联合国 A/HRC/46/37/Add.5

大会

Distr.: General
27 January 2021
Chinese
Original: English

人权理事会
第四十六届会议
2021年2月22日至3月19日
议程项目3
促进和保护所有人权——公民权利、政治权利、
经济、社会及文化权利，包括发展权

对阿根廷的访问

隐私权特别报告员约瑟夫·坎纳塔奇的报告* **

概要

隐私权特别报告员2019年5月对阿根廷进行了访问，本报告反映了截至2020年10月底的情况。特别报告员发现，该国保护隐私的法律制度相对健全和完善，最高法院开展了世界领先的活动，包括发布保护个性发展空间的判决。自2000年以来制定的数据保护法体系正在步入新一轮的改革——阿根廷2019年2月加入了《关于在自动处理个人数据方面保护个人的公约》，2019年9月签署了修正《关于在自动处理个人数据方面保护个人的公约》的《议定书》，因此必须加以改革——同时，该国在国际数据保护界发挥的新作用受到称赞和鼓励。关于国家主导的监视，特别报告员发现，截获的电话数量极多，而用于监听和分析截获通信的系统使用的是过时的技术和有缺陷的方法。阿根廷历届政府，既包括市政府，也包括联邦政府，至少在过去12年里都面临非法监视的指控，特别报告员建议作为紧急事项大力强化独立监督系统，对事后和事前监视进行监督。特别报告员还就数据保护立法的现代化、加强国家数据保护机构的独立性、健康数据、大数据和开放数据、性别与隐私以及儿童与隐私等问题提出了建议。

* 报告概要以所有正式语文分发。报告正文附于概要之后，仅以提交语文和西班牙文分发。

** 因提交方无法控制的情况，经协议，本报告迟于标准发布日期发布。

Annex

Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on his visit to Argentina

I. Introduction

1. The present report was finalized towards the end of 2020, after an evaluation of the preliminary results of the in situ country visit undertaken from 6 to 17 May 2019, and cross-checking of that information against follow-up research and developments to date. The benchmarks used in the report include the privacy metrics set out in a draft document prepared in 2019 by the Special Rapporteur on the right to privacy.[1]

2. Much of the content of the present report reflects and builds upon the findings already included in the Special Rapporteur's end-of-mission statement,[2] but it also includes additional observations made during an informal visit to Salta Province following the end of the official visit on 17 May 2019.

3. The Special Rapporteur thanks the Government (Ministry of Justice and Human Rights, in particular the Secretariat for Human Rights, and the Ministry of Foreign Affairs and Worship) for its invitation to visit the country and for its generous cooperation. The Special Rapporteur also thanks the United Nations entities in Argentina for their support during his visit. Additional thanks are due to the government of Salta Province for its collaboration in organizing his visit there and answering a number of detailed questions about the development of systems designed to tackle the issue of teenage pregnancies.

4. During his visit, the Special Rapporteur assessed the situation of the right to privacy in Argentina by studying recent reforms and existing mechanisms to prevent violations of the right to privacy, and by hearing concerns expressed by civil society organizations, experts and other actors. He also received useful information on current best practices in Argentina.

5. As part of the Special Rapporteur's fact-finding mission, he visited the Autonomous City of Buenos Aires, and Comodoro Rivadavia and Rawson in Chubut Province. The Special Rapporteur met with senior officials of the government at the national and provincial levels, the legislature, law enforcement agencies, national and provincial data protection authorities and human rights institutions, United Nations entities and non-governmental organizations. He would like to thank them all for their time and their valuable input both before and during the visit. After the conclusion of the official part of the visit, he visited Salta Province in order to further investigate the use of certain technologies relevant to the protection of children's right to privacy.

II. Constitutional and other legal protections of privacy

6. The legal safeguards and remedies in Argentina protecting against infringement of the right to privacy compare relatively well and can be considered to be among the leading examples in South America.

7. The Constitution does not make explicit mention of a right to privacy, but the Supreme Court has interpreted the Constitution, and especially article 19, as recognizing a right to privacy: "The private actions of men that in no way offend public order or morality, nor injure a third party, are reserved only to God, and are exempt from the authority of the magistrates.

[1] Available at www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf. The document was developed during the period 2017–2019 to enable the Special Rapporteur to maximize the number of common standards against which a country's performance could be measured. It was released for public consultation in March 2019.

[2] Available at www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E.

No inhabitant of the Nation shall be compelled to do what the law does not order, or be deprived of what it does not forbid."[3]

8. The Supreme Court has tackled various dimensions of privacy in a number of its decisions.[4] Some of its more recent decisions, such as in *Castillo, Carina Viviana y otros* in 2017, include conceptualizations which, although under a general heading of privacy, are closer to those of autonomy and free development of personality:

> The obligation imposed by the provincial government on parents to complete a form declaring if they want their children to receive "religious education", and, if such is the case, which religion they desire to be taught to them, as well as the fact that this statement is to be kept in the student's personal file as part of the institutional student information record, constitutes a violation of the right to privacy, since it involves an interference with an individual's personal sphere insofar as it requires revealing an aspect of the individual's spiritual personality, a dimension which belongs to each person's inner self.[5]

9. It is heartening to see that the direction of the Supreme Court is very much in line with Human Rights Council resolution 34/7 of March 2017 on the right to privacy in the digital age, whose preamble includes the following:

> *Recognizing* that the right to privacy can enable the enjoyment of other rights and the free development of an individual's personality and identity, and an individual's ability to participate in political, economic, social and cultural life, and noting with concern that violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association.

10. In *Castillo, Carina Viviana y otros*, the Supreme Court interestingly and explicitly associates the right of personality to one of the "other human rights" referred to by the Human Rights Council in its resolution 34/7 – the right of freedom of religion – explicitly declaring unconstitutional an infringement of what is today considered to be sensitive data in modern privacy and data protection law: "A provision compelling parents to reveal an aspect of their spiritual personality, a dimension which belongs to each person's inner self, constitutes a violation of their right to privacy, and shall be declared unconstitutional."[6]

11. In this 2017 decision, the Supreme Court is following a tradition most notably articulated recently in *Arriola, Sebastián y otros* in 2009, which may be interpreted as an explicit recognition of the right to free development of personality as linked to autonomy and the right to privacy:[7]

> "(2) Article 19, Argentine Constitution, directly connected with individual freedom, legally protects a sphere of individual autonomy including feelings, practices and customs, family relations, financial situation, religious beliefs, mental and physical health, and, in sum, any actions, events, or information which, considering the lifestyles accepted by the community, are reserved for the individual (opinion of Justices Highton de Nolasco and Maqueda and opinion of Justice Petracchi).
>
> "(3) The provision of article 19, Argentine Constitution, is the very foundation of modern freedom, i.e. the freedom of conscience and personal will, the conviction that it is an essential tenet of ethics that acts worthy of merit be made by virtue of the

[3] See www.wipo.int/edocs/lexdocs/laws/en/ar/ar075en.

[4] See, for example, *Arriola, Sebastián y otros*, Case No. 332:1963, 25 August 2009, *Supreme Court of Argentina: Relevant Cases = Corte Suprema de Justicia de la Nación Argentina: fallos relevantes*, Spanish-English bilingual edition (2018), p. 59.

[5] *Castillo, Carina Viviana y otros c/ Provincia de Salta – Ministerio de Educación de la Prov. de Salta*, Case No. 340:1795, 12 December 2017, *Supreme Court of Argentina: Relevant Cases*, p. 15, at p. 24.

[6] Ibid., at p. 25.

[7] The American Declaration of the Rights and Duties of Man (1948) is the first international legal instrument to deal explicitly with the notion of the free and unhindered development of personality. Article XXIX reads as follows: "It is the duty of the individual so to conduct himself in relation to others that each and every one may fully form and develop his personality."

> individual's free will in connection with the values that person holds (opinion of Justices Highton de Nolasco and Maqueda and opinion of Justice Petracchi)."[8]

12. The Justices of the Supreme Court support their reasoning by also citing trends in international jurisprudence relevant to the treaty obligations of Argentina:

> International treaties recognize several rights and guarantees established in the 1853 Argentine Constitution, including the right to privacy protecting persons from being subject to arbitrary or abusive interference in their private lives (article 11.2, American Convention on Human Rights; article 5, American Declaration of the Rights and Duties of Man; article 12, Universal Declaration of Human Rights, and article 17.1, International [Covenant] on Civil and Political Rights). In connection with such right and its relation with the principle of "personal autonomy", at the Inter-American level it has been stated that "the development of the human being is not subject to the initiatives and care of public power". Under a general perspective, that principle includes the ability to lead their life, decide on the best way to do it, to resort to means and instruments for that purpose, selected and used with autonomy which is a sign of maturity and a condition for freedom and even to legitimately resist or reject improper interference and any aggressions (opinion of Justices Highton de Nolasco and Maqueda).[9]

13. Also in *Arriola, Sebastián y otros*, the Supreme Court formally pushes the envelope on privacy, personality and autonomy further than the protection afforded in many other countries, declaring ultra vires attempts by the National Congress to criminalize the possession of drugs for personal use:

> Article 14, second paragraph, Law No. 23737 is unconstitutional, as it criminalizes the possession of drugs for personal use when such use does not entail a specific danger or harm to rights or interests of others. Under such circumstances, that statutory provision violates article 19 of the Argentine Constitution, to the extent that it invades the sphere of personal freedom excluded from the authority of governmental bodies (opinion of Justices Highton de Nolasco and Maqueda).[10]

14. In the same case, the Supreme Court examines the fine line between the rights of the executive and those of the legislature:

> While in principle the decision regarding the best way to prosecute the crime and which are the legally-protected interests which require further protection are criminal-policy issues pertaining to the other branches of Government, as this case is about the challenge of a normative system (article 14, second paragraph, of Law No. 23737) which criminalizes conducts which have been made under circumstances which do not entail any harm to others and which are protected under article 19 of the Argentine Constitution, it is appropriate for this Court to find that the Congress has exceeded the powers recognized under the Constitution (opinion of Justices Highton de Nolasco and Maqueda).[11]

15. The Supreme Court Justices also deliver an obiter dictum about surveillance, which may well be cited in future court decisions in Argentina:

> If criminal law could restrict any conduct affecting individual morals, the Government would be imposing a given set of morals, which would be almost totalitarian, as the Government could surveil without any limits the activity of all inhabitants, whether public or private in nature (opinion of Justices Highton de Nolasco and Maqueda and opinion of Justice Petracchi).[12]

16. The Constitution, in its 1994 revision, also embraces the principle of habeas data in its article 43, which reads as follows:

[8] *Arriola, Sebastián y otros, Supreme Court of Argentina: Relevant Cases*, p. 61.
[9] Ibid., pp. 62–63.
[10] Ibid., p. 61.
[11] Ibid., p. 62.
[12] Ibid., p. 61.

> Any person shall file a prompt and summary proceeding regarding constitutional guarantees, provided there is no other legal remedy, against any act or omission of the public authorities or individuals which currently or imminently may damage, limit, modify or threaten rights and guarantees recognized by this Constitution, treaties or laws, with open arbitrariness or illegality. In such case, the judge may declare that the act or omission is based on an unconstitutional rule. This summary proceeding against any form of discrimination and about rights protecting the environment, competition, users and consumers, as well as about rights of general public interest, shall be filed by the damaged party, the ombudsman and the associations which foster such ends registered according to a law determining their requirements and organization forms. 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. When the right damaged, limited, modified, or threatened affects physical liberty, or in case of an illegitimate worsening of procedures or conditions of detention, or of forced missing of persons, the action of habeas corpus shall be filed by the party concerned or by any other person on his behalf, and the judge shall immediately make a decision even under state of siege.[13]

17. This principle, originally inspired by the right of access principle enshrined in article 8 of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, is one found fairly frequently in modern Latin American constitutions. Argentina was the fourth country in Latin America to adopt the principle in its Constitution, after Brazil (1988), Paraguay (1992) and Peru (1993).[14] In this sense, Argentine constitutional law also compares favourably with the principle established in article 8 (2) of the Charter of Fundamental Rights of the European Union, which stipulates inter alia that "[e]veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

18. The Constitution also contains what may be termed standard search and seizure provisions protecting private and family life, the home and correspondence in its article 18, which provides that "[t]he 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".[15]

19. The vigilance of the Supreme Court is also to be noted in matters of surveillance. In June 2019, barely a month after the conclusion of the official visit by the Special Rapporteur, the Supreme Court cited the Special Rapporteur's end-of-mission statement, taking on board some of his observations and recommendations regarding the interception of communications and who should have access to the entire content of intercepted material (see below).[16]

20. Insofar as regional human rights frameworks are concerned, Argentina adheres to the American Convention on Human Rights, and cases regarding breaches of privacy brought by citizens of Argentina may be referred to the Inter-American Court of Human Rights by either the Inter-American Commission on Human Rights or the Government. It is worth noting that article 11 of the American Convention on Human Rights is a fairly comprehensive legal articulation of the conceptualization of privacy. It paints a picture in which a number of aspects come together to create a sphere of intimate human activity that is worthy of significant protection: a person's privacy and those places where it is most clearly manifested, namely family life, the home and correspondence. Within this protected sphere, one finds dignity, reputation and – to cross-refer to article XXIX of the American Declaration of the

[13] See www.wipo.int/edocs/lexdocs/laws/en/ar/ar075en.

[14] Andrés Guadamuz, "Habeas data: the Latin-American response to data protection", *Journal of Information, Law and Technology*, no. 2 (2000).

[15] See www.wipo.int/edocs/lexdocs/laws/en/ar/ar075en.

[16] Hernán Cappiello, "La Corte reguló el uso de escuchas telefónicas y advirtió sobre las filtraciones", La Nación, 20 June 2019.

Rights and Duties of Man – the free development of personality. To date, however, it would seem that the domestic remedies afforded by the Supreme Court, inter alia, have been sufficient to protect the right to privacy in Argentina without recourse to the Inter-American Court of Human Rights.

A. Data protection law and international standards

21. Argentina adheres to the international gold standard in privacy and data protection law: the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. The Convention entered into force on 1 June 2019, following the passing on 6 December 2018 of Act No. 27,483 by the National Congress to incorporate it into the domestic legal framework. Argentina was granted access to the Convention largely on the basis of its omnibus data protection legislation dating from October 2000. The Personal Data Protection Act (Act No. 25,326), of October 2000, is quite closely modelled on Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Directive 95/46/EC was in turn largely inspired by the Convention. In June 2003, the Commission of the European Communities adopted a decision establishing that the legal framework in Argentina provided an adequate level of protection for personal data, consistent with the standards applied in Europe. On 19 September 2019, Argentina signed the Protocol amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, becoming the thirty-third country to do so.

22. Another relevant statute, which complements the Personal Data Protection Act, is Act No. 26,951, enacted in 2014, through which the *No Llame* (Do Not Call) national registry was created, and which was substantially similar to the sectoral laws in the Autonomous City of Buenos Aires and the Province of Buenos Aires.

23. The compatibility of the Personal Data Protection Act with the Convention is maintained through, inter alia, its applicability in matters of both law enforcement and national security, under the terms of article 23:

> Personal data that have been stored for administrative purposes and must be permanently registered in the databases of the armed forces, security forces and police and intelligence services shall be subject to the provisions of the present Act; the same applies to personal data provided by such databases at the request of administrative or judicial authorities in accordance with the law.
>
> The processing of personal data for the purposes of national defence or public security by the armed forces, security forces and police and intelligence services without the consent of those affected shall be confined to particulars and categories of data strictly necessary in order to carry out the tasks legally assigned to those bodies in the interests of national defence, public security or the prosecution of offences. Databases in such cases shall be specialized and designed for that purpose, and shall be classified in categories according to their degree of reliability.
>
> Personal data registered for police purposes shall be deleted when no longer necessary for the investigations for which they were stored.[17]

24. While the Argentine legal framework on data protection is thus in fairly robust shape, it is to be noted that the European Union has moved on from Directive 95/46/EC, on which the law in Argentina is currently based, to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), which entered into force on 24 May 2016 and has applied since 25 May 2018. Thanks to its signature of the Protocol amending the Convention, which established standards extremely close to those of the General Data Protection Regulation, Argentina has made a commendable international

[17] CED/C/URY/1, paras. 199–201; see also https://necessaryandproportionate.org/uploads/2020-argentina-en-faq.pdf#question2.

commitment to raise its standards of privacy protection even further. It is expected to be only a matter of time before the Personal Data Protection Act, of 2000, is replaced or complemented by a version modernized in a way to take into account all the technological and legal developments that have taken place over the past two decades. Some authors have pointed out the possibility that if Argentina does not do so, it will be putting at risk the adequacy assessment made by the Commission of the European Communities in 2003.[18] Indeed, Argentina had been taking steps to modernize its law through a bill presented to the legislative branch of Government on 19 September 2018 (No. S-979/18). However, the legislative process concluded unsuccessfully in 2020.[19]

25. If it continues on its current trajectory, there is no reason to doubt that Argentina will increasingly take a leading role in the international privacy world. It has made the most of its participation in activities related to the Convention, and the Director of the Agency for Access to Public Information (the Argentine data protection authority), Eduardo Bertoni,[20] is well regarded and has been elected as a member of the influential Bureau of the Consultative Committee that administers and oversees the deployment and growth of the Convention as amended. Under his guidance, the Agency,[21] which succeeded the National Directorate for the Protection of Personal Data as the national data protection authority, has continued to contribute to the creation of subsidiary legislation, helping keep the 20-year-old federal Act afloat in a rapidly changing world. This subsidiary legislation has included the following:

(a) In January 2019, the Agency issued Resolution No. 4/2019, in which it established a set of best practice guidelines for the interpretation and application of the Personal Data Protection Act with respect to the right of access to personal data collected through closed-circuit television cameras, automated processing of data, dissociation of data, biometric data, and consent, including consent of minors;[22]

(b) In May 2019, the Agency issued Resolution No. 86/2019, in which it set out guidelines for the processing of data for electoral purposes;

(c) In January 2020, in order to plug a gap in the Personal Data Protection Act, which does not provide for data protection impact assessments, the Agency, together with the enforcement authority of Uruguay, published guidelines for conducting such assessments, thus making the Argentine situation more compatible with the General Data Protection Regulation;

(d) In April 2020, the Agency issued Resolution No. 70/2020, in which it set out guidelines for the handling of personal data in the context of the pandemic and for the use of geotracking tools. In line with many other members of the international community, especially the parties to the Convention, the Agency stated that data protection principles should be strictly applied, even in an emergency situation such as the pandemic. It is a reminder to all that health data is sensitive data and should be treated as such, though it could be shared by health professionals working under conditions of professional secrecy.

B. Data protection as viewed by civil society in Argentina and the national data protection authority

26. The above positive points notwithstanding, the position regarding data protection was subject to some criticism during the Special Rapporteur's visit.

27. Civil society organizations criticized the Personal Data Protection Act, stating that by placing the National Directorate for the Protection of Personal Data – the precursor to the

[18] Adrián Furman and Francisco Zappa, "Argentina", in *The Privacy, Data Protection and Cybersecurity Law Review*, 7th ed., Alan Charles Raul, ed. (London, Law Business Research, 2020).

[19] Ibid.

[20] Mr. Bertoni has since resigned from the Agency, effective 1 January 2021.

[21] The Agency reports to the Chief of the Cabinet, a legislative position, which could be construed as not being in complete compliance with the requirements under the Convention as amended and the General Data Protection Regulation for a truly independent body. Its Director is appointed for a five-year term, renewable once.

[22] Furman and Zappa, "Argentina".

Agency for Access to Public Information, the Argentine data protection authority – under the Office of the Undersecretary for Registry Affairs of the Ministry of Justice, its financial and administrative independence from the executive power is limited.

28. Another reason for concern is that the Act excludes the need for consent when data is collected by public institutions in the exercise of their functions. This concern may be addressed by having more detailed laws explicitly outlining specific measures and the data that may be collected in pursuit of a specified purpose.

29. Since 2016, the data protection authority has been the Agency for Access to Public Information. When questioned specifically on the matter, the Director of the Agency expressed himself as being satisfied with the level of autonomy that it is accorded in real-life practise. With a staff of 41 employees, the Agency proposes and executes its own budget and designs its own institutional structure. Its director, who serves a five-year term, may only be removed from the post by the President with the approval of the National Congress. As evidence of its autonomy, the Director cited the many cases that it has brought against the Administration. Still, civil society organizations propose giving the data protection authority constitutional status and complete autonomy from the executive.

30. As mentioned above, consideration of the new data protection bill, which was presented to the National Congress on 19 September 2018, appears to have come to an unsuccessful conclusion, with the bill losing parliamentary status in February 2020. Several aspects of that proposed law have been criticized by civil society, including the following:

(a) It provides that consent for the use of data may be given implicitly. This may cause confusion and generally erode the protection of the data subject;

(b) It does not explicitly protect metadata, which should be given the same level of protection as personal data;

(c) It blurs the principle of finality by allowing the use of data that can be "reasonably presumed" by the data subject according to the context, allowing for the expansion of the use of data beyond the aim for which consent was specifically provided;

(d) It allows public institutions to collect data without consent if the collection is done within its competencies and for a legitimate aim;

(e) It does not establish an obligation for human intervention in automated decisions;

(f) It allows the export of personal data to third countries with weaker data-protection frameworks;

(g) It does not include biometric data in the "sensitive data" category;

(h) The penalties that it establishes law are insufficient: without linking the amount of the fine to the company's revenue (as is the case with the General Data Protection Regulation), the penalties will not have a strong deterrent impact on powerful multinational technology corporations against violations of data protection legislation in Argentina.

31. Some of the concerns recorded above are justified, others less so, but clearly there is room for improvement in the next attempt at modernizing data protection law.

C. Latest developments on the right to be forgotten

32. The legal position of Argentina vis-à-vis privacy and data protection continued to develop during the summer of 2020 when, in August, a court delivered the first decision on yet another matter related to the General Data Protection Regulation: the right to be forgotten. The National Civil Appeals Court enforced that right for the first time in *Denegri, Natalia Ruth C/ Google Inc. S/ Derechos Personalisimos: Acciones Relacionados*.[23] The judges ordered Google to erase all links to the search engine, the words "Natalia Denegri", "Natalia

[23] Case File No. 50016/2016, Judgment, 10 August 2020.

Ruth Denegri" and "Natalia Denegri caso Cóppola", and any images or videos recorded 20 years before from its video-sharing platform.

D. Legislation on surveillance

33. The Special Rapporteur presented a draft legal instrument on Government-led surveillance to the Human Rights Council in March 2018 (see A/HRC/37/62), and this may be used as an interim benchmark. However, there is not yet a universally agreed international binding multilateral treaty regulating such matters. Member States have therefore been left to establish their own safeguards and remedies with respect to State-led surveillance. The approach of Argentina to this subject has been very much an autochthonous one, as further outlined in the following section on surveillance. While, as will be seen, there exists ex ante authorization of surveillance, which is carried out using rather old-fashioned interception of telephone communications, the number of interceptions authorized seems to be prima facie disproportionately high.

E. Surveillance

34. The Special Rapporteur observed a general lack of trust in the intelligence services in Argentina. Possibly owing to the country's past, a strong culture of opacity and some highly-publicized cases of illegal surveillance, many individuals suspect that they are personally under surveillance and that intelligence agents act without oversight or supervision.

35. Since 2015, exclusive capacity to intercept communications has been held by a subsidiary body of the Supreme Court, the Legal Assistance Directorate on Complex Offences and Organized Crime (known as "DAJuDeCO").

36. In December 2015, the Government transferred the Legal Assistance Directorate from the Public Prosecution Service to the Supreme Court. After three years of reforms, the results are as follows:

(a) The Legal Assistance Directorate is the only body in Argentina with the executive authority to intercept communications and does so only at the request of both federal judges and prosecutors;

(b) Interception requests from all intelligence agencies and police forces must be channelled through federal judges, who must approve surveillance warrants before the interception is conducted by or at the request of the Legal Assistance Directorate;

(c) Presently, the total number of lines intercepted per month peaks at 6,000, of which only 69 are directly intercepted, with the Legal Assistance Directorate officials listening in live, while 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 Legal Assistance Directorate officials, but is automatically recorded onto compact discs without human intervention and then distributed to the authorities indicated in the surveillance warrant. In 2018, the total number of lines intercepted was 41,000.[24]

37. The Special Rapporteur is convinced that the safeguards put in place at the Legal Assistance Directorate are adequate and preserve the privacy of the individual. The Directorate has presented evidence that, in terms of both the personnel working there and the institutional design and work protocols, it is trying its best to minimize human intervention, ensure that personal data is protected and guarantee that the only people to have access to the content of the interceptions are the legal beneficiaries of a surveillance warrant issued by the judiciary.

[24] 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.

38. The level of transparency in many matters at the Legal Assistance Directorate is quite exemplary and class-leading. One further step required would be to publish its annual reports online and not only in hard copy, as was the situation at the time of the visit.

39. However, the technology being used is antiquated. If newer interception technology is procured, enabling not only the interception of landlines and mobile conversations but also, for example, the use of malware on mobile phones, both the institutional design and the safeguards deployed need to be revisited accordingly.

40. The Special Rapporteur also finds that the surveillance system used in Argentina has several inherent vulnerabilities resulting from: (a) the overuse of interception, which is treated as an ordinary measure of investigation for all types of crimes and not as a last resort for serious crimes; (b) weak control in the chain of custody over access to the content of interceptions;[25] and (c) the lack of independent control over the use of interception.

41. It is the Special Rapporteur's strong belief that all security forces, as well as assisting bodies (such as the Legal Assistance Directorate), should invest serious effort towards increasing their transparency, where not already achieved.[26] This can be done in multiple ways, including through online publication of their annual activity reports, where available, and any other relevant information that could help citizens better understand the types of activities being carried out by these organizations and the type of safeguards that they have put in place to protect human rights.

42. In this context, the Special Rapporteur expresses his strong concerns about the overreaching nature of the regulatory framework regarding the classification of information related to the security forces. By classifying as secret all information related to their structure and activities, the law de facto prevents them from putting in place adequate transparency policies, which would contribute to strengthening public trust.[27]

43. It would appear that the intelligence services and the police do not possess the advanced technical capabilities required to conduct surveillance, and Argentina could not be fairly described as "a surveillance State". Indeed, it should be emphasized that this is very far from being the case. On the other hand, those privacy-intrusive technologies are easily available, and a case could easily be made that they are proportionate measures in the fight against organized crime and terrorism. It is essential that Argentina prepare itself immediately for such an eventuality by introducing the right safeguards, especially in the oversight of surveillance capabilities and intelligence.

44. An essential element of oversight already exists in the important work carried out by the National Congress's Joint Standing Committee on Monitoring of Intelligence Bodies and Services. However, that work is insufficient insofar that the Joint Standing Committee has neither the legal ability nor the resources to fully audit, in depth, the conduct of a specific case, nor does it have full access to the contents of a case file. The Special Rapporteur

[25] The Rapporteur is also concerned as to the methodology used for interception. While the rule of law is respected, the system devised to enable the use of the intercepted material is antiquated and of poor design, which increases the risk, in particular, of blackmail and extortion by those who have access to the content of intercepted material (the Legal Assistance Directorate does not have such access in most cases). The current system results in the flow of millions of physical compact discs and similar, which are far more prone to falling into the wrong hands than more modern secure information technology systems in which audit trails are much harder to avoid. Moreover, a system should be introduced, in accordance with international best practices, whereby investigators are not given the entire content of intercepted material, but rather only those parts relevant to the investigations concerned, with transcripts strictly produced by officials who do not form part of the investigating teams.

[26] The Government has expressed a commitment to increasing transparency in relation to intelligence activities.

[27] The Special Rapporteur is encouraged by the recent adoption of regulations that will reduce the amount of information classified as secret with regard to the organization and activity of the security forces.

recommends that a new independent and full-time body be created, whose work should complement that of the Joint Standing Committee (see para. 76 below).[28]

45. Several cases of illegal surveillance have been brought to the Special Rapporteur's attention. In one, in 2015, an agent of the Federal Intelligence Agency followed 26 members of an indigenous Mapuche community, who were part of an anti-mining movement, for several months, working with two police officers, and then shared the information that he had collected with prosecutors in Chubut Province. While the case is still *sub judice*, elements of great concern are the nature and intensity of the surveillance, the fact that it may have been based on grounds prohibited by law (race, ideology and 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. The Special Rapporteur encourages the Government to immediately increase the resources allocated to protecting the welfare and privacy of these indigenous peoples and take all measures necessary to hold all perpetrators accountable, compensate the victims and ensure that the violation does not occur again.

46. In the months subsequent to the Special Rapporteur's visit, there were several media reports – including regarding indictments – that alleged abuse and misconduct by some members of the intelligence service in Argentina.[29] The investigations into illegal spying and court proceedings are still ongoing but, if the allegations are proved to be true, they only further strengthen his recommendations for stronger oversight mechanisms (see paras. 75–76 below).

F. Criminal databases

47. On 22 April 2009, the Government created the National Inquiry System on Default and Detention Orders (CONARC), an online database that allows all law enforcement and justice system officials across the country confidential access to a list of all persons against whom arrest warrants had been issued in Argentina.

48. On 15 November 2016, the Ministry of Justice and Human Rights issued Resolution 1068-E/2016, in which it made the list accessible online to the public. Under article 1 of the resolution, only adults sought for serious crimes would be included. Indeed, the name given to the database is *Los Más Buscados* (Most Wanted), giving an idea of the danger posed to society by the persons listed in the database.

49. The Special Rapporteur has the following observations regarding the database;[30]

(a) As at 16 May 2019, it contains a list of 46,479 persons;

(b) The list provides the name and age of the wanted person, the paternal and maternal surnames, national identification number, the type of offence for which the person is wanted and the institution and authority issuing the warrant. While the identification number could be an important tool for authorities to carry out an arrest, the Special

[28] The Government has provided comments describing reforms of the intelligence service. While the fact that the reforms have been undertaken is not contested, no mention is made of new safeguards and remedies for privacy protection. The Special Rapporteur welcomes the increased internal control and parliamentary oversight, therefore, but these measures do not dispense with the need for proper independent oversight (see paras. 75–76 below), which is a quite separate matter.

[29] See, for example, www.lapoliticaonline.es/nota/84975-personal-assistant-to-former-argentine-president-along-with-his-counterinteligence-director-arrested-on-espionage-charges, www.insightcrime.org/news/analysis/state-intelligence-crime-latin-america, https://intelnews.org/2020/06/02/01-2793, www.batimes.com.ar/news/argentina/afi-illegal-espionage-claims-put-macri-in-spotlight.phtml, https://cpj.org/2020/06/argentine-intelligence-services-surveilled-journalist-hugo-alconada-mon-under-macri-administration and www.world-today-news.com/a-scandal-in-argentina-list-of-state-spies-on-the-internet-by-court-order.

[30] The Special Rapporteur welcomes the measures taken by the Government during the period March–October 2020 to address some of the risks posed by CONARC, by eliminating the personal data of minors from this database and conducting a full revision of its contents.

Rapporteur does not see how it could be considered necessary to release this information to the public;

(c) 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). In 13,703 files (29.5 per cent of the total), there is no information on the type of offence for which the person is wanted;

(d) The list contains 61 children. It is particularly disturbing that juveniles are included on the public database, and it is difficult to justify as being in the best interests of the child, as obliged by the Convention on the Rights of the Child (art. 3 (1)), ratified by Argentina on 4 December 1990. That Convention also recognizes the right of every child alleged as or accused of having infringed penal law to have his or her privacy fully respected at all stages of the proceedings (art. 40 (2) (b) (vii)), and publicizing arrest warrants against juveniles is incompatible with this right;

(e) The database contains multiple errors: as an example, two persons are listed as being aged 2 and 3 years respectively and wanted for assault and robbery. Given the potential infringement of a person's right to privacy, the accuracy of such a list has to be scrupulously ensured;

(f) Another concern that the Special Rapporteur has received is that the list is not properly updated, meaning that warrants over a decade old may still be found in this 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 that they feed into the database, leading to errors and discrepancies.

G. Privacy and children

50. The Special Rapporteur has noted with concern information on two cases in which the right of girls to privacy was violated. In the first case, a 12-year-old girl became pregnant as a result of sexual abuse in Jujuy Province. In January 2019, after having been attended to at the Dr. Guillermo Paterson Hospital and her pregnancy having been confirmed, she and her legal tutors decided to undergo an abortion. However, the hospital staff refused to comply, and the case became the subject of public debate in the media. While the Catholic Church and anti-abortion groups publicly opposed the abortion, the Governor stated that the Criminal Code of Argentina allowed abortion in that case and that he had given the order for the abortion to be conducted. At the Dr. Héctor Quintana Maternity and Children's Hospital, the medical team performed a caesarean section resulting in a live birth. Without the consent of the girl or her family, the provincial Minister of Health publicized in provincial and national media the patient's clinical picture, the medical procedure to be carried out, the time of the surgical intervention and the conditions of her health before and after the treatment.

51. Also in January 2019, "Lucía", an 11-year-old girl from Tucumán Province, and her legal tutors decided to undergo 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 five weeks, and failed to protect the girl's right to privacy. The medical staff, together with the secretary of the provincial health system and the director of the Hospital del Este, revealed sensitive data about the girl's life, with information about her health and clinical history.

52. The Autonomous City of Buenos Aires is implementing several initiatives to protect the rights of children in the digital environment, including the right to privacy.

53. On 15 December 2016, the Autonomous City of Buenos Aires passed the Act No. 5,775 on the prevention of grooming, under which the City's public institutions are required to design and implement awareness-raising and capacity-building activities for children, parents and professionals. Since the passing of the Act, over 25,000 cases have been brought to the attention of the authorities.

54. In the past five years, the City Ombudsman's Office has been running a programme called *Conéctate seguro* (Connect Safely), in order to promote the safe use of data by children. In 2018, approximately 3,500 children participated.

55. After the conclusion of the official visit, and with the full cooperation and assistance of officials from the federal and provincial governments, the Special Rapporteur conducted an informal visit of Salta Province (18–22 May 2019) where, it had been reported to him, new technologies were being deployed in a way that could present some level of risk to the privacy of children.

56. During the informal visit, the Special Rapporteur noted with interest the joint initiative of the provincial Ministry of Early Childhood and Ministry of Public Health together with local non-governmental organizations (NGOs) in Salta Province, aimed at using modern technology to reduce poverty. In spite of continuous government investments in health, education and food security, approximately 30 per cent of the inhabitants of the province live under the poverty threshold and approximately 50 per cent of children abandon school after completing their primary education.

57. In this context, the provincial government decided to use a technological solution to conduct risk assessments on vulnerable individuals, with the aim of better targeting government resources.

58. Following a census model, technological means such as mobile phones and computers are employed to systematically gather relevant information regarding a particular individual or family. The information is collected by multiple agents belonging to both government agencies (such as health and social workers) and NGOs, and relates to a variety of elements, including access to drinking water. Health conditions, level of education, infrastructure, access to government services, and pregnancy rates.

59. Individuals are asked for their consent to participate in this initiative and a declaration of confidentiality is signed. Photographs, where required, are taken only with the consent of the individual concerned and/or legal guardian in the case of minors. All meetings are recorded and the recordings are shared to assist with the fact-checking process.

60. Once it is collected, all the information is uploaded to a database, which is shared with different government agencies through a joint platform created for this purpose.

61. An important aspect of this intervention targets families with children, as it has been discovered that 60 per cent of vulnerable individuals in the province are unable to provide basic care for their children. Public officials use a score system to build profiles of children and parents, which they then use to decide on the type of assistance required by each family.

62. The Special Rapporteur was assured that the database provides for different levels of access and uses multiple security levels. For example, NGOs participating in the project have their own portals that they use to upload the data collected to the central database. They thus have access only to the information that they have collected themselves and not to the entire bank of information stored centrally.

63. The information is collected locally using mobile phones and computers and uploaded at periodic intervals over the Internet to the national database. The local databases stored on the mobile phones and computers are encrypted using commercial cybersecurity products.

64. The information in the database is also employed to produce risk profiles – for example, to identify minors who are at risk of becoming teenage mothers – which are then used to stage interventions.

65. The Special Rapporteur was informed that various algorithms are employed to correct any potential errors in the risk assessment and rating systems, which may lead to bias. Human operators are also tasked with continuously checking the quality of the information before it is uploaded to the central database.

66. Preliminary findings seem to indicate a positive impact of this intervention model, especially visible in the decrease in childhood mortality since the project was launched. Consequently, the model has been exported to other parts of Argentina, such as La Rioja and

Tierra del Fuego, and to other countries, such as Colombia, the Plurinational State of Bolivia and Paraguay.

67. While the Special Rapporteur appreciates the need for more targeted social interventions, there are nevertheless several issues of concern:

(a) The provincial government did not conduct a proper privacy impact assessment before deploying this system, which would have ensured that all the necessary privacy safeguards had been implemented from the design phase;

(b) It is not clear whether the databases (both the local and the central ones) are secure enough, given the sensitivity of the information that they contain;

(c) There is potential for bias in the automated risk assessment of vulnerable individuals, which in turn has the potential to cause lasting emotional and reputational damage to the individuals concerned;

(d) The model has been exported to other areas of Argentina and to other countries in the region before it has been ascertained that it is in accordance with the principles of privacy by design and privacy by default.

H. Closed-circuit television and facial recognition

68. Since 2016, the government of the Autonomous City of Buenos Aires has significantly increased its network of surveillance cameras in an attempt to improve security and prevent crime. Currently, there are more than 7,000 cameras installed in the City and operated by the Ministry of Security. Examples in other cities have shown that the logic of efforts to improve public security by installing surveillance cameras is questionable in some instances and justifiable in others. The justifiability, legitimacy, necessity and proportionality of such a system should have been established by a privacy impact assessment, which does not seem to have been conducted.

69. 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 containing 46,000 files of persons against whom arrest warrants have been issued. The Special Rapporteur's concerns regarding CONARC (see paras. 47–49 above) also apply here. The Special Rapporteur is aware of the need to arrest persons who are suspected of having committed crimes and bring them to justice. However, he fails to see the proportionality of installing such a technology, which has serious privacy implications and involves searching a database of 46,000 persons that includes those wanted for non-serious offences and is not carefully updated or checked for accuracy.

70. The fact that a facial recognition system is being implemented without the necessary privacy impact assessment or the desirable consultation and strong safeguards is also a reason for concern. The City government passed Resolution No. 398/MJYSGC/19 on biometrics, but no detailed legislation on the use of facial recognition.

71. Comodoro Rivadavia, a city of approximately 180,000 inhabitants in Chubut Province, has a network of 120 cameras, which the provincial government plans to increase to 250. The government plans to give the network facial recognition capabilities in the coming months, with a view to identifying and arresting individuals against whom an arrest warrant has been issued. While the database to be used for this purpose will be CONARC, only approximately 100–200 individuals of the 46,000 listed will be covered by the facial recognition software, who 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.

72. The Special Rapporteur is concerned that neither Buenos Aires nor Comodoro Rivadavia conducted a privacy impact assessment before implementing extensive surveillance camera networks and facial recognition and licence plate recognition systems. The officials whom he interviewed all asserted that they were certain that the right to privacy was not being violated by the systems in place and that the systems fulfilled the legal requirements, but were unable to explain their necessity or proportionality. In these and

similar instances, it is essential that privacy impact assessments be conducted without delay and that the resulting recommendations regarding safeguards and remedies be immediately acted upon.

I. Health data

73. In April 2017, the Ministry of Health created the National Directorate for Governance and Integration of Health Systems. The Directorate is promoting the digitization of medical history records (in 2019 only approximately 20 per cent of health institutions in Argentina had 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 own database. The Directorate does not have privacy experts among its staff, but works with lawyers of the Ministry of Health to ensure compliance with data protection regulations.

74. In order to protect health data from unnecessary access, each health professional is given different levels of access according to their needs.

III. Conclusions and recommendations

A. Intelligence oversight, security and surveillance

75. **Intelligence services should conduct an in-depth revision of their culture and practices of opacity, currently imposed by law. Making sure that only information that needs to be is kept secret would allow Argentine 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 Argentine citizens.**

76. **A new independent, full-time body should be created whose work should complement that of the Joint Standing Committee on Monitoring of Intelligence Bodies and Services. This new independent entity should contain a blend of senior judges, technical information and communications technology staff and experienced experts in the domain, in adequate numbers, who would have full authority to conduct oversight both ex ante and ex post, including spot checks of both intelligence agencies and police services in order to assess whether any surveillance being carried out is legal, necessary and proportionate. The excellent system of independent public defenders in Argentina should be involved in the work of this independent oversight agency. In accordance 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 that it oversees. It should report independently to the legislature and not to the executive, and thus also be subject to the oversight of the Joint Standing Committee. It would constitute one of the safeguards required for Argentina to meet the standards set in article 11 of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, as amended by the Protocol, which it signed in September 2019.**

77. **More modern and secure information technology systems than that currently being employed by the Legal Assistance Directorate on Complex Offences and Organized Crime should be introduced for disseminating the content of material obtained through the interception of communications. This modernization should ensure that audit trails are much harder to avoid. The use of compact discs should be eliminated and replaced by the transfer of files exclusively over secure information technology systems.**

78. **It is regrettable that parts of the bill on interception of communications and chain of custody (No. S-979/18), duly revised and updated, have not yet made it into the statute book, since the effect would be to increase the legal measures available, and the deterrent effect, to help avoid breaches of personal information obtained through legitimate surveillance.**

79. **Moreover, a system should be introduced, in accordance with international best practices, whereby investigators are not given the entire content of intercepted material, but rather only those parts relevant to the investigations concerned, with transcripts strictly produced by officials who do not form part of the investigating teams.**

80. **Judges' and prosecutors' awareness and knowledge of international standards and tests of necessity and proportionality in a democratic society should be consolidated through dedicated training programmes and modules.**

81. **Privacy impact assessments should be made mandatory by law as a prerequisite for the deployment of all surveillance technologies, including closed-circuit television cameras with capabilities for licence-plate, facial and gait recognition.**

82. **CONARC, the database on which these technologies depend in certain instances, and 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 includes only 0.001 per cent of the population of Argentina, it is clear that it contains errors, and records on individuals who have not necessarily committed serious crimes. Juveniles should be excluded from this database.**

B. Modernizing the data protection law of Argentina

83. **The attempt to modernize the Personal Data Protection Act (Act No. 25,326, of 2000), first launched in September 2018, should be revived.**

84. **The signature by Argentina in September 2019 of the Protocol amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data has de facto created a to-do list for the Government for when it next seeks to modernize federal legislation relating to privacy and data protection. A gap analysis between the current state of legislation and the minimum standards required by the Convention as amended would quickly populate that list, and would have the added advantage of almost automatically leading to modernized legislation that is compliant with the General Data Protection Regulation.**

85. **When such a process of modernization is undertaken, several provisions may be modelled in such a way as to ensure that the adequacy status currently accorded to Argentina by the European Commission is maintained, and that Argentina complies fully with the obligations that it voluntarily accepted when it signed the Protocol in September 2019. In order to do so, a number of new provisions may be introduced that mirror the expectations created by the Convention as amended and by the General Data Protection Regulation in Europe. Fortunately, Argentina is not starting from scratch, and the many resolutions issued by its data protection authority, the Agency for Access to Public Information, have already helped foster a culture in which many of the newer provisions will be part of a continuum. There is much to be commended in the current approach taken by Argentine judges and institutions such as the Agency. The Special Rapporteur strongly recommends that the Government dedicate as much effort to continuity as it does to legislative innovation. The modernization process should entail further refinement of the principles already contained in the Personal Data Protection Act and consolidation of the many resolutions issued over the past two decades, especially since 2016, into one coherent statute. Privacy and data protection laws should not be overly complicated, and should be accessible and intelligible not merely to domain specialists, but to all citizens. It is important that the exercise be conducted as promptly and comprehensively as possible, since the current patchwork of legal provisions, from the two main statutes (the Personal Data Protection Act and Act No. 26,951) and the subsidiary legislation, may be difficult for non-expert citizens to follow.**

86. **The new law should be an opportunity to dispel any doubts and concerns expressed by civil society during the visit of the Special Rapporteur as to the independence of the Agency for Access to Public Information and thus entrench the autonomy it clearly enjoyed in practise to the moment that the subject was last discussed with its director. This would also be an important step to ensure Argentina's compliance**

with its international obligations under the Convention as amended to have a fully independent data protection authority and thus automatically partially satisfy any further expectations for adequacy requirements prompted by the European Union's General Data Protection Regulation.

87. **One of the successful elements demonstrated by the General Data Protection Regulation is the use of hefty fines to secure compliance and this model is therefore strongly recommended for adoption in the new law.**

C. Privacy and health-related data

88. **While the Special Rapporteur notes action taken by the national data protection authority regarding privacy in the context of the coronavirus disease (COVID-19) pandemic, it should be emphasized that such action is far from enough to ensure that health-related data are adequately protected in Argentina. Approximately 80 per cent of health records in Argentina are still to be computerized. Most, if not all, of the issues raised by such computerization of health records and standards to be respected, even in a pandemic, are addressed by the Special Rapporteur in his recommendation on the protection and use of health-related data,** [31] **as explained in the accompanying explanatory memorandum.**[32] **The Special Rapporteur respectfully draws the attention of the Government to the recommendation, which he presented to the General Assembly in October 2019 (A/74/277). He urges the Government to create an administrative task force, in full collaboration with and possibly under the direction of the Agency for Access to Public Information, in order to translate the recommendation into law, practise and policy.**

D. Gender and privacy

89. **During the course of his visit, the Special Rapporteur observed instances in which enjoyment of the right to privacy could be affected by gender, and occasions when indigenous peoples were subject to violations of that right. The Special Rapporteur respectfully draws the attention of the Government to his findings and his recommendations for protecting against gender-based infringements of privacy, including a section on indigenous peoples, which he presented to the Human Rights Council in March 2020 (A/HRC/43/52). The principles outlined therein should be closely respected and implemented in any forthcoming reform of data protection legislation.**

E. Big data analytics, open data, children and privacy

90. **On more than one occasion during his visit, the Special Rapporteur welcomed with appreciation the genuine concern of some Argentine legislators and civil society regarding the privacy of children. In some instances – including in the above-mentioned example regarding the privacy of children in Salta Province – advanced technologies, including big data analytical techniques, had been deployed or contemplated. The Special Rapporteur respectfully draws the attention of the Government to his findings and recommendations on big data and open data, which he presented to the General Assembly in October 2018 (A/73/438) and October 2017 (A/72/540); to his recommendations for protecting against gender-based infringements of privacy (A/HRC/43/52); and to his findings and recommendations on privacy and children (A/HRC/46/37).**

[31] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf.

[32] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf.

F. Harmonizing federal and state legislation, policy and practice

91. **Like all other federal States, Argentina has layers of complications added by the existence of separate constitutions, governments, ministries and legislatures in each of its 23 provinces plus the Autonomous City of Buenos Aires. This creates a number of risks, including lack of harmonization between state and federal law, and gaps in jurisdiction. This was noted, for example, in the above-mentioned case regarding the privacy of children in Salta Province. It appears that the provincial government proceeded with the project without consulting or even informing the Agency for Access to Public Information. Such situations should be carefully avoided in future.**

92. **First, with the advice of experts on constitutional law in Argentina, the benefits of a newly modernized federal law on privacy and data protection – including new provisions on issues such as the protection of health-related data, big data and open data, gender and children, when not immediately applicable at the state level – should be translated into similar, if not identical, provisions in state law and policies in each of the 23 self-governing provinces and the Autonomous City of Buenos Aires.**

93. **Second, if the solution adopted by the provinces – as is the case, for example, in Germany – was to have an independent data protection authority established in each of the 23 self-governing provinces and the Autonomous City of Buenos Aires, a mechanism should be established for the sharing of information and good practices between those authorities. One form that the mechanism could take would be the creation by federal law of a national council for privacy and data protection, chaired by the director of the Agency for Access to Public Information or its successor. The national council could meet at least four times a year, more frequently if required, thus creating a network to facilitate formal and informal consultations and the dissemination of good practices. Models for successful data protection impact assessments could be more easily exchanged and deployed by this network, and successful practices regarding enforcement and compliance, especially for corporate, state and law enforcement use of personal data, could be shared and co-developed.**

G. Role of Argentina on the international stage

94. **The Special Rapporteur strongly encourages the Government to support the Agency for Access to Public Information to continue and indeed expand its emerging role on the international stage. The Agency Director's membership of the Bureau of the Consultative Committee that guides the implementation of the Convention as amended constitutes an important contribution to the further development of global standards in privacy and data protection, adding an essential Latin American understanding to the African perspectives already present in the Bureau of the Consultative Committee and thus successfully complementing existing expertise from European States. The same applies to the active role of the Agency in the Global Privacy Assembly. The Special Rapporteur views Argentina as especially well positioned to take a leadership role in the development and deployment of privacy safeguards and remedies across Latin America.**