por los Derechos Civiles

Contribution to the UN High Commissioner for Human Rights' Report on challenges to the right to privacy in the digital age

April 2018

Office of the United Nations
High Commissioner for Human Rights
United Nations Office at Geneva (CH 1211 Geneva 10)

Introduction

The Association for Civil Rights (hereinafter Asociación por los Derechos Civiles or ADC for its acronym in Spanish) welcomes the opportunity to provide input for the upcoming report that the Office of the High Commissioner for Human Rights is preparing in order to submit it to the Human Rights Council at its thirty-ninth session.

In this submission, ADC focuses on the challenges that the right to privacy faces in an increasingly digital world. The report will take into account several developments that took place in the immediate past, as well as others currently carried out by the Argentine State. In that regard, we will highlight specific cases in order to be used as examples to draw conclusions and offer recommendations for each of the issues addressed concerning the right to privacy in the digital age.[1]

About Asociación por los Derechos Civiles

Asociación por los Derechos Civiles (ADC) is a civil society organisation based in Argentina, that since its establishment in 1995, has worked to defend and promote civil and human rights in Argentina and Latin America, with a special focus on the needs of those in vulnerable situations on the basis of their gender, nationality, religion, disability condition, or deprivation of liberty. Over more than 20 years, ADC raised strategic allegations of human rights violations and promoted institutional reforms aimed at improving the quality of Argentinian democratic institutions. This activity has been recognized at a national and international level for its expertise and efficacy in the defense and promotion of civil rights and democratic values. ADC's Digital Program is focused on the new challenges that digital technologies generate for human, civil and social rights, working crosswise with the

[1] This document was written by Leandro Ucciferri, Eduardo Ferreyra and Valeria Milanes, from ADC's Digital Area. http://adc.org.ar - https://adcdigital.org.ar

organisation's thematic lines, mainly addressing concerns about the right to privacy, freedom of expression, gender equality, discrimination, among others.

State of Privacy in Argentina

Data protection

The end of the 20th Century brought new data protection legislation to the country. The Law 25.326 on Data Protection was enacted in October 2000 and its regulatory decree issued by the President was heavily criticized due to restraining the independence of the Data Protection Authority, the National Directorate for the Protection of Personal Data (DNPDP, for its acronym in Spanish) under the Secretariat for Registry Affairs of the Ministry of Justice. Limited by its dependence on the Executive Power, both financially and administratively, the DNPDP fell short on succeeding in its enforcement role for the data protection framework. Furthermore, the law allows the State to bypass the requirement of consent from the data subject when the collection of the data is performed for the exercise of functions proper to the powers of the State or by virtue of a legal obligation.[2] This has proven problematic as an increasingly data-hungry government introduces initiatives to make use of citizens' information.

In February 2016, the Ministry of Modernization announced a pilot program to implement 'Facebook at Work' in the national administration, used as a communications platform for certains teams within the Ministry.[3] In July 2016, the Executive ordered the transfer of a database from the National Administration of Social Security to the Secretary of Public Communication under the Chief of Cabinet Office, including patronymic information, addresses, emails, phone numbers, birth dates and civil status of almost every Argentine citizen, to improve the Secretary's communication strategy in order to inform citizens and identify issues arising in every district of the country.[4]

In November 2016, the Ministry of Communications and the Ministry of Security announced the creation of the Mobile Communications Service Users' Identity Registry. The resolution, part of a Government action to fight complex and organized crime, establishes that the National Entity for Communication (ENACOM,

[2] Data Protection in Latin America: Opportunities and Challenges for Human Rights, ADC, August 2017: https://adcdigital.org.ar/wp-content/uploads/2017/09/Data-Protection-in-Latin-America.pdf
[3] Por qué el uso de Facebook at Work en el Estado sería un error, ADC, February 23, 2016: https://adcdigital.org.ar/2016/02/23/por-que-el-uso-de-facebook-at-work-en-el-estado-seria-un-error/
[4] El Estado y los datos personales, ADC, July 28, 2016: https://adcdigital.org.ar/2016/07/28/estado-datos-personales/

for its acronym in Spanish) has to adopt the necessary measures "to identify all users of the Mobile Communications Service of the country in a Registry of Users of the Mobile Communications Service". The responsibility of this obligation fell on mobile operators, who proceeded to the designation of the telephone lines, that is, to relate each telephone number with the name of its owner. Such registry violates privacy in that it limits the ability of citizens to communicate anonymously, while at the same time, it facilitates the tracking and monitoring of all users by law enforcement and intelligence agencies.[5]

In August 2017, the Ministry signed a Memorandum of Understanding with Amazon Web Services in order to develop cloud-ready job skills aimed at deploying a range of education, training and certification programs, support the development of cloud-enabled businesses, as well as support the Argentine government in IT modernization efforts, to encourage a cloud-enabled government.[6]

By the end of 2017, the Executive issued a decree with which, among other things, it modified the attributions given to the newly established Access to Public Information Agency, under the Chief of Cabinet Office, turning it into the enforcement body of the Data Protection Law, taking over the former DNPDP.[7] The Chief of Cabinet Office issued an administrative decision ordering the distribution of the budget for the fiscal year.[8] The Agency's budget was cut in more than half of the stipulated budget originally assigned in the law approved by Congress.

The High Commissioner should take into account the following recommendations when assessing the development of their own conclusions:

- Foster dynamic and inclusive mechanisms which allow us to identify and contain risks generated by technological advances. The development of phenomena such as big data, online markets, algorithmic decision making, automatic learning, and artificial intelligence complicate elements of the data protection system, such as the notion of consent. Thus, legal tools such as the "legitimate interest" or the "compatible use of data" emerge, which

[5] Preocupaciones acerca del Registro de Identidad de Usuarios de celulares, ADC, November 11, 2016: https://adcdigital.org.ar/2016/11/11/preocupaciones-acerca-del-registro-de-identidad-de-usuarios-de-celulares/
[6] Novedades sobre el acuerdo entre el Ministerio de Modernización y AWS, ADC, August 22, 2017: https://adcdigital.org.ar/2017/08/22/novedades-sobre-el-acuerdo-entre-el-ministerio-de-modernizacion-y-aws/
[7] ADC alerta sobre los inconvenientes del decreto que modifica la Agencia de Acceso a la Información Pública, October 2, 2017: https://adcdigital.org.ar/2017/10/02/adc-alerta-sobre-los-inconvenientes-del-decreto-que-modifica-la-agencia-de-acceso-a-la-informacion-publica/
[8] Decisión Administrativa 6/2018: http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/305847/norma.htm

enable data processing facilities to act without the knowledge and consent of the data subject. Automated decision making and profiling by algorithms, that few people know or understand, paradoxically exclude their main protagonists. For proper identification, understanding, containment, and conciliation of these circumstances, and for the consequent generation of alternatives consistent with the right to informational self-determination, we must generate dynamic channels and mechanisms which include participation from stakeholders from the various sectors involved (data protection officials, private and technical sector, academia, and civil society).

- Encourage interaction and dialogue to strengthen informational self-determination and its confluence with other human rights. The right to informational self-determination, while guaranteeing individuals control of their data, generates innumerable and permanent situations of conflict with other essential rights. Beyond the procedural and judicial channels, in which the conflicts in question will ultimately be solved, the generation of spaces for interaction and dialogue which allow the rigorous, expert, and permanent debate of the various confluences of the rights in question will enable expertise and will strengthen the right to informational self-determination as an integral part of the human rights of the individual.
- Data Protection Authorities must be independent, without interference from State powers. They should be provided with sufficient resources (economic, human) to comply with their duties as enforcement bodies.
- For cases in which data protection legal frameworks establish exceptions giving an advantage in terms of storage, processing and transfer of personal data, to the State, these exceptions should be admissible under the circumstance of existing matters of serious, essential and urgent public interest.

Biometrics

Biometrics play a big role within the Argentine State's security scheme. The most ubiquitous and pervasive program implemented nationwide, the Federal Biometric Identification System for Security (SIBIOS, for its acronym in Spanish), was introduced via an Executive Decree in 2011, based on a logic of both security and crime prevention. SIBIOS concentrates fingerprints, palm prints, facial records and patronymic information in a centralized database, such information is collected from every Argentine citizen, including newborns, as well as all foreigners entering the country by one of the international airports or sea ports.

SIBIOS allows the National Migration Office, federal forces -such as the Federal Police, National Gendarmerie, Coast Guard, and the Airport Police- and provincial

police forces to submit queries to the whole database for information about anyone in the country, without the prerequisite of a warrant or a similar authorization provided during a judicial investigation. At the beginning of 2017, the Executive Power broadened SIBIOS' outreach by allowing any agency under the Executive or Judicial Power at the national and provincial levels, as well as within the City of Buenos Aires, to sign agreements with the Ministry of Security and join as users of the System.[9]

It cannot be abide that such a widespread system has been implemented by sorting public debate, much necessary for a healthy democracy. SIBIOS not only raises concerns about the legality principle, but also the guarantee of due process itself and the presumption of innocence, by effectively turning every person enrolled in the database as presumed guilty of the crimes under investigation by the police, until they are proven innocent after their biometric information has been analyzed and discarded.

SIBIOS served as a stepping stone for the introduction of other biometric solutions within the State, not only for security and immigration purposes, but for a much broader range of sectors, including social security services, the tax system, education, football matches, and the electoral system. In this last case, it served as another example of technological solutionism encouraged by the government. The National Electoral Chamber introduced a pilot program in northern provinces during the legislative elections in 2017, with the goal of combating cross-border electoral migration by identifying voters with their fingerprints when they arrived at the polling place. During the second stage, the pilot program was broadened to include polling places in the Province of Buenos Aires, far from the northern provinces originally devised. The National Electoral Chamber was not able to produce evidence that the program served its aim of solving cross-border migration originated by clientelism or even asserting the existence of the problem itself.[10]

The trend that governments seem to fall on with the implementation of biometric technologies can be seen spread throughout several Latin American countries[11], where, broadly speaking, such policies are conceived with little to no transparency towards citizenship, which is also linked to the lack of information available to know -with some degree of precision- which technologies are being put in place, what are the mechanisms, processes and protocols for the collection, processing and storage of the biometric data, as well as who is going to have access to it, how is

[9] The Identity We Can't Change: How biometrics undermine our human rights, ADC, December 2017: https://adcdigital.org.ar/portfolio/the-identity-we-cant-change-sibios/
[10] ¿Es necesario un sistema de identificación biométrica electoral?, ADC, November 7, 2017: https://adcdigital.org.ar/2017/11/07/es-necesario-un-sistema-de-identificacion-biometrica-electoral/
[11] Cuantificando identidades en América Latina, ADC, May 2017: https://adcdigital.org.ar/portfolio/cuantificando-identidades-en-america-latina/

the information going to be shared and/or transfered to. Lastly, the lack of sufficient legal frameworks to guarantee an adequate treatment of the biometric data collected, both by the State and the private sector.[12]

The High Commissioner should take into account the following recommendations when assessing the development of their own conclusions:

- Biometric data, which allow or confirm the unique identification of a natural person, must be considered sensitive data, thus its process needs to be subject to strong limitations.
- Biometric technologies have the potential to directly interfere with the right to privacy, the right to one's identity, as well as several freedoms such as expression, association and assembly. In this regard, the processing of vast amounts of biometric data by States, must be necessary and proportionate in accordance to the legitimate aim pursued and enshrined in a law passed by Congress, with aims to foster public debate and develop accountability mechanisms, thus complying with the legality principle.

UAVs and Open-source Intelligence (OSINT)

Argentine State agencies, and specifically law enforcement, have explored the idea of using Unmanned Aerial Vehicles (UAVs) to pursue their goals since at least 2014. For the past three years, we have seen a rise in the popularity of drones used by federal forces for surveillance and various strategic purposes, with projects and initiatives being led by the Ministries of Defense and Security at the national level, as well as various independent initiatives coming from local cities at the municipal level.

Drones are used by security forces as strategic support in their operations, e.g. during raids and patrolling during big public events. The general reasoning followed by State agencies is that, unless it is necessary for the operation to "view" inside a building or house with the drone's cameras and sensors, circumstance under which they need to request an authorization from a judge, otherwise they consider it is under their established powers being able to collect data from public spaces, without requiring previous authorization.

Although there is a temporary set of rules established by the National Civil Aviation Administration, concerning obligations and limitations on the use of drones, as well as a resolution from the DPA addressing the collection, processing and storage of

[12] Desafíos de la biometría para la protección de los datos personales, ADC, May 2017: https://adcdigital.org.ar/portfolio/desafios-la-biometria-la-proteccion-los-datos-personales/

personal data from the use of UAVs, there is no specific legal framework in place for the use of UAVs by federal and local security forces, resulting in a close to non existent oversight of such activities. How the data is collected, processed, stored and used is not transparent, giving way for possible abuses to occur. Furthermore, the national government and the City of Buenos Aires' administration are inclined to pursue a security narrative on the use of surveillance technologies as being infallible to combat crime, as could be seen with the announcement of balloons equipped with high resolution cameras to surveill specific parts of the city, specifically low income neighbourhoods.

Such a narrative has also spread to include online services and social media users. After the current administration took office in December 2015, the Ministry of Security started to pay closer attention to social media posts. A handful of people were prosecuted and charged between 2016 and 2017 for expressing their anger and publishing threats to public officials on Twitter, as a reaction to a series of measures introduced by the recently appointed administration.[13]

In September 2017, the government of the City of Buenos Aires announced the opening of a public tender to purchase a Big Data platform to prevent fraud and tax evasion by identifying and predicting taxpayers' behaviour through social media analysis -e.g. monitoring Twitter feeds-, among other techniques related to the processing of vast amounts of data to predict patterns.[14]

The government's penchant towards social media hit another turning point by early December 2017. Amidst the first days before the beginning of the World Trade Organization Ministerial Conference in Buenos Aires, the Argentine government revoked accreditations to certain Civil Society representatives and activists -that had been already approved by the WTO- claiming security reasons, as some of those people "had made explicit statements to incite manifestations of violence through social media networks, expressing their vocation to provoke intimidation and chaos schemes".[15] Civil Society organizations in the Americas called on the Argentine government to explain what were the security issues taken into account

[13] For more information on the details of such cases, visit Argentina's country report on 'Freedom on the Net', in the section 'Violations of User Rights'; Freedom House, 2017: https://freedomhouse.org/report/freedom-net/2017/argentina

[14] 'El gobierno porteño gastará casi $18 millones en un sistema de datos para espiar hasta los tuits de los contribuyentes', Política Argentina, September 19, 2017: http://www.politicargentina.com/notas/201709/22764-el-gobierno-porteno-gastara-casi-18-millones-en-un-sistema-de-datos-para-espiar-hasta-los-tuits-de-los-contribuyentes.html

[15] 'Sobre la acreditación de ONG's a la Conferencia Ministerial de la OMC en Buenos Aires', Ministerio de Relaciones Exteriores y Culto, December 2, 2017: http://www.mrecic.gov.ar/sobre-la-acreditacion-de-ongs-la-conferencia-ministerial-de-la-omc-en-buenos-aires

and how they arrived to that decision.[16] Critics warned about the potential influence of the Intelligence Agency over the Ministry of Security, and the possibility of undisclosed use of OSINT techniques, given its history of lack of transparency and flimsy democratic oversight.

The High Commissioner should take into account the following recommendations when assessing the development of their own conclusions:

- The processing of personal data collected by the use of UAVs must be prescribed in specific legal frameworks (e.g. in the case of security forces) addressing: limitations on data retention and processing; security measures implemented to protect databases; specific purpose of the data collected; clear guidelines on authorization procedures detailing the circumstances when UAVs can be used; among others.
- The fact that data is 'publicly available' does not justify unregulated and un-checked collection, retention, analysis and other processing.
- Following the UN's Guiding Principles on Business and Human Rights, as well as the EU's GDPR, both private companies and States should carry out Human Rights Impact Assessments –especially concerning the rights to privacy, freedom of expression, association and assembly–, as well as Data Protection Impact Assessments, before the implementation of technological solutions, that are likely to result in a high risk to the rights and freedoms of natural persons.

[16] Preocupa la negación de acreditaciones a organizaciones de la sociedad civil a la reunión de OMC en Buenos Aires, ADC, December 1, 2017: https://adcdigital.org.ar/2017/12/01/preocupa-la-negacion-acreditaciones-organizaciones-la-sociedad-civil-la-reunion-omc-buenos-aires/