**Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to Argentina, 6-17 May 2019**

[Spanish](https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=S)

Buenos Aires, 17 May 2019

1. I would like to thank Government of Argentina for its invitation to visit the country from 6 to 17 May 2019, and for its generous cooperation. I thank the Ministry of Justice and Human Rights, in particular the Secretariat of Human Rights and Cultural Pluralism, and the Ministry of Foreign Affairs and Worship. I also thank the United Nations in Argentina for their support to my visit.
2. The views expressed in this statement are of a preliminary nature. My final findings and recommendations will be presented in my report to the United Nations Human Rights Council in March 2020.
3. During my visit, I assessed the situation of the right to privacy in Argentina. I studied recent reforms, existing mechanisms to prevent violations of the right to privacy and heard concerns expressed by civil society organizations, experts and other actors. I also received useful information on best practices being carried out in Argentina.
4. As part of my fact-finding mission, I visited Buenos Aires, Comodoro Rivadavia and Rawson, in Chubut province. I met with senior officials of the Argentinian Government at the national and provincial levels, the legislature, law enforcement, national and provincial data protection authorities and human rights institutions, United Nations entities and non-governmental organizations. I would like to thank all of them for their time and their valuable inputs received both before and during the visit.

**Surveillance**

1. During my visit, I have observed a general lack of trust on Argentina’s intelligence services. Possibly due to Argentina’s past, a strong culture of opacity and some highly-publicized cases of illegal surveillance, many persons in Argentina suspect that they are personally under surveillance and that intelligence agents act without oversight or supervision.
2. Since 2015, Argentina gave the exclusive capacity to carry out interceptions of communications to a subsidiary body of the Supreme Court - DAJuDeCO.
3. In December 2015, the Government transferred the Legal Assistance Directorate for Complex and Organized Crime (DAJuDeCO) from the Public Ministry to the Supreme Court. After three years of reforms carried out since then it now results that:
	1. DAJuDeCO is the only body existing in Argentina with the executive authority to carry out interceptions of communications and it only does so at the request of both federal and provincial judges and prosecutors,
	2. Requests for interceptions by all Argentinian intelligence agencies and police forces must be channelled through judges who must approve surveillance warrants before interceptions can be carried out at the request of or by DAJuDeCO;
	3. Presently the total number of lines intercepted per month peaks at 6.000 out of which only 69 are direct interceptions listened in to by DAJuDeCO while all the rest are not listened to live but are executed by service providers. The vast bulk of interception content is therefore never listened to by DAJuDECO officials but is automatically recorded onto CDs without human intervention and then distributed to the authorities indicated in the surveillance warrant. In 2018 the total number of lines intercepted was 41.0000[1](https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E" \l "_ftn1).
	4. I am convinced that the safeguards put in place at DAJuDeCO are adequate and preserve the privacy of the individual. The organization has presented evidence that, both in terms of personnel working there as well as institutional design and work protocols they are trying their best to minimize human intervention, ensure that personal data is being protected and that the only people have accessing to the content of the interceptions are the legal beneficiaries of a surveillance warrant issued by the judiciary;
	5. The level of transparency in many matters at DAJuDeCO is quite exemplary and class-leading. One further step required would be to put their Annual Reports on-line. (If they are on-line we could not find them but are grateful for the paper copies we have received).
	6. However, the technology being used is quite an antiquated one. Should newer interception technology be procured, enabling not only the interception of landlines and mobile conversations but, for example  also the use of malware on mobile phones, both the institutional design and the safeguards deployed need to be revisited accordingly.
	7. The above being said I also find that Argentina’s surveillance system also has several inherent vulnerabilities resulting from: (a) over-use of interceptions, treated as an ordinary measure of investigation for all types of crimes and not as a last-resort one for serious crimes; (b) weak controls in the chain of custody over accessing the content of the interceptions[2](https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E" \l "_ftn2); and (c) lack of an independent control over the use of interceptions.
	8. It is my strong belief that all security forces in Argentina as well as assisting bodies (e.g. DAJuDeCO) should invest serious effort towards increasing their transparency where this has not been already achieved. This can be done in multiple ways, including through publishing online their annual activity reports, where these are available as well as any other relevant information which could help citizens better understand the types of activities being carried out by these organizations and the type of safeguards they have put in place to protect human rights.
	9. In this context, I would like to express my strong concerns over the overreaching nature of the regulatory framework in what concerns classification of information related to the intelligence function of the Argentinian security forces. By making all information related to their structure and activities secret the law de facto prevents them from putting in place adequate transparency policies which would help contribute to strengthening public trust.
4. It would appear that Argentina’s intelligence services and police do not possess advanced technical capabilities required to carry surveillance and there is no way that Argentina could be fairly described as “a surveillance state”. Indeed it should be emphasised that this is very far from being the case. On the other hand, those privacy-intrusive technologies are easily available and a case for their being proportionate measures in fighting organised crime and terrorism could easily be made.  It is therefore essential that Argentina prepare itself immediately for such an eventuality by introducing the right safeguards especially in the oversight of surveillance capabilities and intelligence.
5. An essential element of oversight already exists in the important work carried out by the Bicameral Commission on Intelligence of the Argentine legislature. That however is insufficient insofar that the Commission does not use its legal ability to its full or have the resources to fully audit, in-depth the conduct of a specific case, and does not have full access to the contents of a case file. The Special Rapporteur is therefore recommending the creation of a new independent full-time body whose work should complement that of the Bicameral Commission (see recommendations below).
6. Several cases of illegal surveillance have been brought to my attention. In one of them, in 2015, an agent of AFI followed 26 members of an indigenous Mapuche community and of an anti-mining movement for several months, worked together with two police officers, and then shared the information he had collected with prosecutors of Chubut province. While the case is still *sub iudice*, the nature and intensity of the surveillance, the fact that it may have been based on grounds prohibited by law (race, ideology, membership of social organization) and targeted a vulnerable community, and the willingness of police officers and justice system officials to accept the product of the surveillance, which may show trends found elsewhere in the country, are elements of great concern. I encourage the Government to immediately increase the resources allocated to protecting the welfare and privacy of these indigenous peoples as well as take all necessary measures to hold all perpetrators accountable, compensate the victims, and ensure that the violation does not occur again.

**Criminal databases**

1. On 22 April 2009, the Government presented the Consulta de Rebeldías y Capturas (CONARC), an online database that allowed all law enforcement and justice system officials across the country to confidentially access the list of all persons that had an arrest warrant in Argentina.
2. On 15 November 2016, the Government issued Resolution 1068 – E/2016, making the list of persons with an arrest warrant accessible online to the public. On its article 1, the Resolution states that only adults sought for serious crimes would be included. In fact, the name given to the database is “LOS MAS BUSCADOS” (“THE MOST WANTED”), giving an idea of the danger that the persons in the database pose to society.
3. However, I have observed that the database, which is fully available for download:
	1. As of 16 May 2019, it contains a list of 46,479 persons.
	2. The list provides the name and age of the wanted person, the father’s and mother’s names and surnames, national ID number (DNI), the type of offence they are wanted for and the institution and authority issuing the warrant. While the ID number could be an important tool for authorities to carry out an arrest, I do not see how it could be considered necessary to release this information to the public.
	3. The list contains persons wanted not only for serious crimes, such as rape, extortion or homicide, but also for others such as simple theft (3,259 files). On 13,703 files (29.5% of the total), there is no information on the type of offense for which the person is wanted.
	4. The list contains 61 children. It is particularly disturbing that juveniles are included on the public database, which would be difficult to justify as being in the best interest of the child as obliged by the Convention of the Rights of the Child (article 3.1), ratified by Argentina on 4 December 1990. The convention also recognizes the right of any child accused of having infringed penal law “to have his or her privacy fully respected at all stages of the proceedings” (article 40.b.2.vii), which would be incompatible with publicizing arrest warrants against juveniles.
	5. The database contains multiple errors: as an example, two persons are listed as being 2 and 3 years old, and wanted for assault and robbery. Due the potential infringement of a person’s right to privacy, the accuracy of such a list has to be scrupulously ensured.
	6. Another concern I have received is that the list is not properly updated, so warrants that could be over a decade old are still found on the public database. Even though the database is refreshed every morning at 7 a.m. with the data provided by criminal courts across the country, not all courts revise the information they feed to the database, leading to errors and discrepancies.

**Privacy and children**

1. I have noted with concern information on two cases where the right to privacy of girls was violated. On the first case, a 12-year-old girl became pregnant as a result of sexual abuse in the province of Jujuy. In January 2019, after being attended at the Dr. Guillermo Paterson Hospital and her pregnancy being confirmed, she and her legal tutors decided to carry out an abortion. However, the hospital staff refused to comply, and the case became the subject of public debate on the media. The Catholic Church and anti-abortion groups publicly opposed it, the Governor stated that the Criminal Code of Argentina allowed abortion in that case and said that he had given the order for the abortion to be done. At the Provincial Maternity Ward of Dr. Héctor Quintana, the medical team performed a caesarean section and generated a live birth. The provincial Minister of Health publicized in provincial and national media, without the consent of the girl or her family, the clinical picture of the patient, the medical procedure to be carried out, the time of the surgical intervention and the conditions of her health before and after the therapeutic action.
2. Also in January 2019, "Lucía" an 11-year-old girl from the province of Tucumán and her legal tutors decided to carry out an abortion at a public hospital after she had been victim of sexual abuse. However, the provincial health system delayed the interruption of pregnancy for 5 weeks, and failed to protect the girl’s right to privacy. The medical staff, together with the Secretary of the Health System of the Province of Tucumán and the Director of the Hospital de Este revealed sensitive data on the girl's life, with information on her health and clinical history.
3. The City of Buenos Aires is implementing several initiatives to protect the rights of children in the digital environment, including the right to privacy.
4. On 15 December 2016, the City of Buenos Aires passed the 5.775 Law against “Grooming”, which obliges the public institutions of the city to design and implement awareness raising and capacity building activities for children, parents and professionals for the prevention of grooming. Since the passing of the law, over 25,000 cases have been brought to the attention of the authorities.
5. In the last five years, the City’s Ombudsperson Institution has implemented a programme called "Conectate seguro" (Connect safely), in order to promote the safe use of data by children. In 2018, about 3500 children participated.

**CCTV and facial recognition**

1. Since 2016, the Government of the City of Buenos Aires has significantly increased the network of surveillance cameras in the city as an attempt to improve security and prevent crime. Currently, there are over 7,000 cameras installed in the City of Buenos Aires and operated by the City’s Ministry of Security. Examples in other cities have shown that the improvement of public security by the installation of surveillance cameras is questionable in some instances and justifiable in others. The justifiability of such a system, its legitimacy, necessity and proportionality should have been established by a Privacy impact Assessment (PIA) which does not seem to have been carried out.
2. On 25 April 2019, a facial recognition system was activated on 300 of the City’s surveillance cameras. The system is connected to CONARC, the public database of persons wanted by justice, composed by 46,000 files. My concerns regarding CONARC (see paragraph X) also apply here. I am aware of the need to arrest persons who are suspected of having committed crimes and bring them to justice, but I fail to see the proportionality of installing a technology with serious privacy implications for searching a list of 46,000 persons that includes non-serious crimes and is not carefully updated and checked for accuracy.
3. The fact that facial recognition is being implemented without the necessary PIA as well as the desirable consultation and strong safeguards is also a reason of concern. The Government has passed low-level regulation regarding biometrics but not detailed legislation for the use of facial recognition: Resolución Nro. 398/MJYSGC/19.
4. The city of Comodoro Rivadavia, a city of around 180,000 inhabitants in Chubut province, has a network of 120 cameras, which the Government plans to increase up to 250. The Government plans to give the network facial recognition capabilities in the coming months, in order to be able to identify and capture persons who have an arrest warrant. While the database used for this purpose will be CONARC, only around 100-20-0 persons from the over 46,000 list will be included in the facial recognition software. They will be chosen according to the seriousness of the alleged crimes. The cost of the facial recognition system will be partially covered by the oil companies present in the city.
5. I am concerned that neither Buenos Aires nor Comodoro Rivadavia carried out any privacy impact assessment before implementing extensive surveillance camera networks or facial recognition and license plate recognition systems. The officials I interviewed all said they were certain that the right to privacy was not being violated by the systems in place and that they fulfilled the legal requirements, but could not explain their necessity and proportionality. In these and similar instances it is essential that PIAs are carried out immediately without delay and their recommendations regarding safeguards and remedies be immediately complied with

**Data protection**

1. In October 2000, Argentina passed Law 25.326 on Data Protection. Civil society organizations criticized that, by placing the National Directorate for the Protection of Personal Data (Argentina’s Data Protection Authority) under the Secretariat for Registry Affairs of the Ministry of Justice, its financial and administrative independence from the executive power was limited.
2. Another reason of concern expressed to us is that the law excludes the need for consent when data is collected by public institutions in the exercise of their functions.
3. Since 2016, the Data Protection Authority is part of the Agency for Access to Public Information. Its director is satisfied with its level of autonomy: the Agency, with a staff of 41 persons, proposes and executes its own budget, and designs its own institutional structure. Its head can only be removed from the post, which has a duration of five years, by the President with the approval of Congress. As evidence of its autonomy, the director cited the many cases it has brought against the administration. Still, despite the difficulty involved in changing the Argentine constitution, civil society organizations propose giving the Data Protection Authority constitutional status and complete autonomy from the executive.
4. On 19 September 2018, a new data protection law was presented in Congress. It is very necessary and important that a new data protection law will be passed at the earliest opportunity. While everybody agrees that a new law is necessary, several aspects of the proposed law have been criticized by civil society, including:
	1. It admits that consent for the use of data can be given implicitly. This can cause confusion and generally erode the protection of the data-holder.
	2. It does not explicitly protect metadata, which should be given the same level of protection as personal data.
	3. It blurs the principle of finality by allowing use of data that can be “reasonably presumed” by the data holder according to the context, allowing for expanding the use of data beyond the aim that consent was provided for.
	4. It allows public institutions to collect data without consent if the collection is done within its competencies and for a legitimate aim.
	5. It does not establish an obligation for the human intervention in automated decisions.
	6. It allows exporting personal data to third countries with weaker data protection frameworks.
	7. It does not include biometric data in the “sensitive data” category.
	8. The penalties established by the law are insufficient: without linking the amount of the fine to the company’s revenue (like the European GDPR does), they will not have a strong deterring impact against violations of data protection legislation in Argentina by powerful multinational tech corporations.
5. Some of the above concerns are justified, others less so, but clearly there is room for improvement in the current draft before Congress can finalise the very necessary new law

**Health data**

1. In April 2018, the Ministry of Health created the National Directorate of Health Information Systems. The Directorate is promoting the digitalization of medical histories (currently only 20% of health institutions in Argentina have digital records) in order to improve their safety and reliability, but will not create a single national health database, as each province will still manage its database. The Directorate does not have privacy experts among its staff, but works with lawyers of the Ministry of Health in order to ensure compliance with data protection regulations.
2. In order to protect health data from unnecessary access, each health professional is given different levels of access according to their needs.

**Recommendations**

1. The Congress of Argentina expedite the passage of the new data protection law duly revised in line with the above.
2. The Congress of Argentina should urgently introduce a draft law for discussion, which properly covers the data protection and privacy aspects of use of personal data by police forces, which at present is not covered by the current draft.
3. Intelligence services should conduct an in-depth revision of its culture and practices of opacity, currently imposed by law. Making sure that only information that needs to be kept secret is in fact secret, would allow Argentinian society to better understand the role and working methods of its various intelligence services. Ultimately, and together with strict oversight and adherence to the law, it would allow intelligence services to gain trust from Argentinians.
4. There should be created a new independent full-time body whose work should complement that of the Bicameral Commission on Intelligence. This new independent entity should contain a blend of senior judges, ICT technical staff and experienced domain experts, in adequate numbers and who would have full authority to carry out snap-checks of both intelligence agencies and police services in order to assess whether any surveillance  being carried out is legal, necessary and proportionate. Argentina’s excellent system of independent public defenders should be involved in the work of this independent oversight agency. In line with international best practise, this new oversight body should have full and permanent remote electronic access to all databases held by the intelligence and police forces it oversees. It should report independently to the legislature and not to the executive and thus also be subject to the oversight of the Bicameral Commission.
5. More modern and secure IT systems should be introduced for the dissemination of content of interception of communications, than the one currently being employed by DAJuDeCO. This modernisation should ensure that audit trails are much harder to avoid. The use of CDs should be eliminated and replaced by transfer of files exclusively over secure IT systems.
6. It is regrettable that parts of the draft law on interception of communications and chain of custody (S-979/18), duly revised and updated, has not yet made it onto the statute book since this would increase the legal measures and deterrent devised to help avoid breaches of personal information obtained through legitimate surveillance;
7. Moreover, a system should be introduced in line with international best practices, whereby investigators are not given the entire content of intercepted lines but rather only those parts relevant to the investigations, with transcripts being strictly carried out by officials who do not form part of the investigating teams.
8. Consolidate judges’ and prosecutors’ awareness and knowledge of international standards and tests of necessity and proportionality in a democratic society through dedicated training programs/modules.
9. Privacy Impact Assessments should be made mandatory by law as a pre-requisite to the deployment of all surveillance technologies, including CCTV cameras with license plate,facial and gait recognition capabilities.
10. The CONARC database on which these technologies have been made to depend in certain instances or, more probably, the system of laws on which it is based - should also be reviewed. While the CONARC database cannot be described as being disproportionate to the extent that it only includes 0.1% of the population of Argentina, it is clear that it contains errors as well as people who have not necessarily committed serious crimes. Juveniles should also be excluded from this database.
11. I would like to express my satisfaction at the Government’s willingness to engage in open dialogue, and to review and discuss legislation and practices, which need improvement. I hope that my report will support the Government in this process and would like o express my willingness to assist in this endeavour.

\_\_\_\_\_\_\_\_\_\_\_\_

[1/](https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E" \l "_ftnref1)This number, while it may look high is actually significantly smaller per capita than the average number of interceptions carried out per year for all security forces in a comparable medium-sized European country.

[2/](https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E" \l "_ftnref2)The Special Rapporteur is also concerned as to the methodology used in interceptions. While the rule of law is respected, the system devised to enable use of the intercepted material is antiquated and of poor design which increases risks especially of blackmail and extortion by the persons who have access to the content of interceptions (which excludes DAJuDeCO). The current system results in the flow of millions of physical CDs and similar devices which are far more easily prone to falling into the wrong hands than had more modern secure IT systems be used where audit trails are much harder to avoid. Moreover, a system should be introduced in line with international best practices, whereby investigators are not given the entire contents of intercepted lines but rather only those parts relevant to the investigations with transcripts being strictly carried out by officials who do not form part of the investigating teams.