the use of private surveillance technology;
    e. Procedures for notification of individuals victims of surveillance, as well as access to adequate remedies;
    f. Independent oversight bodies, endowed with the necessary powers to effectively audit, investigate and prosecute any abuse in the usage of surveillance technologies by State, state bodies or other state authorized actors; this includes having absolute access to any information, installations or equipment necessary to carry out their functions.
    g. Human rights impact and risks assessments before the acquisition of surveillance technologies, in order to assess and monitor potential human rights abuses and/or violations enabled by the deployment of such technologies;
    h. Mechanisms to monitor and impose appropriate penalties towards companies abusing human rights standards

73. Adopt have a comprehensive personal data protection law which meets internationally recognised standards and principles to protect people, their data and their enjoyment of fundamental rights and freedoms, including by ensuring the establishment of an independent authority for oversight and accountability of the law.

58 More and more adulterations. Abc Color. January. 2017. https://www.abc.com.py/nacionales/mas-y-mas-adulteraciones-1558716.html [Accessed on October 08, 2020]

74. To ensure that any extraordinary measures adopted to respond and tackle COVID19 are in line with human rights law and standards, are temporary and as a result their implementation should be limited in time to the pandemic, and that public health is not used as a justification to undermine and curtail disproportionally fundamental rights and freedoms.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471),
and a company limited by guarantee registered
in England and Wales (04354366).