Submission to the Office of the High Commissioner for Human Rights

Introduction

This report is a submission by Asociación por los Derechos Civiles (ADC), a non-governmental, non-profit and non-partisan organisation based in Buenos Aires that promotes civil and social rights in Argentina and other Latin American countries. It was founded in 1995 with the purpose of furthering and strengthening a legal and institutional culture that guarantees people's fundamental rights, based on the respect for the Constitution and democratic values.

ADC wishes to provide information about specific technologies that introduce a pressing threat to the exercise and enjoyment of human rights in the context of peaceful assemblies. We do so by presenting concrete examples of these technologies being implemented in Argentina, while highlighting that there is a growing trend among States in the region to pursue the adoption of these technologies through public policies.

Constitutional grounds

Argentina has ratified a number of international human rights treaties with privacy implications. It has ratified the International Covenant on Civil and Political Rights (ICCPR), which 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 honour and reputation”. The Human Rights Committee has noted that states party 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].”[1]

Since 14 August 1984, Argentina is a signatory to the American Convention on Human Rights or “Pact of San José de Costa Rica” (the “American Convention”) which under Article 11 establishes that “No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.”

All of these treaties ratified by Argentina have been accorded the same legal weight as the Argentine Constitution under Section 75.22.[2]

[1] General Comment No. 16 (1988), paragraph 1.
[2] Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

In accordance with Article 21 of the ICCPR, the Constitution recognises the right to peaceful assembly in Section 14, where it states the right of every person "...to petition the authorities; enter, stay, transit and exit the Argentine territory; to publish their ideas through the press without prior censorship; to associate with useful aims...".

While the Argentine Constitution[3] does not mention the word 'privacy,' it does refer to 'private actions' in Section 19, which the Argentine Supreme Court has interpreted as the right to privacy. The section states: "The private actions of men which in no way offend public order or morality, nor injure a third party, are only reserved to God and are exempted from the authority of judges. No inhabitant of the Nation shall be obliged to perform what the law does not demand nor be deprived of what it does not prohibit."

In addition, Section 18 of the Constitution states: "the domicile may not be violated, as well as the written correspondence and private papers; and a law shall determine in which cases and for what reasons their search and occupation shall be allowed."

Regarding data, Section 43 reads: "any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of journalistic information shall not be impaired."

Areas of concern

Surveillance capabilities

As a result of the lack of transparency of Argentina's surveillance policies and practices, it is unclear what surveillance capabilities it currently has. Nevertheless, several reports emerged over the past few years documenting a system that differed substantially from what was indicated in the law. In July 2015, Wikileaks published 400GB of internal company material and correspondence from Italian surveillance company Hacking Team[4]. Whilst there is no evidence that Argentina purchased any equipment from Hacking Team, the leaked documents revealed that the government of Argentina had met with representatives from Hacking Team, and the company presented its products and services to various government bodies including Ministry of National Security, the National Criminal Intelligence Directorate, the Public Prosecutor, and the Complex Investigations Unit[5]. We are concerned these

[3] Available at: http://www.biblioteca.jus.gov.ar/argentina-constitution.pdf

[4] Asociación por los Derechos Civiles, La ADC alerta: software de interceptación y vulneración a los derechos humanos, August 2015. Available at https://adcdigital.org.ar/wp-content/uploads/2015/08/Software-de-interceptacion-y-DDHH.-Informe-ADC.pdf

[5] Asociación por los Derechos Civiles, La ADC alerta: software de interceptación y vulneración a los derechos humanos, August 2015. Available at

various government bodies have attempted to purchase such equipment from Hacking Team.

Mandatory SIM card registration

Mandatory SIM card registration violates privacy in that it limits the ability of citizens to communicate anonymously, thus curtailing the freedoms of assembly and association. It also facilitates the tracking and monitoring of all users by law enforcement and intelligence agencies. Research shows that SIM card registration is not a useful measure to combat criminal activity, but actually fuels the growth of identity-related crime and black markets to those wishing to remain anonymous.[6]

Law No. 25.891 from 2004 on Mobile Communications Services mandates the registration of all mobile phone users[7]. In April 2016, the Minister of Security announced that the Ministry would start a joint work with the Ministry of Communications to create a national registry of SIM cards in order to remove stolen phones from the market as well as to render them useless with the help of telephone companies[8].

Through the joint resolution 6-E/2016[9] published in the Official Bulletin on 10 November 2016, the Ministry of Communications and the Ministry of Security resolved the creation of the Mobile Communications Service Users' Identity Registry. The resolution is part of a Government action to fight complex and organized crime, based on the Decree 228/16[10], which declares the state of emergency of national security.

---

https://adcdigital.org.ar/wp-content/uploads/2015/08/Software-de-interceptacion-y-DDHH.-Informe-ADC.pdf

[6] Donovan, K.P., and Martin, A.K., The rise of African SIM registration: Mobility, identity, surveillance and resistance, Information Systems and Innovation Group Working Paper No. 186, London School of Economics and Political Science, London.

[7] Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

[8] ENACOM, Resolution 2549/2016. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/261599/norma.htm ; ENACOM, Se aprobó el procedimiento para el bloqueo de celulares robados, 20 May 2016. Available at: https://www.enacom.gob.ar/noticias/institucional/se-aprobo-el-procedimiento-para-el-bloqueo-de-celulares-robados_n1214; Telam, Fue detenida una banda que se dedicaba a clonar y comerciar de forma ilegal teléfonos celulares, 5 April 2016. Available at: http://www.telam.com.ar/notas/201604/142128-operativo-clonar-celulares-telefonos-patricia-bullrich.html

[9] Joint resolution of the Ministry of Communications and the Ministry of Security, 6-E/2016. Available at: https://www.boletinoficial.gob.ar/#!DetalleNorma/153684/20161110

[10] Decree 228/2016. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/258047/norma.htm

The resolution establishes that the National Entity for Communication (Ente Nacional de Comunicaciones, ENACOM) has to adopt the necessary measures "to identify all users of the Mobile Communications Service of the country in a Registry of Users of the Mobile Communications Service". The responsibility of this obligation is on the mobile operators, who must proceed to the designation of the telephone lines, that is, to relate each telephone number with the name of its owner. Operators must undertake the development –operation and administration of the registry– at their own cost and must store the information in a "secure, auditable and durable" way, being available to an eventual request from the Judiciary or the Public Prosecutor's Office.

Centralized biometric databases

Since 1968, Argentine citizens are obliged to issue a National ID card (DNI, Documento Nacional de Identidad) from the National Citizen's Registry (RENAPER, Registro Nacional de las Personas), an agency under the Ministry of Interior. In 2014, RENAPER issued Resolution 3020/14[11] in which it established that the only valid identification document is the new digital ID card, and that the citizen's biometric data will be digitised and collected into a unified database. Since November 2009, RENAPER has issued more than 41 million new ID cards. The database in question is the Federal Biometric Identification System for Security or SIBIOS (Sistema Federal de Identificación Biométrica para la Seguridad), created in 2011 by Executive Order 1766/11[12] under the Ministry of Security. The biometric data collected by SIBIOS consists mainly of fingerprints and facial features. The main users of SIBIOS are the Federal Police, the National Gendarmerie, the National Coastguard, the Airport Security Police, RENAPER and the National Immigration Directorate; furthermore, each province can sign an adhesion agreement to include their police force as a user and contributor. This was further broadened in 2017 –through the Decree 243/17– allowing any agency under the Executive or Judicial powers at the national, provincial and municipal levels to join as users of SIBIOS. Key concerns include the lack of requirement to obtain consent from the data subject when data is processed for the States' functions or legal obligations, the lack of a judicial order as a prerequisite to access and obtain citizens' information from the System, as well as the security threats that pose over centralized databases.

Facial Recognition Technology

In April 2019, the Government of the City of Buenos Aires (GCBA) deployed a face recognition system using the city's surveillance cameras (CCTV) already in place. The government licensed the software to an Argentine company, DANAIDE S.A., in order to use face recognition on 300 video cameras simultaneously, which are installed in subway and

[11] Available at:
http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/237457/norma.htm

[12] Available at:
http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm

train stations[13]. The aim of the system is to detect fugitives or people who has failed to appear before a court.

This technology has raised concerns for many reasons. Some of them are the following ones. Firstly, the system was not implemented by a law approved by the Legislature. Instead, the government issued an administrative resolution[14] without bringing the issue under a public and broad deliberation. Secondly, there were many cases of wrongful identifications, where innocent individuals were identified as fugitives and put under custody of the Police for hours or days due to a typo in the database with their ID numbers[15]. These mistakes were made because the database is not updated and checked for accuracy. Thirdly, no Privacy Impact Assessment (PIA) was carried out. This way, the legitimacy, necessity and proportionality of the measure could not be established by an independent review. Last May, the UN Special Rapporteur on the right to privacy visited Argentina and recommended that PIA should be made mandatory by law as a pre-requisite to the deployment of all surveillance technologies, including CCTV cameras with license plate, facial and gait recognition capabilities[16].

Open source intelligence (OSINT) and social media intelligence (SOCMINT)

Open source investigation refers to the use of techniques and technologies that allow or facilitate the collection of information that is publicly available, meaning it can be accessed without the need of login credentials (i.e. username and password) or special permissions. OSINT can be used to acquire text, images, videos, photos, audios, and even geolocation information. SOCMINT is the implementation of such techniques but on social media platforms.

The use of OSINT and SOCMINT techniques by law enforcement agencies is being adopted at a quick pace, often without proper human right impact assessments as well as safeguards for accountability and transparency.[17]

---

[13] Asociación por los Derechos Civiles, "#ConMiCaraNo: Reconocimiento facial en la Ciudad de Buenos Aires", May 2019, available at: https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

[14] Resolution 398/19 of the Government of the city of Buenos Aires, available at: https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PE-RES-MJYSGC-MJYSGC-398-19-5604.pdf

[15] Página 12, "Seis días arrestado por un error del sistema de reconocimiento facial", available at: https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

[16] "Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to Argentina", 6-17 May 2019, available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E

[17] Asociación por los Derechos Civiles, "Seguidores que no vemos", October 2018, available at: https://adc.org.ar/wp-content/uploads/2019/06/045-seguidores-que-no-vemos-10-2018.pdf

In the past few years, government agencies all over the world have turned to the use of OSINT and SOCMINT, from monitoring protests and movements, such as *Black Lives Matter* [18] and *Muslim Lives Matter*[19] in the United States, to incarcerating people because of their tweets like in Venezuela, where at least two dozen cases have been reported.[20] In Argentina, a new term has been coined for the activities carried out by security forces online: "cyber patrolling". Between 2016 and 2018, at least four people were indicted with criminal charges because of their tweets against the current President.

[18] American Civil Liberties Union, "The Government Is Watching #BlackLivesMatter, And It's Not Okay", August 2015, available at: https://www.aclu.org/blog/racial-justice/government-watching-blacklivesmatter-and-its-not-okay

[19] Boston Globe, "Boston police's social media surveillance unfairly targeted Muslims, ACLU says", February 2018, available at: https://www.bostonglobe.com/metro/2018/02/07/boston-police-social-media-surveillance-unfairly-targeted-muslims-aclu-says/9JUpzPmy8Tsr5RLxvCm61M/story.html

[20] Derechos Digitales, "Encarcelado por tuitear", June 2018, available at: https://www.derechosdigitales.org/12273/encarcelado-por-tuitear/