PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
28th Session – Argentina

The Right to Privacy in Argentina

Submitted by the Asociación por los Derechos Civiles and Privacy International

March 2017

Introduction

1. This stakeholder report is a submission by Asociación por los Derechos Civiles (ADC) and Privacy International (PI). The Asociación por los Derechos Civiles (ADC) is a non-governmental, non-profit 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 helping to strengthen a legal and institutional culture that guarantees the fundamental rights of the people, based on respect for the Constitution and democratic values. PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.[1]

2. ADC and PI wishes to bring concerns about the protection and promotion of the right to privacy for consideration in Argentina's upcoming review at the 28th session of the Working Group on the Universal Periodic Review.

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments. It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.[2]

4. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[3] As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection

1 For further information, please refer to collaborative research produced by ADC and PI, State of Privacy, last updated in November 2016. Available at: https://www.privacyinternational.org/node/981

2 Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

3 Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

of personal data.[4] A number of international instruments enshrine data protection principles[5] and many domestic legislatures have incorporated such principles into national law.[6]

Follow up to the previous UPR

5. In Argentina's previous review in the second cycle of the UPR, no express mention was made of the right to privacy in National Report submitted by Argentina, the report of the Working Group nor the stakeholder submissions.

Domestic laws related to privacy

6. While Argentina's constitution[7] 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."

7. 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."

8. 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."

International obligations

9. 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

4 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)

5 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)

6 As of December 2013, 101 countries had enacted data protection legislation. See: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN: http://www.biblioteca.jus.gov.ar/argentina-constitution.pdf

7 Available at: http://www.biblioteca.jus.gov.ar/argentina-constitution.pdf

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]."[8]

10. 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."

11. All of these treaties ratified by Argentina have been accorded the same legal weight as the Argentine constitution under Section 75.22.[9]

AREAS OF CONCERN

I. Communications surveillance

12. The National Intelligence Law, Law No. 25.520[10], regulates communications surveillance conducted by the State. The surveillance of private communications can be conducted only if a court order is issued specifically for the case in question.

13. Until December 2015, the only state body that was legally allowed to conduct 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[11], but through the Decree No 256/15 the Executive transferred DICOM to the orbit of the Supreme Court[12], which later replaced DICOM with the Directorate of Captation of Communications (Dirección de Captación de Comunicaciones, DCC)[13].

14. The reform of the intelligence system in Argentina had been long coming since the scandal that struck the Argentinian intelligence agencies in December 2014, and it was officially triggered in early 2015, when the then President, Cristina Fernandez de Kirchner, announced plans to disband Argentina's intelligence agency.[14] At the time of this announcement, ADC

8 General Comment No. 16 (1988), paragraph 1
9 See: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm
10 See Law No 25.520, Article 5. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm
11 Law No. 27.126, Article 17. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm
12 Decree No. 256/15. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257346/norma.htm
13 Centro de Información Judicial, La Corte Suprema creó la Dirección de Captación de Comunicaciones del Poder Judicial, 15 February, 2016. Available at: http://cij.gov.ar/nota-19854-La-Corte-Suprema-cre--la-Direcci-n-de-Captaci-n-de-Comunicaciones-del-Poder-Judicial.html
14 BBC News, Argentina to dissolve intelligence body after prosecutor death, 27 January 2015. Available at: http://www.bbc.co.uk/news/world-latin-america-30995722

published a timely report it had just undertaken over the dysfunctional, opaque intelligence system in Argentina. Key concerns including the use of the state intelligence apparatus for the benefit of the Presidency, the lack of oversight and transparency, and no accountability of budgets.[15]

15. The announcement of reform in early 2015 was welcomed by civil society despite concerns of the process of initiation reform thought a Presidential Decree. However, in early 2016 when the new agency was created – to replace DICOM – the DCC, concerns were raised about certain aspects of the newly created DCC. Of particular concern was the organisational structure of the DCC such as the very short 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. It also includes a very broad reference to the use of "data mining" technologies in order to collaborate with legal operators to obtain information from data bases to be used in the legal process, without any further explanations.[16]

16. In late September 2016, the Supreme Court created the Directorate of Judicial Assistance in Complex and Organized Crimes[17] (Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado) to assist judicial authorities in cases of illegal drug trade, human trafficking, kidnapping, money laundering, terrorism financing and crimes against the environment.

17. Within the new Directorate, the Office of Captation of Communications (Oficina de Captación de Comunicaciones, OCC) was established to replace the DCC. The new institutional position of the OCC -inside the Directorate- raise some concerns because it could lead to conceive the interception of communications as a mere auxiliary tool for investigations of crimes

18. In addition to the mandate granted previously to the DCC, the newly-created Directorate of Judicial Assistance in Complex and Organized Crimes has extended tasks of the OCC to include: developing new technological tools in order to improve the efficiency of the judicial proceedings, facilitating judges and prosecutors the access to information in order to detect common patterns on complex and organized crimes, and offering new tools for communication interceptions, among others.[18]

15 Asociación por los Derechos Civiles (2015) El (des) control democrático de los organismos de inteligencia en Argentina. Available at: http://www.adc.org.ar/wp-content/uploads/2015/01/2015-01-23-Informe-Final-Inteligencia.pdf

16 Asociación por los Derechos Civiles, Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones, 19 February 2016. Available at: https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-de-comunicaciones/

17 Supreme Court Agreement 30/2016. Available at: http://old.csjn.gov.ar/docus/documentos/verdoc.jsp?ID=100091

18 Article 4 of Supreme Court Agreement 30/2016

Lack of comprehensive and independent oversight of state surveillance

19. There are no requirement for the publication of reports on the surveillance activities of the intelligence agencies. However, under Article 13(9) of the National Intelligence Law, Law No. 25.520, intelligence agencies are required to submit annual reports on their activities to the Bicameral Commission on the Supervision of Intelligence Bodies and their Activities (thereafter Commission).[19] Since these reports are classified as confidential, it is not possible to find out if the oversight system works. Further, the powers of the oversight body to obtain relevant information is very limited. Under the Regulatory Decree 950/2002[20] the Commission must seek authorisation from the Secretariat of Intelligence, the very organ the Commission is meant to control and whose activity it has the mandate to oversee.

20. An investigation conducted by ADC revealed that the only report that the Committee has to submit to the Congress and the Executive, as mandated by Article 33.2 of the Act, is the annual report, and after consulting with various deputies in office for several years, ADC found that none of them had ever received a copy of that report.[21]

21. Furthermore, 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.

22. With the change in administration following the presidential elections, in May 2016 Decree 656/16 gave even more autonomy to the intelligence agency's Director, who can 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.[22]

Surveillance capabilities

23. 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.

19 Created in 1991 by the Internal Security Act No. 24.059
20 Articles 11 and 20 of Regulatory Decree 950/2002
21 Asociación por los Derechos Civiles (2014) Who's watching the Watchers? A comparative study of intelligence organisations oversight mechanisms in Latin America, pp. 12-13. Available at: https://www.privacyinternational.org/sites/default/files/Who%27s%20Watching%20the%20Watchers_0.pdf
22 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 of cials, which puts into question their professional suitability for such sensitive positions. Savoia, Claudio. See: Clarin, La interna de la ex Side arde con las designaciones polémicas", Clarín, 19 de diciembre de 2015. Available at: http://www.clarin.com/politica/Agencia_federal_de_ Inteligencia_0_1489051101.html ; Asociación por los Derechos Civiles, ICCSI: Problemas en la designación de autoridades de la AFI, 30 March 2016. Disponible en: https://adcdigital.org.ar/2016/03/30/iccsi-problemas-designacion-autoridades-afi/

24. In July 2015, Wikileaks published 400GB of internal company material and correspondence from Italian surveillance company Hacking Team.[23] 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.[24] We are concerned these various government bodies have attempted to purchase such equipment from Hacking Team.

Mandatory SIM card registration

25. Law No. 25.891 from 2004 on Mobile Communications Services mandates the registration of all mobile phone users.[25] 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.[26]

26. Mandatory SIM card registration violates privacy in that it limits the ability of citizens to communicate anonymously. 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.[27]

27. Through the joint resolution 6-E/2016[28] 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[29], which declares the state of emergency of national security.

23 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

24 Please see documentation published by Wikileaks in July 2015: https://wikileaks.org/hackingteam/emails/emailid/587154; https://wikileaks.org/hackingteam/emails/emailid/765194; https://wikileaks.org/hackingteam/emails/emailid/596983

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

26 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

27 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.

28 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

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

28. 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.

Reform of the Code of Criminal Procedure

29. Argentina has initiated a process of reforming its Code of Criminal Procedure in 2016.[30] The Bill presented for an open consultation raised some concerns as it proposes the introduction of special methods of investigation including: remote surveillance of computer equipment, surveillance through the means of capturing images and localisation and monitoring. The proponents of the Bill argue that these techniques of investigation are justified by the need to react appropriately and flexibly to the difficult task of combatting against organised and transnational criminal activity.

30. Whilst the introduction of the billnotes that the measures proposed would be implemented once submitted to a test of reasonability and for a specific time period, respecting the recommended standards of the UN, the Council of Europe, the Inter-American Court of Human Rights, and the European Court of Human Rights, some of the provisions fall short of those minimum standards. Activities that interfere with the rights to privacy and freedom of expression, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim and proportionate to the aim pursued.

31. In particular, we wished to express our concerns with regards to the introduction of hacking as a lawful investigative method within this proposal is particularly concerning. 'Hacking' presents unique and grave threats to our privacy and security. The default starting point should therefore be to question whether hacking can be a legitimate component of state surveillance.

32. If the government is to engage in hacking, its powers must be prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued. That law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the

30 Angulo, M., Reforma al Código Procesal Penal: el Gobierno busca limitar las excarcelaciones, 6 October 2016. Infobae. Available at:http://www.infobae.com/politica/2016/10/06/reforma-al-codigo-procesal-penal-el-gobierno-busca-limitar-las-excarcelaciones/

intrusion. It should be subject to periodic review by means of a participatory legislative process. Specific comments on the proposal include:

- There is a failure to provide a definition of hacking and merely refers to the use of 'software which enables or facilitate the remote access';
- There is a lack of necessary information as to who will be the relevant authority to conduct the 'remote access', the hack.

33. The UN Special Rapporteur on freedom of expression expressed his concerns over such offensive spyware and stated that "[F]rom a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter –inadvertently or purposefully- the information contained therein. This threatens not only the right to privacy and procedural fairness rights with respect to the use of such evidence in legal proceedings."[31]

Reported cases of surveillance

34. Although there is little to no information available regarding the surveillance practices and technical capabilities of the intelligence agencies, there have been several reported cases of surveillance.

35. Left-wing activists, however, still feel targeted by the government. Speaking to Privacy International[32], human rights lawyer Nicolas Tauber says he has encountered several cases of people who had received voicemail messages containing tapped phone conversations they had had in the past. He also said that there has been multiple instances of human rights lawyers who had been victims of burglary and only the electronic devices had been taken. He said his own office had been targeted and while the other lawyers, who do not work on human rights issues, had not had anything stolen, his own USB sticks had disappeared.

36. Further scandal erupted in early 2015 when Alberto Nisman, a prosecutor that had been carrying out the judicial investigation of Iran's involvement in the attack against the Argentine Israelite Mutual Association of Buenos Aires in 1994, was found dead in his apartment on 18 January. It is alleged that during a 10-year investigation, Nisman had gathered phone recordings that revealed an impunity deal between the Iranian and Argentinian governments in exchange for economic benefits.[33] Nisman worked closely with Jaime Stiuso during his investigations, and it is alleged that the intelligence services were involved in his death.[34]

31 A/HRC/23/40, paragraph 62
32 Interviews conducted in the course of 2015.
33 Bracesco, G., Argentina, Iran and the strange death of Alberto Nisman, 20 February 2015, Opinion, The Guardian. Available at: https://www.theguardian.com/commentisfree/2015/feb/20/argentina-iran-alberto-nisman-prosecutor-death
34 BBC News, Who killed Alberto Nisman?, Magazine, 28 May 2015. Available at: http://www.bbc.co.uk/news/magazine-32887939

37. Of particular concerns are reports of targeting of politicians, journalists and other activists. On 8 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.[35]

38. On 20 October 2015, former deputies Laura Alonso and Patricia Bullrich, led a complaint for alleged illegal spying on journalists, politicians, public prosecutors and judges, carried by the Federal Intelligence Agency.[36] Attached to their complaint they included a list of more than 100 names of individuals subject to surveillance including members of the Supreme Court, several federal judges and prosecutors, members of the opossion of the Krichner administration and dozens of journalists. The complaint was dismissed as false by the former Ministry of Defence, Agustín Rossi, and the former Director of AFI, Oscar Parrilli. Since its unveiling, there have not been new developments around the current state of the case and the investigation on the alleged illegal interception of communications including from Whatsapp, emails, mobile phones, and personal computers.

39. The arrest of suspected Colombian drug trafficker Henry López Londoño in Argentina provides a rare insight into the use of IMSI catchers to arrest individuals, a practice rarely documented. On 27 April 2012, Argentinian judge Norberto Oyarbide authorised a team of Colombian police officers to enter the country and track Londoño. According to Argentinian publication Diario Veloz, the Colombian police asked for permission to use equipment that would allow them to locate Londoño's phone but indicated that the equipment could in no way be used to hear or record phone conversations or messages.It is very concerning that Colombia could ask for an authorisation to track Londoño's phone without clarifying very specifically the type of equipment they were planning on using. IMSI catchers are too often dismissed as a tool of targeted surveillance, when in fact it is equipment—as the Argentinian intelligence services realised—that could be used to indiscriminately surveil anyone in its surroundings.[37]

II. Data protection regime

40. 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.

35 Scott-Railton, J., Marquis-Boire, M., Guarnieri, C., and Marschalek, M. (2015) Packrat: Seven Years of a South American Threat Actor, Citizen Lab, December 2015. Available at: https://citizenlab.org/2015/12/packrat-report/

36 La Nación, Denuncian espionaje de la Secretaría de Inteligencia a jueces, políticos y periodistas, 20 October, 2015. Available at: http://www.lanacion.com.ar/1838176-denuncian-espionaje-de-la-secretaria-de-inteligencia-a-jueces-politicos-y-periodistas

37 Blum-Dumontet, E., IMSI Catch 22: Understanding the Role of Spying Equipment in the Mi Sangre Case, 1 March 2017, Privacy International. Available at: https://medium.com/@privacyint/imsi-catch-22-understanding-the-role-of-spying-equipment-in-the-mi-sangre-case-23c27a001f7c

41. Currently, the protection of personal data in Argentina is regulated by 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. Amongst other concerns, the protective legal framework has two structural weaknesses: excessive allowances in favour of the State regarding storage, processing and communication of personal data; and a weak controlling agency which depends on the executive branch.[38]

42. Recognising the need to discuss a possible reform of the Law. N° 25326, the new Data Protection Commissioner of Argentina appointed in early 2016 initiated a public consultation with all stakeholders. This process of consultation has continued in 2017, and a draft proposal for reform was published as a means of collecting further feedback from external stakeholders. ADC and PI have saluted the open, constructive and consultative process undertaken by the Data Protection Authority and the Ministry of Justice of Argentina.

43. ADC and PI provided their respective extensive analysis of their assessment of the proposed law. Whilst we welcome the reform planned of the Data Protection Authority to ensure that it has the independence and autonomy both in terms of its mandate, function and operations, we remain concerned by various provisions of the proposed law. These include:

    - The need to redefine what constitute publicly accessible data for which lower data protection safeguards apply (Article 2);

    - The introduction of implied consent without clear guidance and conditions as to contexts in which implied consent would be sufficient (Article 12);

    - The inclusion of genetic and biometrics data as sensitive data to award them the highest level of protection (Article 2 and 16);

    - the possible broad interpretation of exceptions 1-3 of Article 36, and that it would permit any authority responsible for the processing of a public database to not have to comply with any of the rights of data subjects provided for by Chapter III and any of the safeguards provided for by Chapter II;

    - State agencies effectively permitted to evade the bans on processing or transferring 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 (Article 58).

38 See: Joint submission by Asociación por los Derechos Civiles and Privacy International in advance of the consideration of Argentina, Human Rights Committee, 117th Session. Available at: https://www.privacyinternational.org/sites/default/files/argentina_english.pdf

44. It is extremely important that Argentina takes necessary measures to ensure its data protection regime meets the highest standards and respects its national and international obligations given some concerning data breaches in recent years, and the deployment of ever expansive data-driven governance systems.

45. Electoral data: In late 2014, 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.[39] After this reached public attention through media reporting, the photographs were taken down. In July 2016, the Chief of Minister Cabinet issued the Resolution 166/2016[40] whereby the National Administration for Social Security (ANSES) would share its database (containing data such as name, identity card number, home address, phone number, email address, date of birth, and marital status) with the Secretariat of Public Communication, which is functionally reliant on the Chief of Minister Cabinet, in order to improve the government's communication strategy. The decision was contested by experts on data protection law[41] and members of opposition parties[42], who alleged that the data transfer does not align with the finality principle, because the data were collected for an efficient operation of the social security system, not for communication or public relations activities.

46. Sibios: In 2014, RENAPER issued Resolution 3020/14[43] 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[44] under the Ministry of Security. The biometric data collected by SIBIOS consists mainly of fingerprints and facial patterns. 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. Key concerns previously expressed 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.

39 Pirlot de Corbion, A., Ignoring repeated warnings, Argentina biometrics database leaks personal data, 9 December 2013. Privacy International. Available at: https://www.privacyinternational.org/node/342
40 Available at : https://www.boletinoficial.gob.ar/pdf/linkQR/TFNSL31FWGNOOUErdTVReEh2ZkU0dz09
41 See: http://www.ditc.com.ar/2016/07/29/sobre-el-acuerdo-anses-una-interpretacion-de-la-25-326-distinta-a-la-utilizada/
42 Politico Argentina, Sectores de la oposición cuestionan la utilización de bases de datos de la Anses, 26 July 2016. Available at: http://www.politicargentina.com/notas/201607/15546-sectores-de-la-oposicion-cuestionan-la-utilizacion-de-bases-de-datos-de-la-anses.html
43 Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/237457/norma.htm
44 Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm

47. Public transport electronic system: On 4 February 2009, by Decree 84/09,[45] the Executive launched a new travel card, the SUBE card (Sistema Único de Boleto Electrónico), under the oversight of the Secretariat of Transportation within the Ministry of Planning. Although one can buy the SUBE card without an ID card at kiosks throughout the various cities where the system is implemented, a user must register the card and link it to their personal data, such as name and surname, national ID card, gender, date of birth, email and phone number in order to consult the remaining balance of the card or the journeys made online, or to access the social tariffs available to specific groups like pensioners. There have been reports that the database is vulnerable, and unauthorised access has been demonstrated by a group called Anons.ar, members of Anonymous. The register of transactions was published online by the group.[46]

45 Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/150000-154999/150105/texact.htm
46 La Nación, Exponen en la Red los registros de viajes de la tarjeta SUBE, 30 January 2012. Available at: http://www.lanacion.com.ar/1444623-exponen-en-la-red-los-registros-de-viajes-de-la-tarjeta-sube

RECOMMENDATIONS

48. We recommend that the government of the Argentina to:

1. 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;

2. Establish strong and independent oversight mechanisms of the mandate and functions of the intelligence agency, and the newly established Office of Captation of Communications, with a view to preventing abuses and ensure that individuals have access to effective remedies;

3. Ensure that any reform of the Code of Criminal Procedure is in compliance with Argentina's national and international human right obligations and in particular the right to privacy;

4. To repeal the provision of Law No. 25.891 imposing mandatory retention of communication data and SIM card registration;

5. Ensure that anyreform of the Law. N° 25326 addresses the main shortfalls of the current legal framework to ensure respect and compliance with internationally recognised data protection principles;

6. Review data-driven initiatives including electoral registry,the Integrated System of Biometric Identification (SIBIOS), and SUBE card, and limit the collection and use of personal data to ensure compliance with the right to privacy and data protection principles.