PRIVACY INTERNATIONAL

Human Rights Committee, 117th Session, 27 June – 22 July 2016

The Right to Privacy in Argentina

Joint submission by Asociación por los Derechos Civiles and Privacy International in advance of the consideration of Argentina, Human Rights Committee, 117th Session

27 June – 22 July 2016

PRIVACY INTERNATIONAL

ADC por los Derechos Civiles

1. Introduction

Asociación por los Derechos Civiles (ADC) and Privacy International note the replies by the government of Argentina to the list of issues prior to the submission of the report, in particular in relation to the laws, policies and practices related to surveillance and protection of personal data.
Privacy International is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.
The Asociación por los Derechos Civiles (ADC) is a Buenos Aires-based independent NGO created in 1995, committed to the promotion of respect for human rights in Argentina and Latin America.[1]

The organisations have on-going concerns related to the respect of the right to privacy and data protection in Argentina. In this submission, the organisations provide the Committee with additional, up to date information to that contained in the briefing submitted to the Committee in advance of the adoption of the list of issues prior to reporting in December 2013.[2]

2. Communications surveillance

According to the National Intelligence Law[3], the surveillance of private communications can be conducted only if a court order is issued specifically for the case in question. Until December 2015, the only state body that was legally allowed for conducting the surveillance of communications was the Department for Interception and Captation of Communications (Departamento de Interceptación y Captación de las Comunicaciones, DICOM) under the orbit of the Public Ministry[4], but through the Decree N° 256/15 the Executive transferred DICOM to the orbit of the Supreme Court[5], which later replaced DICOM with the Directorate of Captation of Communications (Dirección de Captación de Comunicaciones, DCC)[6]. The DCC is going to be presided by a judge, appointed by a raffle, for the duration of one year.

1 See UN doc. CCPR/C/ARG/5, 13 July 2015.
2 Available here:http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/ARG/INT_CCPR_ICS_ARG_16054_E.pdf
3 Law Nº 25.520, art. 5, http://bit.ly/1bp2vWp
4 Law Nº 27.126, art. 17, http://bit.ly/1CLiBGU
5 Decree Nº256/15, http://bit.ly/1RI8wLr
6 "La Corte Suprema creó la Dirección de Captación de Comunicaciones del Poder Judicial" [The Supreme Court created the Directorate of Captation of Communications of the Judiciary], Centro de Información Judicial [Judicial Information Center], February, 2016, http://bit.ly/1Urvf5d

In February 2016, ADC raised concerns about certain aspects regarding the creation of the DCC. Of particular concern regarding the organizational structure of the DCC is the term of office of the Director, that lasts for only one year. This term does not give enough time for the appointed judge to get to know how the system works, bearing in mind that the knowledge of the communications interception system is not a prerequisite for the judges.[7]

Further, the intelligence agencies in Argentina operate with a great deal of autonomy with little effective oversight. Recent years have seen significant changes in the organisation of the intelligence services in Argentina. In July 2015, Decree 1311/2015 introduced the National Intelligence Doctrine, giving a framework to the Federal Intelligence Agency, regarding the organic and functional structure of the new Agency, as well as a new regime of professional staff, for its agents.[8]

However, with the change in administration following the presidential elections, in May 2016 Decree 656/16 abrogated the structure introduced with the National Intelligence Doctrine, and entitled the intelligence agency's Director to approve its own organisational structure, and to issue complementary and clarifying rules. This could lead to the creation of a new organizational structure under absolute secrecy, since the Decree does not require for it to be public, which would mean a major setback in the democratization process of the intelligence system.[9]

Although there is little to no information available regarding the surveillance practices and technical capabilities of the intelligence agencies, concerns remain that surveillance is carried in ways that violate individuals' right to privacy. Of particular concerns are reports of targeting of politicians, journalists and other activists. On 8th December 2015, the Citizen Lab -from the University of Toronto- published "Packrat: Seven Years of a South American Threat Actor", a research report showcasing an extensive malware, phishing, and disinformation campaign active in several Latin American countries, including Ecuador, Argentina, Venezuela, and Brazil.[10] Regarding Argentina, Citizen Lab spoke about the targeting of political figures in the malware campaign, such as the deceased prosecutor Alberto Nisman, and the journalist Jorge Lanata.

On 20th October 2015, former deputies Laura Alonso and Patricia Bullrich, filed a complaint for alleged illegal spying on journalists, politicians, public prosecutors and judges, carried by the Federal Intelligence Agency.[11] The

7 "Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones", February 2016, https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-de-comunicaciones/

8 "ADC researched about the training imparted to intelligence agents during 2015 in its report "Teaching to Surveil", "Educar para vigilar", December 2015, https://adcdigital.org.ar/wp-content/uploads/2016/01/Educar-para-vigilar.pdf"

9 At the beginning of 2016, the government appointed a new Director and Deputy Director of the Federal Intelligence Agency (AFI, for its acronym in Spanish), Gustavo Arribas and Silvia Majdalani, respectively. ADC, together with other organisations, raised concerns about the lack of training and expertise in intelligence matters of the appointed officials, which puts into question their professional suitability for such sensitive positions. Savoia, Claudio. "La interna de la ex Side arde con las designaciones polémicas", Clarín, 19 de diciembre de 2015. Disponible en: http://www.clarin.com/politica/Agencia_federal_de_Inteligencia_0_1489051101.html "ICCSI: Problemas en la designación de autoridades de la AFI", 30 de marzo de 2016. Disponible en: https://adcdigital.org.ar/2016/03/30/iccsi-problemas-designacion-autoridades-afi/

10 John Scott-Railton, Morgan Marquis-Boire, Claudio Guarnieri, and Marion Marschalek, "Packrat: Seven Years of

11 a South American Threat Actor", Citizen Lab, December, 2015, http://bit.ly/1U3dFkI
"Denuncian espionaje de la Secretaría de Inteligencia a jueces, políticos y periodistas" [Denounced spying by the Intelligence Agency to judges, politicians and journalists], La Nación, October, 2015, http://bit.ly/1OGTcm2

complaint was dismissed as false by the former Ministry of Defence, Agustín Rossi, and the former Director of AFI, Oscar Parrilli. Since its filing, there have not been new developments around the current state of the case and the investigation on the alleged illegal interception of communications.

3. Data protection regime

Argentina has strong privacy standards, rooted in the Constitution, as well as data protection laws with standards that compare to those in Europe, although the capacity of the National Directorate for Protection of Personal Data to enforce data protection law has been questioned.[12]

Law. N° 25326 (regulating the Protection of Personal Data) follows international standards, and it applies to the processing of personal data by private and public bodies. However, the law is largely unenforced in practice. The protective legal framework has two structural weaknesses:

- an excessive allowances in favor of the State regarding storage, processing and communication of personal data; and
- a weak controlling agency which depends on the executive branch.

Processing of personal data by state authorities

As for the first issue, Law 25.326 protects personal data including by prohibiting the processing and communicating personal data without the consent of the data subjects.[13] This prohibition seeks to prevent the unauthorized use of personal data by empowering individuals with the capacity to prevent third parties from using their personal data for purposes not authorized by them.

However, this principle, which underpins the protection of personal data, is largely absent vis-à-vis the State.

Section 5 of the law requires consent for processing of personal data but states that such consent shall not be deemed necessary when the data are "collected for the performance of the duties inherent in the powers of the State". This means that the guarantee of consent is useless when the data are collected by the State.

Similarly, Section 11 bans the communication of personal data if the data subject has not previously consented to it. However, this guarantee may be set aside when a law so provides, when the communication of data takes place directly between governmental agencies to the extent of their corresponding competencies.[14]

12 "El estado recolector" [The Collecting State], Asociación por los Derechos Civiles, September, 2014,
13 Law 25326, Sections 5.1 and 11.1.
14 See Law 25.326, Section 11.3.

Section 23 sets different regulation for the army, law enforcement agencies and the intelligence agency's personal databases, in accordance to the purpose for which the data is collected. The Section includes three different regimes.

Firstly, Army, security forces, police force or intelligence agency's databases of personal data that were created for administrative purposes; and databases which provide personal records to administrative and judicial authority are regulated by the general provisions of law 25.326.

Secondly, for databases of personal data, created for national defence or public security purposes, the law does not require the data holder's consent to process their personal data, provided that the following conditions are met:

> a) when established for lawfully assigned tasks on national defence, public security or prosecutions of criminal offences;
>
> b) the processing is limited to those cases and category of data that may be necessary for strict performing of such tasks;
>
> c) the files should be specific and established only for the task. It should be categorized, in accordance to its reliability.

Section 23.2 does not adopt the principle of consent for the processing of personal data, departing from the general rule. Although this solution seems –in principle- to be reasonable –since it would not be rational to request the consent of the data's subject when there is an on-going investigation- the wording of the section is too broad and allows state authorities to process personal data beyond what is strictly necessary and proportionate.. For example, the Spanish law –whose legislation was used as a model to draft the Argentine law- allow the processing of the data without the consent of the data subject, but states that there must be a "real danger"[15] for public security. Argentine law does not require the existence of a "real danger".[16]

Thirdly, Section 23.3 refers to personal data collected for police purposes. In this case, the provision only states that the data must be deleted when it is no longer necessary for the investigations that motivated its storage.

The wording of this provision raises concerns because of its indeterminacy, imprecision and broadness. Firstly, the term "necessary" does not enable that data subjects to know exactly when their data will be deleted. Secondly, it leaves the authorities a broad degree of discretion to decide when to delete or to retain the data. Finally, there is no obligation established to inform the data subject that his data has been deleted, so citizens could never know if their data were removed from the databases.

15 See Section 22.2 "Ley Orgánica de Protección de Datos de Carácter Personal" (Spain) available in http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750. The provision is similar to the former Spanish data protection law, used as a model for the Argentinian data protection law.

16 Cfr. Didier, Federico José "Data Protection and data processing for security purposes in compared legislation" available in http://www.tecnoiuris.com.ar/publicaciones/proteccion-datos-personales1.php

Through these broadly stated exceptions, Law 25.326 allows State agencies effectively to evade the bans on processing or communicating data without the owner's consent or only when strictly necessary and proportionate to the achievement of a legitimate aim. As a consequence, citizens are deprived of the main tool to protect the privacy of their data.

Limited capacity of the data protection authority

The functions of the National Directorate for the Protection of Personal Data (DNPDP, as per its Spanish acronym) set forth by the law and by the regulatory decree are extremely broad and are designed for an independent agency with financial self-sufficiency and with a structure necessary in order to perform such functions properly. Naming just some of such functions: advice for citizens, regulation of powers, control and registration of public and private databases and application of sanctions upon default, with has broad jurisdiction throughout the country.

In fact, the initial version of the Law 25.326 intended to create a monitoring agency with "functional autonomy" that would act "as a decentralized agency within the framework of the National Ministry of Justice and Human Rights." Such agency would have a director appointed by the executive branch, with the approval of the Senate, for a period of four years. However, these guarantees of functional autonomy and financial self-sufficiency were set aside when the executive branch promulgated the law partially by issuing the Executive Order 995/00, which kept the agency within the scope of the executive branch for financial reasons. Such decision was key to undermine the autonomy and effectiveness of the DNPDP.[17]

As ADC´s exposed in its research released in September 2014[18], the DNPDP has been denied the guarantees of autonomy and financial self-sufficiency set forth by the Law 25326 and has to operate on a low budget and a limited number of staff in order to perform activities that exceeded the actual institutional capabilities available. As a result of these constraints, the DNPDP has not been able to fully perform its functions and in particular has exercised limited control over the treatment and use of personal data by the state authorities.

We remark as a good sign that the new authorities of the DNPDP have shown a change in their criteria of control and enforcement, despite the structural weaknesses remain.[19]

17 Even though the Regulatory Decree 1558/01, Section 29.1 states that the "Director shall exclusively devote to his or her functions, shall perform his functions independently and shall not be subject to any instructions".
18 https://adcdigital.org.ar/wp-content/uploads/2016/01/The-Collecting-State.pdf page 6
19 http://www.jus.gob.ar/datos-personales/la-direccion-en-los-medios/2016/04/27/la-direccion-de-proteccion-de-datos-personales-inicio-una-investigacion-sobre-uber.aspx

4. Registration and identification of individuals: the use of biometrics technology

The risks to privacy and protection of personal data arising from poor implementation of the Argentinian data protection legislation are particularly concerning in relation to the growing use of biometrics technology.

The National Registry of People (ReNaPer) was established by law[20] in 1948; in 1968 during the military dictatorship, Argentina enacted a law that made it compulsory for all individuals to obtain an ID card.[21]

In 2011, by Executive Decree the Argentinian government established the Integrated System of Biometric identification – Sibios (Sistema Integrado de Identificación Biométrica). Sibios integrates the existing ID card database, Argentina National Registry of People (ReNaPer). It includes an individual´s digital image and fingerprint, civil status, and place of residence. Sibios' original aim was to facilitate the identification of citizens, enabling cross-referencing of data to support crime investigation and as a tool for preventive security functions. It can be accessed by the National Directorate of Immigration, the Airport Security Police, the National Gendarmerie and others law enforcement agencies, including provincial enforcement entities.

There is a range of human rights concerns related to Sibios.

Firstly, poor oversight of the intelligence and law enforcement agencies and the fact that a wide range of governmental institutions can access Sibios mean that the system could facilitate mass surveillance. Indeed, the government had advanced the idea that in the future this technology will be used to search for missing people through an integrated CCTV system and that even more personal information –such as DNA data and iris scans – may be included in this database.

Secondly, the risk that the Sibios database is used for purposes other than those originally envisaged without adequate safeguards. For example, Sibios was used to check voters' ID in the October 2013[22] and 2015[23] elections; the list of voters (padrón electoral) incorporated citizens' photographs, even though individuals' consent had not been sought for this use.

As the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has noted in a report to the Human Rights Council, in principle, data protection laws should protect information collected for one purpose from being used for another.[24] Further, this practice fails to respect the principle that every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their personal data.[25]

20 Law N° 13,482, Creación del Registro Nacional de las Personas, September 29th, 1948.
21 Law N° 17,671, Identificación, Registro y Clasificación del potencial humano nacional, February 29th, 1968.
22 https://adcdigital.org.ar/wp-content/uploads/2016/01/Si-nos-conocemos-mas.pdf (page 17)
23 http://www.unosantafe.com.ar/pais/La-Camara-Electoral-levanto-las-fotos-de-ciudadanos-del-padron-20150716-0096.html
24 UN doc. A/HRC/13/37, December 28th, 2009.
25 Human Rights Committee general comment N° 16 (1998) on the right to respect of privacy family, home and correspondence, and protection of honour and reputation (article 17).

The collection, treatment, and storage of photographs of citizens constitute an evident threat to the right to privacy. This is particularly so as the data collected can amount to sensitive personal data, such as (according to the definition in Law No. 25326) data which "may reveal race, ethnicity, or religion". Such practices can generate personal profiling that could potentially give way to the creation of databases with unlawful or discriminatory purposes.

Thirdly, weaknesses in the security of the database were identified, putting the personal data at risk of illegal access and use by third parties. In late 2013, following the October elections, a blogger identified a code that was then used by a programmer to set up a site that enabled images to be retrieved form the electoral registry.[26] Only when this failure took public knowledge through media, the photographs were taking down, as it happened again in 2015.

Article 9 of the Argentinian Data Protection Law sets standards to guarantee security and confidentiality of personal data, including prohibiting "to record personal data in files, registers or banks that do not meet the requirements of technical integrity and security."

The National Directorate for the Protection of Personal Data outlined mandatory security measures in Direction 11/2006[27], including basic, intermediate and critical levels of security, depending on factors such as the nature of the data and the risks involved.

The government failed to protect the data stored and inadequately accounted for the risks entailed by using biometric technology and digital identification systems. Through its failures to protect personal data, Argentina is not "ensur(ing) that information concerning a person´s private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant".[28]

26 See Ignoring repeated warnings, Argentina biometrics database leaks personal data, December 10th, 2013. Available at: https://www.privacyinternational.org/node/342

27 DNPDP, Disposition 11/2006. Medidas de Seguridad par a el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y privacos", September 19th, 2006.

28 Human Rights Committee general comment N° 16 (1988) on the right to respect of privacy, family home and correspondence, and protection of honour and reputation (art. 17).

5. Proposed Recommendations

Based on these observations, Asociación por los Derechos Civiles (ADC) and Privacy International propose the following recommendations to the Argentinian government:

- Take all necessary measures to ensure that its surveillance activities, both within and outside Argentina, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under surveillance; refraining from engaging in mass surveillance and adequately and transparently regulating information sharing with intelligence partners.

- Establish strong and independent oversight mandates with a view to preventing abuses and ensure that individuals have access to effective remedies.

- Ensure that the data protection authority is independent and appropriately resourced to fulfill its functions, including having the powers to investigate effectively reports of breaches of data protection.

- Review the Integrated System of Biometric Identification (SIBIOS) and limit the collection and use of personal data to ensure compliance with the right to privacy and data protection principles.