Issues of concern on the implementation of Article 17 and Article 19 of the ICCPR in Argentina

International Covenant on Civil and Political Rights (ICCPR)

Submission to the 110th Session of the Human Rights Committee for the attention of the Country Report Task Force on ARGENTINA

Submitted by Privacy International, United Kingdom, and Asociación por los Derechos Civiles, Argentina, December 2013

Introduction

This stakeholder report is a submission by Privacy International (PI) and Asociación por los Derechos Civiles (ADC) in Argentina. PI 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. It conducts research-based advocacy to promote changes in public policies and uses precedent-setting public interest litigation to challenge violations of civil and political rights (such as women's rights, the right to be free from discrimination, freedom of expression, access to public information) and to promote social and economic rights.

Privacy International and Asociación por los Derechos Civiles are submitting this report to inform the list of issues for Argentina's review before the Human Right Committee, specifically in relation to articles 17 and 19 of the ICCPR. This report discusses communications surveillance carried out by the Argentinian government as well as Argentina's failure to protect personal biometric data collected for identity registration.

Contact:

Carly Nyst
Head of International Advocacy
Privacy International
Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Telephone: +44 (0) 203 422 4321
Email: carly@privacyinternational.org
Website: www.privacyinternational.org

Ramiro Álvarez Ugarte
Director of access to information and privacy
Asociación por los Derechos Civiles
Córdoba 795 Piso 8 C1054AAG, Buenos Aires, Argentina
Tel.Fax (54 11) 5236.0555
Email: rugarte@adc.org.ar
Website: www.adc.org.ar

ICCPR provisions on the right to privacy and freedom of expression

The right to privacy is guaranteed under article 17 of the International Covenant on Civil and Political Rights (ICCPR), which affirms 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. Article 17(2) states that everyone has the right to the protection of the law against such interference or attacks.

The right to freedom of opinion and expression is guaranteed under article 19 of the International Covenant on Civil and Political Rights (ICCPR), which affirms that everyone has the right to hold opinions without interference, and to seek, receive and impart information and ideas of all kinds through any media and regardless of frontiers. Limitations to the right shall only be those that are provided by law and are necessary.

Background information on surveillance, freedom of expression and privacy

Over the last few months, the United Nations has provided a space to debate and discuss communications surveillance, privacy and freedom of expression and these issues are now at the forefront of the agenda across multiple UN agencies.

This development represents the most significant discussion of the right to privacy since CCPR General Comment No. 16 Article 17 (Right to Privacy) *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, adopted by the Human Rights Committee in April 1988. At the time the Human Rights Committee noted:

> "*At present the reports [of states parties] either say nothing about such legislation or provide insufficient information on the subject*,"

On communications surveillance, the comment presciently states:

> *"Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."*

More recently, Frank La Rue, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, noted the interrelation between the right to freedom of expression and privacy in a report[1] presented at the 23rd session Human Rights Council in May 2013. Following an in-depth analysis of the implications of communications surveillance for the exercise of the human rights to privacy and to freedom of opinion, the report concluded that there was a need to further study new modalities of surveillance. It recommended the revision of national laws regulating these practices to bring them into line with human rights standards.

In July 2013, following revelations about the operation of the National Security Agency of the United States of America, leaked by Edward Snowden, the High Commissioner for Human Rights, Navi Pillay stated:

> *"While concerns about national security and criminal activity may justify the exceptional and narrowly-tailored use of surveillance programmes, surveillance without adequate safeguards to protect the right to privacy actually risk impacting negatively on the enjoyment of human rights and fundamental freedoms."*

[1] A/HRC/23/40, 17 April 2013

The 24th Session of the UN Human Rights Council in September 2013 included a side-event on privacy in the digital age hosted by the governments of Germany, Norway, Austria, Hungary, Liechtenstein and Switzerland during which the International Principles on Application of Human Rights to Communications Surveillance were launched.

Following the decision of the Executive Board of the UNESCO, a session was held at Communication and Information (CI) Commission meeting during the UNESCO General Conference on “Internet related issues: including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society”. The resolution requests that the Director-General of the CI Commission prepare a comprehensive study of internet-related issues within the mandate of UNESCO, including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society.

In November 2013, the Third Committee of the General Assembly approved a resolution titled “Right to Privacy in the Digital Age”. The UN General Assembly voted unanimously the resolution on 18 December 2013. In this Resolution, the General Assembly is calling upon Member States to review their procedures, practices and legislation on the surveillance of communications, their interception and collection of personal data, including mass surveillance, with a view to upholding the right to privacy by ensuring the full and effective implementation of all relevant obligations under international human rights law.

Domestic laws and regulations related to privacy and freedom of expression in Argentina

Article 19 of the Constitution states that:

> *"The private actions of men that in no way offend public order or morality, nor injure a third party, are reserved only to God, and are exempt from the authority of the magistrates. No inhabitant of the Nation shall be compelled to do what the law does not order, or be deprived of what it does not forbid".*

Article 1071 bis of the Civil Code protects against unlawful intrusions into private life:

> *“[a]rbitrary interference in the lives of others, by posting pictures, broadcasting correspondence, mortifying others because of their habits or feelings, or in any way disturbing their privacy, and the act committed was not a criminal offense, will be forced to stop such activities, unless they have already ceased, and to pay a compensation that shall be equitably established by a judge, according to the circumstances; in addition, the latter may, at the request of the aggrieved, order the publication of the sentence in a newspaper or periodical, if this measure is appropriate for an adequate compensation.”*

Law No. 25.326 on the protection of personal data, enacted in October 2000 and includes articles vetoed by the Decree No. 955/2000 and the amendments introduced by the laws, Ley 26.343 and 26.388

Article 18 of the Constitution establishes that:

> *"the residence is inviolable, as are letters and private papers; and a law shall determine in what cases and for what reasons their search and seizure shall be allowed"*.

Article 14 of the Constitution guarantees the right of "publishing their ideas through the press without prior censorship"

Article 32 of the Constitution establishes that "the Federal Congress shall not enact laws that restrict the freedom of the press or that establish federal jurisdiction over it".

These protections of the right of freedom of expression are complemented by Article 13 of the American Convention of Human Rights and Article 19 of the ICCPR, which have been incorporated into the Constitution with "constitutional hierarchy" by article 75.22.

Other laws, including the National Defense Act of 1988, the Internal Security Act of 1991 and the Intelligence Act of 2001, regulate the intelligence and security services, but are largely considered to contain ineffective enforcement mechanisms.

Argentina's failure to comply with its obligations under articles 17 and 19 of the ICCPR

1. Communication surveillance

Security forces and intelligence agencies are often involved in surveillance on unions, journalists, political parties and social organizations, despite Article 4 of the National Intelligence Law,[2] which forbids political surveillance. In Argentina, political surveillance is a practice that has been common since the return of democracy in 1983; many political actors in the country believe that their phones are being tapped and their communications monitored.[3] Periodically, the press reports on privacy breaches and politicians complain. However, regrettably, many political actors see surveillance as an inevitable consequence of taking a prominent role in the nation's political life. For example, in May 2013 it was discovered that a journalist who had been working for Agencia Walsh, a left-leaning news organization, for ten years was actually a spy planted by the Federal Police.[4] On 21 May 2013, a criminal complaint was filed to the Federal Tribunal of Comodoro Py by human rights organisations and by left-wing political parties, which are members of the Truth and Justice Memory meeting requesting the infiltration orchestrated by the Federal Police into the news agency Walsh.

Since Argentina's last review, there have been a number of cases of undue interference with personal communications, some of which are mentioned below.

A. Targeted communication surveillance

One key case of targeted communications surveillance by the government was recently leaked by a group known as "Leakymails" (@leakymails). This group is thought to comprise current or former intelligence service operatives who are engaged in an internal struggle with other authorities. In this case, massive volumes of personal information, mainly personal emails by journalists, businessmen and politicians, were published on the Internet. There is an on-going criminal investigation taking place and even though no direct government responsibility has been found so far, the main hypothesis of the investigation is that the people responsible are current or former intelligence agents acting autonomously from higher authorities.[5]

Another example is the case of Adrián Ventura, a journalist from *La Nación* who was a victim of unlawful surveillance and who received civil damages for the illegal invasion of his privacy. In the case it was shown that the Navy had ordered its intelligence operatives to put Mr. Ventura under

---

[2] Ley 24.520, Ley de Nacional de Inteligencia, 3 de Diciembre de 2001

[3] *See* upcoming report on surveillance by ADC, to be published in 2014.

[4] *See* http://www.anred.org/spip.php?article6093.

[5] *See Juzgado Nacional en lo Criminal y Correccional Federal Nº 9, Secretaría Nº 17, en la Causa Nº 9.177/11 caratulada "N.N. s/Revelación De Secretos Políticos Y Militares".*

surveillance because of his reporting on a corruption scandal that involved high-ranking Navy officials.[6]

Recently, the Supreme Court has ruled in several cases in which citizens asked for information about themselves that was held by intelligence agencies. In those cases, the Court sided with the plaintiffs, holding in favour of access to information and rejecting broad claims about the need for secrecy made by the authorities. These judicial precedents are valuable in and of themselves, because they suggest that further inquiries may succeed in trumping secrecy and making intelligence agencies accountable. This is important in a context where the oversight mechanisms established by the Intelligence Act of 2001 are not operating effectively.[7]

B. Access to communications data

The law specifies that access to communications data or metadata must be authorized by a warrant issued by a Court of law. This requirement was established by the 2009 Supreme Court decision *Halabi.*[8] In this case, the Supreme Court held that requiring telecommunications companies to retain personal data was unconstitutional. Even though this is the legal standard currently in place, several press reports suggest that informal access of this kind of information takes place without judicial oversight.

C. Restrictions on anonymity

Law 25/891 on Mobile Communications Services mandates the registration of all mobile phone users. The law was introduced in April 2004 in response to a campaign launched by the father of a young man who was kidnapped and killed, and justified as necessary for security and law enforcement purposes.

Under the law, companies are obliged to register and retain personal information that will allow for "a clear identification of the subscribers" of mobile phone services. The law also requires companies to keep a list of devices that have been reported as lost or stolen, and mandates that they must "establish mechanisms to provide, immediately, every time and every day of the year, with no charge to the State, the information contained in this registry when required by a judge or a prosecutor". Companies are also required to cut off services to any device included on this list.

The Communications Secretariat is responsible for maintaining the National and Public Registry of Users and Clients of Mobile Communication Services (National Registry). This not only contains the personal information of all registered mobile phone users, but also whether they have been found guilty of any crimes.

Compulsory SIM card registration restricts the constitutional right to privacy, and the lack of protections within the National Registry and allows for the abuse of information supplied to companies and the State. Interference requires an element of proportionality and necessity, which is lacking in the arguments put forward by the government for setting up the National Registry to combat criminality.

D. Lack of judicial oversight

---

[6] See Juzgado Nacional en lo Contencioso Administrativo Federal No. 5. Caso Ventura, Adrián c. Estado Nacional EMGFFAA s/ daños y perjuicios. Decision of June 5, 2007, par. 3.

[7] *See* Ramiro Álvarez Ugarte, *Inteligencia, Democracia y Acceso a la Información*. LA LEY 2011-E, pág. 398 (2011).

[8] Halabi v. P.E.N., Supreme Court of Argentina, decision of Feb. 24, 2009.

The Intelligence Secretariat (SI), an agency that reports directly to the President, is the key player in government surveillance. Two investigations by journalists have revealed the way the SI works: it serves at the pleasure of the President, but it is a highly autonomous body with career officials under the public service system that survives all changes in the federal government.[9] The oversight mechanism is a parliamentary commission that operates in secret and, to a large extent, is completely ineffective.[10] The parliamentary commission does not make its meetings public nor publish public reports. Towards the end of 2012, ADC and another organization asked the parliamentary commission for basic information on its meetings, the production of reports ordered by law, and other matters. This request was not answered and the case went to court in 2012.[11]

From a legal point of view, the intelligence agencies operate with a great deal of autonomy. Despite the National Intelligence Law,[12] and the Interior Security Law,[13] the powers granted to the intelligence services are done so in vague and ambiguous terms and the only oversight mechanism is ineffective.

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

The National Registry of People (ReNaPer) was established by law[14] in 1948; in 1968 during the military dictatorship, Argentina enacted a law that made it compulsory for all individuals to obtain an ID card.[15]

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, Argentine National Registry of Persons (ReNaPer). It includes an individual's digital image and fingerprint, civil status, and place of residence. Sibios is aimed at facilitating 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, including provincial enforcement entities.

Poor oversight of the intelligence agencies and the fact that a wide range of governmental institutions can access Sibios means that the system could facilitate mass surveillance. Indeed, the government has 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. A private, but state-supported, initiative by the Argentine Football Association will use biometric data and the CCTV systems in football stadiums to monitor fans as they arrive and leave football matches to identify those who have been previously involved in violent episodes.

---

[9] Boimvaser, J. (2000) *Los Sospechosos de Siempre. Historia del espionaje en la Argentina*, Editorial Planeta and Young, G. (2006) *SIDE: La Argentina secreta*, Editorial Planeta. These investigations present a rather complete and uncommon picture of the way the Intelligence Agencies work in Argentina.

[10] Ugarte, J. M. (2012) *El control público de la actividad de inteligencia en América Latina*, Ediciones CICCUS, Buenos Aires

[11] http://www.ilsed.org/index.php?option=com_content&task=view&id=894&Itemid=1

[12] Ley 24.520, Ley de Nacional de Inteligencia, 3 de Diciembre de 2001

[13] Ley 24.059 Seguridad Interior, Actualizada según leyes 25520 y 25443, 17 de enero de 1992

[14] Ley No. 13.482, Creación del registro nacional de las personas, 29 de septiembre de 1948

[15] Ley No. 17.671, Identificación, registro y clasificación del potencial humano nacional, 29 de febrero de 1968

Issues of concern include “function creep” of the use of the Sibios database. The information gathered is already being used for purposes unrelated to Sibios’s original objectives. For example, Sibios was used to check voters’ ID in the October 2013 elections; the list of voters (padrón electoral) incorporated citizens' photographs, even though individuals’ consent had not been sought for this use.

As Martin Scheinin, the 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.[16] National security and law enforcement policies are usually exempted from these restrictions, but the use of photographs from the Sibios database for the electoral registry would not fall under this exemption. In addition, this context has failed 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 files”.[17]

It addition, a rights-affirming interpretation of Law No. 25,326 (regulating the Protection of Personal Data) deems images as sensitive information and, thus, grants them special treatment. Data which “may reveal race, ethnicity, or religion", among other criteria, are defined as sensitive. Such practices can generate social profiling that could potentially give way to the creation of databases with unlawful or discriminatory purposes.

The collection, treatment, and storage of photographs of citizens constitute an evident threat to the right to privacy. Since privacy is a constitutional right, any limitations must be subjected to a proportionality test. The improper operation of the electoral registry in the past, the fact the electoral registry database only includes around 30 per cent of voters and is merely intended to inform voters of where they were registered to vote, means the decision to collect further personal data on individuals is a disproportionate limitation.

The failures of the government were exacerbated following its failure to act after it was notified of certain weakness in the online database, which ultimately permitted a leak of personal data. In August 2013 in the first round of the elections, the government was first notified by a tech news agency of a weakness that permitted access to the database; however, the relevant authorities took no action. 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 from the electoral registry[18].

These examples illustrate that the government is failing to respect its international and national obligations to protect the right to privacy and ensure the protection of Argentinians’ personal data.

Article 9 of the Argentinian Data Protection Law (PDPL) states:[19]

---

[16] A/HRC/13/37, 28 December 2009

[17] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

[18] Pirlot de Corbion, A., *Ignoring repeated warnings, Argentina biometrics database leaks personal data, Privacy International*, 10 December 2013. Available at: https://www.privacyinternational.org/blog/ignoring-repeated-warnings-argentina-biometrics-database-leaks-personal-data; Villa, E., and Álvarez Ugarte, R., *Photos of Argentinians Up for Grabs,* Digital Rights, No.5, 22 November 2013. Available at: http://www.digitalrightslac.net/en/las-fotos-de-los-argentinos-al-mejor-postor/

[19] Ley 25.326. Protección de los Datos Personales (Incluye artículos vetados por Decreto Nº 955/2000 y las modificaciones introducidas por las Leyes 26.343 y 26.388), Octubre 2000

1. The person responsible for or the user of data files must take such technical and organizational measures as are necessary to guarantee the security and confidentiality of personal data, in order to avoid their alteration, loss, unauthorized consultation or treatment, and which allow for the detection of any intentional or unintentional distortion of such information, whether the risks arise from human conduct or the technical means used.

2. It is prohibited to record personal data in files, registers or banks that do not meet the requirements of technical integrity and security.

The National Commission for the Protection of Personal Data outlined mandatory security measures in Direction 11/2006[20], including basic, intermediate and critical levels of security, depending on factors such as the nature of the data and the risks involved.

The government's initial failure to consider privacy and data protection in the design of the electoral registry was then followed by poor practices in its management. The government then failed to protect the data it stored and inadequately accounted for the risks entailed by using biometric technology and digital identification systems.

3. Data protection

As innovations in information technology have enabled previously unimagined forms of data collection, storage and sharing, the right to privacy has evolved to encapsulate obligations around the protection of personal data.[21] A number of international instruments enshrine data protection principles and many domestic legislatures have incorporated such principles into national law.[22] Data protection is also emerging as a distinct human or fundamental right: numerous countries in Latin America and Europe have now recognised data protection as a constitutional right, and the recently adopted ASEAN Human Rights Declaration explicitly applies the right to privacy to personal data (Article 21).

Even though Law No. 25,326 (regulating the Protection of Personal Data) follows international standards in theory, in practice it is largely unenforced. The body charged with overseeing and applying the law is understaffed, incapable (or possibly unwilling) to undertake the duties the law assigns it.

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".[23]

---

[20] Dirección Nacional de Protección de Datos Personales , Disposición 11/2006, Apruébanse las "Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados". Bs. As., 19/9/2006 Publicación en B.O.: 22/9/2006

[21] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

[22] 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)

[23] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).