July 2022

Contribution to the Universal Periodic Review - Fourth Cycle, Republic of Argentina.

Organizations submitting this report

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.

Privacy International (PI) is a non-governmental organization in consultative status with ECOSOC. PI researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

Introduction

1. This stakeholder report is a submission by the Association for Civil Rights (ADC) and Privacy International (PI).

2. ADC and PI wish to bring concerns about the protection and promotion of the right to privacy for consideration in Argentina's upcoming review at the 42nd session of the Working Group on the Universal Periodic Review.

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, assembly and association(1).

4. Activities that restrict the right to privacy, such as surveillance, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued(2). 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 of personal data(3). A number of international instruments enshrine data protection principles and many domestic legislatures have incorporated such principles into national law(4).

Follow up to the previous UPR

5. In Argentina's previous review in the third cycle of the UPR, no express mention was made of the right to privacy in the 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 does not mention the word 'privacy'**(5)**, it does refer to 'private actions' in Section 19, which the Argentine Supreme Court has interpreted as the right to privacy**(6)**. 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 personal data, Section 43 of the Constitution reads: "any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or databases, 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 which enshrine the right to privacy. It has ratified the International Covenant on Civil

and Political Rights (ICCPR), which in 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 honor 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 [to privacy]".**(7)**

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 "Interamerican Convention") which under section 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.**(8)**

AREAS OF CONCERN

Surveillance technology.

12. During the cycle under review, Live Facial Recognition Technology has been deployed for surveillance by local authorities across the country. Córdoba**(9)**, Salta**(10)**, Mendoza**(11)** and Tigre**(12)** are cities whose local governments are using this kind of technology.

13. But the most relevant case is Buenos Aires, the capital city of Argentina. In April 2019, the government of the city of Buenos Aires rolled out the Fugitive Facial Recognition System. Around 300 cameras with facial recognition software were installed in streets and subway stations with the goal of detecting people subject to a warrant arrest. These cameras scan people's faces and compare them with biometric data -face images- provided by the National Registry of Persons (RENAPER) belonging to individuals included in CONARC, a national database run by Argentina's Minister of Security, containing a list of people wanted by the Police across the country.**(13)** City of Buenos Aires government was supposed to access only data from people in the CONARC's watchlist. However, it was reported that more than 10 million biometric data queries were made on around 7.5 million people, including politicians, social activists and journalists. Based on this information, in April 2022 the system was suspended by a judge although the government immediately appealed the ruling.**(14)**

14. Soon after the launching of the system, different violations of human rights occurred. Various people were misidentified as fugitives and were detained by the Police. The most serious case was Guillermo Ibarrola, an Argentine citizen who spent six days arrested in July 2019, wrongly accused of being a fugitive for robbery**(15)**. In 2019 too a woman included in CONARC's list for not appearing to provide testimony in court in 2008 was detained. She was released ten hours later because the judicial process had expired**(16)**. This and other cases happened due to mistakes in CONARC's database. People who never committed a crime were included and individuals whose criminal charges were dropped were never removed from the list as well.

15. Children's rights were also affected. The CONARC database contained data about child suspects such as their names, ages, national ID numbers, the alleged offense, and the location and the authority issuing the warrant. This private information was published online in CONARC's website and could be accessed by any person. As we mentioned before, this database feeds the Buenos Aires facial recognition system and as a result, children were also targeted by this technology. This results in a special concern with respect to international child protection standards. Because of their ongoing development,children and adolescents' facial features are constantly changing , so there is a greater chance of false positives. If such surveillance systems continue to be used, it must be ensured that they are not unfairly implemented to target children suspected of or charged with criminal offenses and are not used in a manner that violates their right to privacy and dignity**(17)**. After a letter from Human Rights Watch was sent, the national government restricted the access to CONARC's database and allegedly eliminated personal data of children. However, Argentina still lacks a proper legal framework to protect children's data **(18)**.

16. The former UN Special Rapporteur on the right to privacy stressed similar concerns in his report on his visit to Argentina in 2019. Regarding Buenos Aires' facial recognition system, he pointed out that the fact that it was "implemented without the necessary privacy impact assessment or the desirable consultation and strong safeguards is also a reason for concern"**(19)**. Also, the former rapporteur highlighted that public officials were unable to explain the necessity or proportionality of said system**(20)**.

17. Facial recognition systems are highly intrusive because they rely on the capture, extraction, storage or sharing of people's biometric facial data often in absence of explicit consent or prior notice. As such, its use by the Police

poses significant privacy and data protection issues. Further, the introduction of facial recognition technology in public spaces will inevitably result in the normalisation of surveillance across all societal levels and accordingly cast a "chilling effect" on the exercise of fundamental rights, such as our freedom of expression and peaceful assembly **(21)**.

Data protection legal framework

18. Data protection is regulated by Law 25.326, passed by the National Congress in 2000. From the beginning, the law showed two shortcomings. The first one was the excessive power given to public authorities to store, process and transfer personal data. Section 5.2.b exempts government bodies from having to obtain data subject's consent when collecting their personal data if they are collected to perform public functions.. Likewise, Section 11.3.C allows public agencies and departments to share data with each other without requesting consent from data subjects. Argentinian courts have ruled that these broad powers infringe on the right to privacy and data protection. In 2018 the Federal Court of Administrative Appeals ordered the national social security agency (ANSES) not to share the email and phone number of one of its beneficiaries with the Secretariat of Public Communication**(22)**. The court ruled that consent is the general principle to process personal data and legal exceptions must be narrowly interpreted. Also, it declared that the government cannot use data for purposes other than which it was collected for**(23)**.

19. The second shortcoming is the lack of enforcement capacity by the data protection authority. In March 2022, the General Audit Office -Congress audit institution- concluded that the Access to Public Information Agency (AAIP) -Argentina's data protection authority- didn't effectively guarantee the right to

data protection and its autonomy was affected by its legal and financial dependence on the Executive power**(24)**.

20. In addition to those problems, the data protection law is outdated to be able to deal with data exploitation in the face of the pervasiveness of digital technologies in our daily life. The law was passed twenty years ago before the popularization of phenomena like social media platforms, digital economy, surveillance technology, artificial intelligence or the use of technology for commerce, health or education**(25)**. To name some examples:

    - the law doesn't contain specific provisions to protect biometric data, weakening people's rights against biometric surveillance;

    - data subject's consent is never required to process data collected from public sources, enabling social media intelligence by law enforcement authorities;

    - there is no regulation on children's data protection, one of the most exposed groups to data exploitation by digital platforms**(26)**;

    - rights related automated decision making (including profiling) are not included;

    - requirements to undertake data protection impact assessments are missing from the obligation of data controllers and data processors;

    - and safeguards such as privacy by default/design are absent.

21. While Law 25.326 does contain provisions in line with human rights standards, it has fallen behind with respect to modern data protection legal framework (i.e. European Union's General Data Protection Regulation, California Privacy Rights Act or Brazil's General Personal Data Protection Law)**(27)**.

22. Since February 2019, Argentina is Party to the Convention for the protection of individuals with regard to Automatic Processing of Personal Data, also

known as "Convention 108". In October 2019, Argentina signed Convention 108+, a modifying protocol that incorporates modern data protection principles -.i.e. transparency, proportionality, accountability, data minimization and privacy by design- to address the challenges posed by digital technologies. The protocol has yet to be ratified by the Argentine Congress(28).

Security vulnerabilities in public databases

23. Several cases of data breaches of public databases were reported in the last few years. The most serious one is related to the National Registry of People (RENAPER), the Argentina's agency responsible for issuing citizens ID cards. In October 2021 an anonymous attacker claimed to have accessed RENAPER's database and obtained private information about 45 million Argentine citizens, including photos, full names, and home addresses. This information was put on sale online. To support their claims, the attacker shared ID photos from celebrities, politicians and even the president via Twitter. National authorities denied that a massive data breach had occurred and stated that it was a case of an unauthorized access -via an irregular use of an authorized account or a password steal(29). However, RENAPER didn't respond to a freedom of information request submitted by ADC, refusing to provide further information about the details of the incident.

24. In September 2020, the National Migration Directorate was attacked by the ransomware Netwalker group. It was reported that the attackers stole information about exits and entries to the country during Covid lockdown and Syrian refugees, among others. The government refused to pay the US$ 4 million ransom and the information was published online(30).

25. In January 2022, the Senate's website was attacked by the ransomware group Vice Society. More than 30,000 files with private information about employees, such as digital footprints and passports from employees and visitors to the Senate Office were stolen. The Senate took no actions, and finally data was published online in March 2022**(31)**.

26. In light of these cases -particularly the RENAPER case- ADC and other civil society organizations published an open letter in January 2022, calling for a moratorium in new deployments of initiatives involving massive data processing by the Argentinian State**(32)**. The letter highlights different requirements that the government should meet before considering acquiring and/or developing technology that may represent a serious risk to people's rights. With respect to improving databases' security we requested the State to conduct external security audits, the protection to independent security experts exposing security faults and the commitment to hold open and inclusive processes prior to any decision to deploy sensitive technology.

Mobile Phone Extraction (MPE) Tools

27. In recent years, police forces in Argentina have been using mobile device forensic extraction tools on a regular basis. Mobile phone extraction tools enable police and other authorities to download content and associated data from people's phones. This can apply to suspects, witnesses, and even victims of crime – often without their knowledge or consent. Mobile Phone Extraction (MPE) involves the use of 'push-button' extraction tools, retention and analysis of data extracted from a phone and cloud-stored data. Such technologies enable police and others to obtain device information, phonebooks, call logs, texts, videos and photos, audio files, emails and other information contained in the device**(33)**.

28. In 2021 ADC conducted research exploring the extent of the use of this technology in Argentina. We collected information -via freedom of information requests, interviews and articles in newspapers or companies' websites- about how law enforcement authorities and offices of Public Prosecutors across the country are increasingly relying on these tools and we were able to find out the information detailed below.

29. The most widely used tool in Argentina is the "Universal Forensic Extraction Device'' (UFED) developed by the company Cellebrite. UFED allows access to digital device data, by bypassing locks, performing advanced unlocks or performing logical/full file system/physical extractions**(34)**. UFED is used by different law enforcement authorities such as National Gendarmerie (military force with law enforcement duties among the civilian population and border guard), Airport Security Police (law enforcement agency created to protect and guard national public airports), Argentine Federal Police (national civil police force) and Argentine Naval Prefecture (coast guard) **(35)**.

30. At the provincial level, the use of UFED is spread in Public Prosecutor's Offices and the Police. In 2010, the National Ministry of Justice and Human Rights provided funding and equipment for the creation of forensic laboratories across the country**(36)**. An official document from the Ministry of Justice informed that Cellebrite UFED was one of the tools provided**(37)**. In October 2021, the Ministry of Justice and Human Rights allocated new funds for the creation and implementation of Regional Forensic Investigation Laboratories. Part of the funds was used to update the UFED licenses acquired by the public prosecutors' offices of different provinces**(38)**. Among the laboratories that benefited from this initiative are those of Entre Ríos, Mendoza, San Juan, San Luis, Formosa, Neuquén, Chubut, La Pampa, Corrientes and Misiones.

Journalistic sources report that there are more than 350 UFED licenses in Argentina, so it is to be expected that the cases mentioned here only show a small percentage of the total number of the acquisitions**(39)**.

31. The deployment of MPE technologies so invasive of privacy and personal data protection is done without the sufficient legal guarantees or necessary safeguards. The sensitivity of the information that our cell phones currently have requires that the practices by which the tasks of data extraction and analysis are carried out, as well as the regulations that allow the use of such information in a judicial process, be respectful of the rights of the accused. The extraction and analysis of a mobile device is one of the most privacy-invasive measures available and, therefore, when a judge orders it, he or she must apply strict criteria of necessity and proportionality to justify the measure.

32. Extraction of mobile devices may produce information relevant to the investigation, but also a large amount of personal information of the user that has nothing to do with the case. This poses the challenge as to how seizure and search warrants for information on electronic equipment should be issued to avoid a potential infringement of the right to privacy. Argentina doesn't have specific regulations to deal with electronic searches and provisions about searches in physical spaces are used instead. However, traditional rules governing physical searches are inadequately suited to the search for information on digital devices. To mitigate the impact on privacy of accessing a cell phone, the authorities should ensure that the analysis of the information is limited by the object of the investigation that motivated the order.

33. As for companies, because of their role in the development and sale of these technologies, efforts should be made to promote transparency in

procurement and development. People should know how these tools work and independent external audits must be conducted.

Health Data

34. The use of digital technologies for the provision and management of healthcare services is raising concerns for the protection of the right to privacy and other rights including the right to health(40). More and more people in Argentina are turning to computers, tablets or mobile devices as a way of accessing medical care and information(41). At the same time, the government is taking measures to have each patient's health information (medical history) stored in electronic format (electronic medical record).

35. According to Section 2 of the Argentina data protection law, health information is considered sensitive data and therefore as a data processor the government must take the utmost precautions to protect it. The reason why health data is awarded additional protection is that its processing carries a risk of discrimination for the data subject based on their health conditions as has historically been the experienced by people living with HIV and tuberculosis(42). There are also concerns about this data being used by third-parties like the private sector for commercial gains(43).

36. We are concerned about the Argentinian government's attempt to establish a Single System for the Registration of Electronic Health Records(44). This proposal - already approved by the Senate in 2020 - would lead to the creation of a single database with the health data of every user of both the public and private health systems. If the bill is approved by the Chamber of Deputies -the other house of the Congress- it will become law, setting up a single system whereby any medical treatment performed in public and private

health centres across the country will be digitised. This data would be accessed by the patient and medical practitioners when necessary.

37. The creation of a single health database poses a serious risk if it is not accompanied by adequate legal and technical safeguards including security measures. These concerns need to be understood in context. First, Argentina has a poor record of effectively safeguarding personal data and protecting people's rights. Information leaks or data hijackings through ransomware attacks suffered by the public sector give good reasons to be wary about the vulnerability of state databases as outlined in the section above on 'Security vulnerabilities in public databases'**(45)**. Unless additional safeguards are adopted for this new system, there is a possibility of this centralized information system being exposed to similar risks which would affect all residents' sensitive health information.

38. Secondly, prior instances of poor governance and accountability highlight the gap between the letter of a law and the reality of its enforcement which can be extremely wide. Beyond the government's promises to process health data with integrity and security, it remains to be seen whether the necessary financial and human resources are to be channelled, and to what extent there is a real understanding of and readiness to preserve data security**(46)**. Furthermore, the mere pledge of protecting data and ensuring security does not suffice in building public confidence in the absence of an effective and independent authority to monitor and enforce the law**(47)**.

39. In this sense, a part of the problem lies in the fact that the safeguards and security measures necessary for the effective protection of personal data, including health data, have not been updated. The Argentinian data protection law was passed in 2000 and has become outdated after twenty

years with the passage of time and new technological developments as outlined elsewhere in this submission(48). In addition to the need to update the current regulatory framework, given that the mere modernization of regulations does not guarantee their automatic compliance, it is also vital to create a culture of information security and for data protection authority to have the necessary expertise and resources to be able to supervise the observance of such standards.

40. In the absence of adequate legislation and policy, as well as sufficient safeguards to protect people and their data, there are serious concerns about the governments' plan to propose a single database containing the health data of the Argentinian population.

41. Since the outbreak of the Covid 19 pandemic in 2020, like many countries around the world, Argentina has relied on digital technologies as an important part of the strategy to combat it(49).

42. The government deployed several mobile apps and websites to enable citizens to access health information, perform self-diagnosis, obtain waivers during restrictions, receive test results, and manage vaccination documentation(50). ADC audited some of these government-provided applications and websites, and found security vulnerabilities that exposed citizens' personal data. These vulnerabilities were reported to the authorities but we didn't receive any response(51). This example reflects broader concerns about technological tools being deployed during the Covid-19 pandemic without adopting the necessary human rights due diligence and ensuring the effective enforcement of existing human rights obligations and responsibilities of governments and private entities.

Recommendations

43. We therefore recommend that Argentina:

a. To prohibit the use of facial recognition technologies for surveillance purposes in public spaces without the necessary safeguards in respect of Argentina's human rights obligations including:
    i. ensuring compliance with the principles of legality, proportionality, and necessity,
    ii. conducting data protection impact assessments whenever this system is deployed as it imposes a high risk to the citizens' fundamental rights and civil liberties,
    iii. the creation of strong and independent oversight bodies.

b. Update data protection legal framework to align with the international human rights standards, and to at least include:
    i. the obligation to conduct privacy and data protection impact assessment in cases where a type of processing is likely to result in a high risk to the rights and freedoms of people;
    ii. the designation of a data protection officer in cases where the processing is carried out by a public authority, sensitive data are being processed or there is a systematic monitoring of data subjects on a large scale;
    iii. the narrowing of the state power to transfer personal data without requiring consent to the data subjects;
    iv. the duty to adopt all the necessary measures to protect security and integrity of databases, considering the risk and sensibility of the data, previous record of vulnerabilities and the consequences of a potential

data breach for data subject's rights.

v. the right not to be subject to automated individual decision making, including profiling.

vi. putting in place a strong and independent data protection authority, with enough human and economic resources to perform investigations and conduct legal and technical analysis. This authority should also have sufficient normative powers to issue consequential sanctions to private and public institutions in case of violations to Argentine data protection law.

vii. Including new rules around the protection of children's data in alignment with guidance of the "best of the interests of the child" principle and the Committee of the Rights of the Child's General comment No. 25 (2021) on children's rights in relation to the digital environment.

    i. Based on the case of the Buenos Aires face recognition system, we particularly stress that the State should ensure that surveillance mechanisms, such as facial recognition software, that are deployed in the prevention, investigation and prosecution of crimes are not used to unfairly target children suspected of or charged with criminal offences and are not used in a manner that violates their rights.

c. Ratify the Modernised Convention 108+ For the Protection of Individuals with regard to the processing of personal data.

d. Refraining from acquiring, developing and/or deploying technologies with the goal of processing vast amounts of personal data until certain safeguards are implemented including:

i. strengthening the security of government databases and establish oversight by external auditors;
ii. carrying out open and inclusive consultations prior to the deployment of any technological innovation that may pose risks to individual and collective rights.

e. Publish and facilitate information on agreements with private companies for the acquisition of surveillance technologies, specifically mobile phone extraction tools.

f. Update legal framework on criminal investigations to include safeguard on the use of mobile phone extraction tools such as:
i. There needs to be a clear legislation, policy framework, or regulation for the extraction of data from mobile phones
ii. There needs to be independent oversight in place for the police use of MPE technology.
iii. There should be a requirement for police to obtain a warrant for searching the contents
iv. The police and law enforcement agencies should limit the data obtained from the mobile phones only to what is strictly necessary for direct lines of enquiry.
v. Police must delete these data when there is no legal reason to retain it, particularly if they are innocent of any crime
vi. Data must be held securely to prevent exposure of personal data as a result of loss of records, misuse or security breach.

g. Refrain from rolling out nationwide unique databases of individuals' health data as the proposed Single System for the Registration of Electronic Health

Records.

h. Develop and enforce a variety of technical and legal measures to be adopted by public health institutions and private providers of health services including:
    i. Conducting regular security audits and privacy assessments,
    ii. Adopting security measures such as encryption of data;
    iii. adopting organisational measures such as limiting the access of staff to data or the classification of data (for example, as strictly confidential/confidential/public) according to their level of sensibility;
    iv. Providing education to health systems staff on how to protect patients' privacy patients when handling their data;
    v. Engaging with the data protection authority and civil society organizations in order to collaborate to improve the current data protection practices in the health system.

i. Undertake an evaluation and audit of technological tools deployed during the Covid-19 pandemic, and take measures to ensure they are subject to comprehensive due diligence mechanisms.

Notes

1. 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.

2. 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.

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

4. As of August 2021, Nearly 140 countries and self-governing jurisdictions and territories around the world (118 UN Member States, and 20 self governing jurisdictions) have now adopted comprehensive data protection/privacy laws to protect personal data held by private and public bodies. See: Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2021 (August 30, 2021). Available at SSRN: https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

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

6. Ponzetti de Balbín, Indalia c/ Editorial Atlántida S.A. s/ daños y perjuicios, Corte Suprema de Justicia de la Nación, 11/12/1984 https://cdh.defensoria.org.ar/wp-content/uploads/sites/3/2018/01/ponzetti-de-balb--n.pdf

7. General Comment No. 16 (1988), paragraph 1

8. See: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

9. Policía de la Provincia de Córdoba, *Presentación del nuevo sistema integral de reconocimiento biomètrico y video vigilancia*, 17 October, 2019 https://www.policiacordoba.gov.ar/2018w3/Nota.aspx?id=4005

10. Que pasa Salta, *Así funciona el reconocimiento facial del 911 en Salta*, 16 May, 2019 https://es-la.facebook.com/quepasasalta/videos/as%C3%AD-funciona-el-reconocimiento-facial-del-911-en-salta/1353997684753890/

11. Los Andes, *Instalan en Mendoza cámaras que pueden reconocer en el acto a delincuentes*, 9 March, 2018, https://www.losandes.com.ar/policias-mendocinos-usan-software-de-reconocimiento-facial-para-encontrar-profugos/

12. Perfil, *Tigre presentó un nuevo sistema de reconocimiento facial con historiales de recorrido en la vía pública,* 13 May, 2019 https://www.perfil.com/noticias/policia/tigre-presento-neocenter-sistema-reconocimiento-facial-historiales-recorrido-via-publica.phtml

13. Gobierno de la Ciudad de Buenos Aires, *Rodríguez Larreta presentó el Sistema de Reconocimiento Facial De Prófugos: "El objetivo es que los vecinos estén más seguros"*, 26 April, 2019 https://www.buenosaires.gob.ar/jefedegobierno/noticias/rodriguez-larreta-presento-el-sistema-de-reconocimiento-facial-de-profugos

14. Página 12, *Espionaje ilegal en CABA: se usó el sistema de reconocimiento facial con políticos, periodistas y jueces*, 13 April 2022 https://www.pagina12.com.ar/414933-espionaje-ilegal-en-caba-se-uso-el-sistema-de-reconocimiento

15. Página 12, *Seis días arrestado por un error del sistema de reconocimiento facial,* 4 August, 2019 https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

16. Chequeado, *Video-vigilancia en Buenos Aires: la otra cara del control,* 28 May, 2020 https://www.chequeado.com/investigacion/video-vigilancia-en-buenos-aires-la-otra-cara-del-control/

17. Paragraph 119. Committee on the Rights of the Child General; *"Comment No. 25 on children's rights in relation to the digital environment*". 2021 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/053/43/PDF/G2105343.pdf?OpenElement

18. Human Rights Watch, *Argentina: Child Suspects' Private Data Published Online*, 9 October, 2020 https://www.hrw.org/news/2020/10/09/argentina-child-suspects-

private-data-published-online

19. Cannataci, Joseph A.; UN. Human Rights Council. Special Rapporteur on the Right to Privacy, *Visit to Argentina : report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci*, Paragraph 70, 27 January, 2021 https://digitallibrary.un.org/record/3901540?ln=es

20. Cannataci, Joseph A.; UN. Human Rights Council. Special Rapporteur on the Right to Privacy, *Visit to Argentina : report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci*, paragraph 72, 27 January, 2021 https://digitallibrary.un.org/record/3901540?ln=es

21. Privacy International, *Facial Recognition*, https://privacyinternational.org/learn/facial-recognition

22. "Torres Abad, Carmen c/ EN-JGM s/Habeas Data", Cámara Contencioso Administrativo Federal, July 2018, https://s3.amazonaws.com/public.diariojudicial.com/documentos/000/080/348/000080348.pdf

23. Marval, O'Farrell, Mairal, *Consent is Required for Personal Data Transfer,* 2 October, 2018 https://www.marval.com/publicacion/exigencia-de-consentimiento-para-la-cesion-de-datos-personales-13236&lang=en

24. Agencia de Acceso a la Información Pública (AAIP), *La Auditoría General de la Nación detectó incumplimientos y vulneración de derechos en el funcionamiento de la Agencia en su anterior gestión,* 21 March, 2022 https://www.argentina.gob.ar/noticias/la-auditoria-general-de-la-nacion-detecto-incumplimientos-y-vulneracion-de-derechos-en-el

25. Asociación por los Derechos Civiles (ADC), El RGPD y la ley argentina de Protección de Datos Personales, 14 June 2018, https://adc.org.ar/informes/analisis-comparativo-entre-el-rgpd-y-la-ley-nacional-de-proteccion-de-datos-personales/

26. 5 rights, Disrupted Childhood: the Cost of Persuasive Design , 2018 https://5rightsfoundation.com/uploads/5rights-disrupted-childhood-digital-version.pdf

27. Asociación por los Derechos Civiles (ADC), El RGPD y la ley argentina de Protección de Datos Personales, 14 June 2018, https://adc.org.ar/informes/analisis-comparativo-entre-el-rgpd-y-la-ley-nacional-de-proteccion-de-datos-personales/

28. Agencia de Acceso a la Información Pública (AAIP), *Argentina se suma al Convenio 108+*, 20 September, 2019 https://www.argentina.gob.ar/noticias/argentina-se-suma-al-convenio-108

29. The Record, *Hacker steals government ID database for Argentina's entire population,* 18 October, 2021 https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population/

30. Clarín, *Ciberataque a Migraciones: qué información robaron y publicaron los ciberdelincuentes,* 10 September, 2020 https://www.clarin.com/tecnologia/ciberataque-migraciones-informacion-robaron-publicaron-ciberdelincuentes_0_Pfe1OVNII.html

31. Clarín, *Publicaron los datos que le robaron al Senado en enero: son más de 30 mil archivos con información interna,* 13 March 2022, https://www.clarin.com/tecnologia/publicaron-datos-robaron-senado-enero-30-mil-archivos-informacion-interna_0_JLxR5q88lf.html

32. Asociación por los Derechos Civiles, OSC piden la suspensión del desarrollo e implementación de tecnologías de procesamiento masivo de datos personales, 28 January 2022 https://adc.org.ar/2022/01/28/osc-piden-la-suspension-del-desarrollo-e-implementacion-de-tecnologias-de-procesamiento-masivo-de-datos-personales/

33. Privacy International, *Mobile Phone Extraction,* https://privacyinternational.org/learn/mobile-phone-extraction

34. Cellebrite UFED, Product Overview, https://cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf

35. Asociación por los Derechos Civiles (ADC), *¿Quién revisa tu teléfono?*, 11 January 2022, https://adc.org.ar/informes/quien-revisa-tu-telefono/

36. Ministerio de Justicia y Derechos Humanos. Laboratorios Regionales de Investigación Forense, Agosto 2014 http://www.saij.gob.ar/docs-f/ediciones/libros/Laboratorios_Regionales_de_Invest._Forense.pdf

37. Ibid.

38. Ministerio de Justicia y Derechos Humanos, El Ministerio de Justicia invierte $125 millones para que los Ministerios Públicos Fiscales y de la Defensa mejoren los laboratorios de investigación forense, 12 october 2021 https://www.argentina.gob.ar/noticias/el-ministerio-de-justicia-invierte-125-millones-para-que-los-ministerios-publicos-fiscales

39. Asociación por los Derechos Civiles (ADC), *¿Quién revisa tu teléfono?*, 11 January 2022, https://adc.org.ar/informes/quien-revisa-tu-telefono/

40. Privacy International, *Digital Health: what does it mean for your rights and freedoms* https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms;
Privacy International, *Why we need to talk about digital health* https://privacyinternational.org/long-read/4674/why-we-need-talk-about-digital-health

41. iProup, Crece la demanda de médicos online: boom de la telemedicina en Argentina y qué prepagas evitan ir a una guardia, 9 April 2020 https://www.iproup.com/innovacion/12744-medicos-online-prepagas-como-es-el-boom-de-telemedicina-en-argentina

42. UN News, Workers with HIV-AIDS continue to face stigma, discrimination: ILO, 30 November 2021 https://news.un.org/en/story/2021/11/1106802;

    UN News, Marking World Tuberculosis Day, UN seeks to address stigma, protect patient rights, 24 March 2017 https://news.un.org/en/story/2017/03/553962-marking-world-tuberculosis-day-un-seeks-address-stigma-protect-patient-rights

43. Privacy International, *Why we need to talk about digital health* https://privacyinternational.org/long-read/4674/why-we-need-talk-about-digital-health

44. Proyecto de ley S-0733/17 https://www.senado.gob.ar/parlamentario/parlamentaria/387980/downloadPdf

45. The Record, Hacker steals government ID database for Argentina's entire population, 18 October, 2021 https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population/; Security Affairs, Netwalker Ransomware hit Argentina's official immigration agency, 6 September, 2020 https://securityaffairs.co/wordpress/107987/malware/netwalker-ransomware-argentina-immigration-agency.html; Data Breaches, "It took 6 hours to get access to every IT system" of Argentina's Senate – Vice Society, 22 March, 2022 https://www.databreaches.net/it-took-6-hours-to-get-access-to-every-it-system-of-argentinas-senate-vice-society/

46. Asociación por los Derechos Civiles (ADC), *Privacy is health*, March 2021 https://adc.org.ar/en/reports/privacy-is-health/

47. Ibid.

48. Asociación por los Derechos Civiles (ADC), El RGPD y la ley argentina de Protección de Datos Personales, 14 June 2018, https://adc.org.ar/informes/analisis-comparativo-entre-el-rgpd-y-la-ley-nacional-de-proteccion-de-datos-personales/ and Privacy is Health. A preliminary review of the legal framework and technological developments on electronic health records and telemedicine in Argentina, March 2021,https://adc.org.ar/wp-

content/uploads/2021/06/ADC-Privacy-is-health.pdf

49. Privacy International, *Tracking the Global Response to Covid-19* https://privacyinternational.org/examples/tracking-global-response-covid-19

50. Asociación por los Derechos Civiles (ADC), En caso de emergencia: descargue una app, 21 May 2020 https://adc.org.ar/2020/05/21/en-caso-de-emergencia-descargue-una-app/ and Asociación por los Derechos Civiles (ADC), En caso de emergencia: descargue una app Parte II, 22 December 2020 https://adc.org.ar/2020/12/22/en-caso-de-emergencia-descargue-una-app-parte-ii/

51. Consideraciones sobre la implementación de tecnologías digitales como respuesta ante la COVID-19. Asociación por los Derechos Civiles. https://adc.org.ar/2020/05/07/consideraciones-sobre-la-implementacion-de-tecnologias-digitales-como-respuesta-ante-la-covid-19/
Asociación por los Derechos Civiles (ADC). (2020). En caso de emergencia descargue una app - Parte II.https://adc.org.ar/wp-content/uploads/2021/03/202012-En-caso-de-emergenia-descargue-una-app-Parte-II_V2.pdf
En caso de emergencia: descargue una app. (2020, 21 mayo). Asociación por los Derechos Civiles. https://adc.org.ar/2020/05/21/en-caso-de-emergencia-descargue-una-app/