



Access Now and Association for Civil Rights Joint-Submission to the United Nations Human Rights Council on the Universal Periodic Review 42nd Session Fourth Review Cycle

13 July 2022

About Access Now and Association for Civil Rights

Access Now is an international organization that works to defend and extend the digital rights of users at risk around the world. Through representation around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions and convenings such as RightsCon, we fight for human rights in the digital age. As an ECOSOC accredited organisation, Access Now routinely engages with the United Nations in support of our mission to extend and defend human rights in the digital age.¹

Association for Civil Rights 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.²

I. Introduction

1. The Universal Periodic Review (UPR) is an important United Nations (U.N.) mechanism aimed at addressing human rights issues across the globe. Access Now and Association for Civil Rights (ADC) welcome the opportunity to contribute to Argentina's fourth review cycle.
2. This submission examines the right to access to information, data protection and the right to privacy. Specifically, this submission raises concerns regarding the mass collection of personal data, the lack of public policies and safety measures to protect

¹ Access Now, About Us, 2022, <https://www.accessnow.org/>.

² Association for Civil Rights, 2022

citizens data, the increasing leak of public data, and the deployment of surveillance technology.

II. Follow up from previous review

3. During the third UPR cycle, Argentina received 188 recommendations, out of 175 were supported and 13 noted. The supported recommendations related to legal and general framework of implementation, universal and cross-cutting issues, civil and political rights, economic, social, and cultural rights, women's rights, and rights of other vulnerable groups and persons. It did not include recommendations related to privacy.
4. The third UPR cycle included recommendations on access to public information, including recommendations on the continued adoption of measures aimed at ensuring the effective regulation and implementation of the Law on Access to Public Information in All Branches of the State.³
5. A recommendation on freedom of opinion and expression focused on the intensification of efforts to consolidate a broad national multisectoral strategy to combat structural discrimination, including verbal expressions, against indigenous peoples, Afro-descendants and other vulnerable groups, considering their specific needs and capacities, through the empowerment of their rights and fair reparation mechanisms.⁴
6. Since the third UPR cycle in 2017, Argentina has made some progress in the implementation of the voluntary commitments. Argentina's National Plan on Human Rights (2017-2020) defined the Government priorities in the field of human rights in accordance with the Sustainable Development Goals and the recommendations from the universal periodic review, treaty bodies and special procedures mandate holders.
7. Argentina also advanced in the implementation of the National Mechanism for the Prevention of Torture, by completing the appointment of its members and establishing Local Mechanisms for the Prevention of Torture in eight provinces. Finally, the delegation emphasized that the President of the Republic had promoted that a wide and open debate be held in the Argentine Parliament on the decriminalization of abortion and the universalization of sexual education.

III. International, regional, and domestic human rights obligations

³ OHCHR (2017, November). Universal Periodic Review - Argentina. Matrix of Recommendations (Page 16). Available at <https://www.ohchr.org/en/hr-bodies/upr/ar-index>

⁴ OHCHR (2017, November). Universal Periodic Review - Argentina. Matrix of Recommendations (Page 6). Available at <https://www.ohchr.org/en/hr-bodies/upr/ar-index>

8. As of 19 February 1968, Argentina is a state party to the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR).⁵
9. As of 14 August 1984, Argentina is signatory to the American Convention on Human Rights or "Pact of San José de Costa Rica".⁶
10. Article 19 of the National Constitution of Argentina guarantees the right to privacy by establishing that "the private actions of men that in no way offend public order and morals, or harm a third party, are only reserved to God and exempt from the authority of magistrates. No inhabitant of the Nation will be forced to do what the law does not mandate, nor deprived of what it does not prohibit." Article 18 declares that "the place of residence is inviolable, as are epistolary correspondence and private papers; and a law will determine in what cases and with what justifications their search and occupation may be carried out."
11. Article 1 and 33 of the National Constitution of Argentina recognizes the right to access public information by adopting the republican system which implies the publicity of the government's acts. This right is also regulated by Law N° 27275⁷ which guarantees "the effective exercise of the right of access to public information, promote citizen participation and transparency of public management."
12. The right to the protection of personal data is enshrined in the Law 25.326.⁸ Article 9 of the regulation establishes that "the person in charge or user of the database must adopt the technical and organizational measures that are necessary to guarantee the security and confidentiality of personal data, in order to avoid its adulteration, loss, consultation or unauthorized treatment, and that allow deviations to be detected, intentional or not, of information, whether the risks come from human action or from the technical means used."

⁵ OHCHR, UN Treaty Body Database,
https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=7&Lang=EN.

⁶ United Nations Treaty Collection
<https://treaties.un.org/pages/showdetails.aspx?objid=08000002800f10e1>

⁷ Law 27275. Derecho de Acceso a la Información Pública.
<http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm>

⁸ Law 25.326. Ley de Protección de Datos Personales.
<http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>

13. As of 1 June 2019, Argentina is a state party of Convention 108 which guarantees the protection of individuals with regard to automatic processing of personal data.⁹

IV. The state of the right to privacy in Argentina

14. In the last couple of years there have been a number of incidents that increased the already fragile state of privacy in Argentina, in addition to the lack of public policies regarding the protection of personal data and information security, especially regarding mass data processing of residents and habitants of the Argentine Republic.

15. There is a reluctance from public authorities to share information regarding a number of vulnerabilities and the use of technologies. The lack of transparency and accountability not only aggravates the human rights situation in the country, but also prevents civil society and other stakeholders from conducting a proper assessment of the state of the right to privacy.

16. This scenario motivated a number of organizations, including Access Now and Association for Civil Rights, to request the suspension of the acquisition and development of new technologies that involve mass personal data processing.¹⁰

17. Some of the circumstances that motivated the request are the following:

IV. a. Public data leaks

18. In October 2021, it became known that the database of the National Registry of Persons (RENAPER) had suffered a security breach where information was extracted from national identity documents such as photos and procedure numbers. This last piece of information is used to carry out different acts before the public administration and could be used to commit identity theft.

19. Details about how the breach occurred are varied and contradictory. According to official communications,¹¹ the improper use of a password granted to the Ministry of Health of the Nation was detected, through which the system was accessed and the data was obtained. Although the Ministry of the Interior does not consider it a violation or data leak, quite the contrary, this represents a serious violation of the computer system.

⁹ Council of Europe. Chart of signatures and ratifications of Treaty 108. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=108>

¹⁰ Access Now. January 28, 2022. <https://www.accessnow.org/proteccion-datos-personales-argentina-medidas-urgentes/>

¹¹ Argentine Government. October 13, 2021. <https://www.argentina.gob.ar/noticias/el-renaper-detecto-el-uso-indebido-de-una-clave-otorgada-un-organismo-publico-y-formalizo>

20. Despite numerous attempts by civil society organizations and experts in the field, it has not been possible to obtain answers to clarify the facts. In particular, the security systems implemented and the policies for granting and managing access keys are unknown.¹² RENAPER's refusal to respond to requests for access to public information goes against national regulations and obscures the transparency with which the State should act.
21. This vulnerability adds to a long list of incidents in the last couple of years, making this already a structural problem. Among them, the incident known as "La gorra leaks",¹³ the leak of the database of the Institute of Social Security of the Armed Forces,¹⁴ the violation of the database of the National Migration Directorate and the leak of data from the Ministry of Health,¹⁵ to mention the most recent cases.

IV. b. Census 2022

22. For more than two years, civil society organizations have been expressing their concerns about the inclusion of the identity document data in the census that was carried out this year.¹⁶ Despite numerous communications with the authorities and reports prepared in conjunction with academic organizations, there was no confirmation as to whether said data will be removed from the census.
23. The census was finally conducted using the traditional method, which did not request citizens IDs, and optionally, online. This last option did request users' IDs, according to authorities, only to validate the identity of the person. That information was allegedly not stored nor linked to the data collected with the census form. This procedure was conducted despite warnings from civil society and experts in the field that explained the lack of need to request IDs and the dangers of creating a new point of failure given the bad record of security breaches in public databases.

¹² Asociación por los Derechos Civiles (ADC), November 8, 2021 <https://adc.org.ar/en/2021/11/08/adc-requests-renaper-to-explain-huge-data-breach/>

¹³ Argentine government. March 03, 2020. <https://www.argentina.gob.ar/noticias/sancion-la-policia-federal-por-una-filtracion-de-datos>

¹⁴ Argentine government. October 01, 2021. <https://www.argentina.gob.ar/noticias/iosfa-emitio-un-comunicado-sobre-la-filtracion-de-su-base-de-datos>

¹⁵ El Cronista. October 10, 2021. <https://www.cronista.com/economia-politica/el-ministerio-de-salud-denuncio-la-filtracion-de-informacion-que-involucra-a-mas-de-964-millones-de-datos/>

¹⁶ Association for Civil Rights, March 22, 2022 <https://adc.org.ar/2022/03/23/la-adc-pide-informacion-al-indec-y-expresa-su-preocupacion-sobre-la-falta-de-accesibilidad-y-la-proteccion-de-datos-personales/>

24. In addition, the email sent by the government with the link to fill the digital version of the census form included trackers from the company "mdirector.com", a private company dedicated to do digital marketing, in direct violation of data protection principles and practices.

IV. c. Outdated data protection law

25. The current Data Protection Law was enacted more than 20 years ago, before the Internet was a massive tool and data processing was carried out on a large scale by both the public and private sectors. Digitization has even accelerated as a result of the Covid-19 pandemic, driving many aspects of citizens' lives online and the development of public data collection applications for health purposes.

26. The law requires an urgent update to adjust to modern standards, guarantee the right to privacy of the inhabitants in this new context and protect critical public computer systems. Failing to accomplish this urgently could risk more violations of fundamental rights and the continuity of the adequacy granted by the European Union.

IV. d. Development and implementation of technologies without transparency and due safeguards

27. In recent years, national, provincial, and municipal governments have developed and implemented inherently dangerous technologies such as facial recognition technologies and thermal cameras.

28. In 2020 Access Now and ADC reached out to governments and companies regarding the use of surveillance technologies, receiving no or limited answers to our questions about the safeguards adopted, privacy impact assessments and use of personal data. The outcomes of this outreach were reported in "Made Abroad, Deployed at Home"¹⁷ where we expressed concerns about abuse of these technologies and the dangers they represent to human rights.

29. During the COVID-19 pandemic, governments also developed and implemented mobile applications to help contain the health emergency situation without consultation, transparency, nor independent audits to assess potential vulnerabilities.

¹⁷ Access Now. August 10, 2021. <https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf>

30. According to official statements, the data collected by the mobile app “Cuidar” developed by the national government to fight the pandemic, is now being used to prosecute criminals. In other words, it is being used for completely different purposes for which it was created, contrary to the principles of the right to personal data protection.
31. In summary, Argentine public authorities continue adopting technologies without security measures to avoid their harmful potential, open discussions or consultations in order to determine the necessity and proportionality of those tools, privacy impact studies, independent audits, nor transparency in the purchase and deployment.

VII. Recommendations

32. For the reasons stated and given the current context, we recommend Argentina
33. Commit to responding to civil society’s **access to public information requests**.
34. Create a procedure of **public consultations and independent audits** prior to the acquisition and deployment of new technologies.
35. Conduct **privacy impact assessments** of currently deployed technologies and for those that will be implemented in the future.
36. Implement **security mechanisms** for the protection of personal data.
37. **Update the data protection law** in accordance with the highest existing international standards.
38. Create mechanisms to **redress** those who have been affected by data breaches.
39. **Ban the use of mass surveillance technologies for public security** that inherently and disproportionately interfere with the right to privacy of citizens.
40. **Do not repurpose the data** collected from technologies deployed to combat Covid-19.
41. The UPR is an important U.N. process aimed to address human rights issues worldwide. Access Now and Association for Civil Rights are grateful to make this submission.

For more information, please contact: un@accessnow.org & adc@adc.org.ar