

Asunción, June 3, 2019

Attention

Gabriella Habtom
Secretary of the Human Rights Committee
ghabtom@ohchr.org

Cherry Rosniansky
Programme Assistant of the Human Rights Committee
crosniansky@ohchr.org

CCPR mailbox
ccpr@ohchr.org

Postal address of the Secretariat Geneva:

Human Rights Committee Secretariat
8-14 Avenue de la Paix
CH 1211 Geneva 10
Switzerland

Re: NGO (alternative) reports for the HRCtte at its sessions – Paraguay (4th)

TEDIC¹ is a non-profit organization based in Asunción, Paraguay, which defends human rights on the Internet. We respectfully send this letter to Human Rights Committee Members: "Submission of the Human Rights Committee (hereinafter 'the HRCtte') to examine the situation reports of Paraguay (4th).

Introduction

In the framework of the **4th examination of the report of the Paraguayan State by the Human Rights Committee Members**, from TEDIC we present the following introduction on the state of surveillance of communications in Paraguay:

The fundamental rights to freedom of opinion and expression (**Art 19 CCPR**) are intimately intertwined with the exercise of the right to privacy. As such, state surveillance has a considerable impact on these rights. Especially, taking into consideration its potential to provoke a chilling effect on the online expression of any individual, which may derive in the predominance of self-censorship out of fear of being constantly monitored or tracked.

1 TEDIC Association: Non-profit organization based in Asunción, Paraguay that develops civic technology and defends human rights on the Internet. More information in www.tedic.org

As the UN Special Rapporteur² has already recognized, “*surveillance exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children*”. The capacity of surveillance to produce such a disproportionate impact becomes particularly relevant considering that, in recent years, there has been an increased acquisition and use of commercial surveillance by States in Latin America, often without adequate safeguards in place which has resulted in several cases of abuse, particularly against human rights defenders, journalists and activists.

This trend is especially worrisome taking into account the rooted context in the region, derived from a tradition of long-standing dictatorships and armed conflicts, of systematic and generalized human rights violations, implying recourse to unclear and disproportionate data collection and surveillance mechanisms, all within a predominant culture of lack of transparency, corruption and impunity.

Accordingly, nowadays the exercise of surveillance practices in Latin America has not been in line with a comprehensive human rights approach, comprising the appropriate control mechanisms and safeguards against abuse. The lack of such an approach has given rise to the infringement of the rights to privacy, freedom of expression and freedom of peaceful assembly, thus undermining the basis of democracy, of institutions and of the overall respect for the rule of law.

Bearing in mind the above, along with the rise of the surveillance industry and the intrusiveness and sophistication of the technology used, the existence of appropriate legislation to limit, regulate and control the exportation, acquisition and deployment of commercial surveillance tools becomes essential.

Nevertheless, to date there is an overall lack of clear, precise, unambiguous and detailed laws, administrative regulations, judicial decisions and/or other policies to regulate the export, import and use of surveillance technology in Paraguay.

In 2016, TEDIC and Privacy International³ presented these concerns in the **UPR report** and recommendations **102.62** and **102.63** of the **Principality of Liechtenstein** on surveillance activities were accepted by the Paraguayan State. These are:

“102.62: Ensure that all State surveillance activities are in line with international human rights law and do not infringe the fundamental rights and freedoms of the citizen.

102.63 Adopt the necessary measures to ensure that the operations of the intelligence agencies are supervised by an independent monitoring mechanism in order to guarantee transparency and accountability”.

2 We hope that these inputs of the UN Special Rapporteur will serve for a better interpretation to address this issue by the HRCtte.

3 <https://www.privacyinternational.org/>

Within the framework of this last scenario, there was no progress on the part of the State of Paraguay to make its uses transparent and the development of specific protocols and regulations in the acquisition and use of surveillance software in Paraguay.

Details of emblematic cases of State use of private surveillance technology against individuals in Paraguay

Today there are technologies that facilitate efficient and low-cost state surveillance. The Paraguayan State has obtained a series of tools that serve this purpose: there is evidence of the purchase of the Finfisher⁴, software, a highly invasive surveillance malware developed by the North American company Gamma. It was acquired by the Anti-Drug Secretariat (SENAD)⁵, as evidenced by publications of invoices and purchase receipts of the newspaper ABC Color and research by the Citizen Lab of the University of Toronto in Canada⁶.

Finfisher allows the authorities to follow the movements of each cell phone user or other selected device. Specifically, it gives the possibility of: navigating the history of a user's locations for years; record, covertly, audio and video of microphones and cameras of the smartphone and laptop of the user; retrieve the contact list or remotely implant incriminating evidence on the user's device.

There are also records of acquisition of software for wiretapping by the State: Wikileaks has leaked diplomatic conversations between the Ministry of the Interior and the Embassy of the United States of 2010, which talks about the purchase of a wiretapping software.⁷

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

With this background, it is not surprising that wiretapping has been verified without a judicial order⁸, and that they continue to be carried out under the excuse that they are used only and exclusively for cases of extortion and kidnapping, thus violating due process.

Finally, through a leak of one of the most well-known malware providers in the world - the Italian company Hacking Team - using WikiLeaks, and thanks to the careful work of

4 Más preguntas y dudas sobre software malicioso adquirido por SENAD. Disponible en <https://www.tedic.org/mas-preguntas-y-dudas-sobre-software-malicioso-adquirido-por-senad/> y Mapping Finfisher <https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/> [Fecha de consulta: 20 de octubre, 2016].

5 Disponible en Senad gastó casi G. 200 millones solo en "montaje y configuración" 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 y Senad niega la compra del software <http://www.hoy.com.py/nacionales/senad-niega-negociado-en-compra-de-equipo-de-escuchas> [Fecha de consulta: 20 de octubre, 2016].

6 Disponible en <https://citizenlab.org/> [Fecha de consulta: 20 de octubre, 2016].

7 Disponible en https://wikileaks.org/plusd/cables/10ASUNCION97_a.html [Fecha de consulta: 20 de octubre, 2016].

8 Informe Canal 4 Telefuturo: Escuchas telefónicas sin orden judicial se darán en caso de extorsión y secuestro - 26/11/2014 <https://www.youtube.com/watch?v=3Bkdspxae8> [Fecha de consulta: 20 de octubre, 2016].

investigative journalists, it was evidenced that the Public Ministry, through the The Office of the Comptroller of Computer Crimes, has held conversations for the purchase of surveillance software for this company⁹. It can not be confirmed that the purchase has been made so far.

Another form of violation of freedom of expression can be seen in cases of espionage that have affected several countries in the region, such as Paraguay. In these cases, women's communications with visibility and a certain degree of power were illegally monitored. to influence policies, as journalists and human rights activists.

State espionage is a violation of the right to freedom of expression, privacy - and when it affects journalists - the exercise of freedom of the press: all guarantees contemplated in the Constitution of the Republic.

Beyond that, from a gender perspective, surveillance is exercised in such a way that they end up controlling, silencing, intimidating or extorting women who challenge the status quo - the patriarchal state. As more women occupy public positions or offices where men have traditionally played a leading role, vigilance emerges as a tool to stop these advances in equity. It becomes the weapon of control of the expression, thought and movement of them.

The most notorious case of surveillance in Paraguay involved a journalist from the newspaper ABC Color, the highest-ranking newspaper in the country, which was spied on by high-level military commanders¹⁰ (specifically a military intelligence team with possible police support). According to the newspaper, the surveillance was carried out within the framework of some publications on corruption in the Armed Forces and its objective was to find out who was carrying out this journalistic investigation. Specifically, two cell phones were intercepted to access the call register, with the collaboration of an employee of the private telephone service used by the journalist. Despite all the evidence collected, to date there have been no significant advances by the Justice in this case.

On the other hand, the Public Ministry has technology to intervene in communications (including communications over the Internet) for the prosecution of punishable acts: telephone tapping systems and malwares¹. This high technology today is questioned for undermining the guarantee of due process by the Special Rapporteurs of Freedom of Expression of the UN and OAS, alleging that any violation of the privacy of any individual has a direct impact on democratic systems, as well as the right to freedom of expression, since it generates censorship or self-censorship.

In Paraguay, the Ministry of Interior was responsible for the purchase of national security face recognition software in 2018. The software was lately installed in the capital downtown¹¹ as well as in football stadiums¹². The official argument is that they wanted to

9 Disponible en <https://wikileaks.org/hackingteam/emails/emailid/249535>

10 Gobierno usó su sistema de inteligencia para espiar periodista <http://www.abc.com.py/edicion-imprensa/notas/gobierno-uso-su-sistema-de-inteligencia-para-espiar-periodista-1511976.html> [Fecha de de consulta] 27 de noviembre, 2017

11 La inteligencia artificial como aliada en la cruzada antiviolencia (July 12, 2018) <https://www.hoy.com.py/deportes/la-inteligencia-artificial-como-aliada-en-la-cruzada-antiviolencia>

12 Biometría y video-vigilancia en Paraguay. TEDIC (July 11, 2018) <https://www.tedic.org/biometria-y-video-vigilancia-parte1/>

offer higher security in crowded areas. We submitted a request for a report through the portal for access to public information and the response of this ministry was to deny us information on transparency and use of the same due to national security issues¹³.

In the TEDIC publication of 2019¹⁴ on the cameras of surveillance of facial recognition in the capital, it is described that the funds of Universal Services (FSU) that has as objective the promotion and extension of the telecommunication for rural and vulnerable zones, besides cost reduction in the provision of health and education services; they are financing the acquisition of a surveillance system from the Ministry of the Interior, under an agreement that has little to do with the fund's objectives.

Recommendations

For all the above, we will list a series of suggestions that could be taken into account when developing recommendations

Implement the appropriate regulatory framework to guarantee the transparency and accountability in the acquisition of surveillance technology.

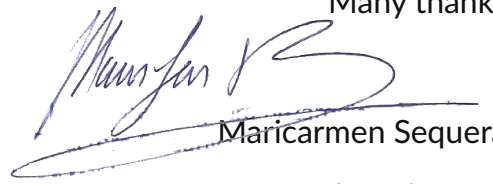
1. Implement the appropriate legislative framework to regulate and impose limits on the State usage of surveillance technology, which must include the establishment of necessary safeguards against abuse including:
2. specific regulation on the use of surveillance tools like hacking, malware, drones as well as biometric technologies, which incorporates the principles of necessity and proportionality.
3. Independent judicial authorization and oversight mechanisms.
4. Regulations that ensure that the use of private surveillance technology is auditable by oversight bodies.
5. Transparency regarding the general surveillance capabilities of the State and meaningful information regarding the scope and extent of the use of private surveillance technology.
6. Ensure that individuals that are targeted with private surveillance technologies are eventually notified and have access to a remedy.
7. Guarantee the existence of independent, impartial oversight bodies, endowed with the necessary powers to effectively audit, investigate and prosecute any abuse in the usage of surveillance technologies by State actors, this includes having absolute access to any information, installation or equipment necessary to carry out their functions;
8. Adopt human rights due diligence measures in their acquisition of surveillance technologies in order to assess and monitor potential Human Rights abuses and/or violations offered by the deployment of such technologies.
9. Monitor and impose appropriate penalties and guarantee the enforcement of those towards companies that deploy private surveillance technologies for their own business with the purpose of violating human and socio-environmental rights.

13 FOIA - TEDIC - Cámaras de reconocimiento facial en Asunción - Ministerio del Interior <http://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/19983>

14 La enajenación continua de nuestros derechos. Sistemas de identidad: Biometría y cámaras de vigilancia no reguladas en Paraguay <https://www.tedic.org/investigacion/la-enajenacion-continua-de-nuestros-derechos-sistemas-de-identidad-biometria-y-cameras-de-vigilancia-no-reguladas-en-paraguay/>

Thank you for your consideration, any questions or need clarification, do not hesitate to contact us.

Many thanks

A handwritten signature in blue ink, appearing to read 'Maricarmen S', with a long horizontal flourish underneath.

Maricarmen Sequera

Executive Director

TEDIC