GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

ARGENTINA

"Your software is my biology":[1] The mass surveillance system in Argentina

Nodo TAU
Flavia Fascendini and María Florencia Roveri
www.tau.org.ar

Introduction

In 2011 Argentine President Cristina Fernández de Kirchner created, through an executive decree,[2] a federal biometric system for the identification of citizens, named SIBIOS (*Sistema Federal de Identificación Biométrica para la Seguridad*). It was developed, according to the decree, to provide a centralised system of information regarding individual biometrics registers. This would be used for appropriate testing when identifying people and faces, optimising the investigation of crimes and supporting national security.

The adoption of this measure involved very little – almost no – public discussion, except for a few civil society organisations that warned the government about the risks involved in these kinds of surveillance methods, and their implications for people's right to privacy.

Two strong arguments emerged:

- There is a risk involved in this information being in the hands of a government in a democratic regime. In Argentina this argument is made within the context of the dictatorial governments the country experienced following military coups, the last of them extending from 1976 until 1983.
- The low level of public awareness regarding the possible violation of human rights related to the implementation of the system revealed the absence of social debate around the violation of human rights related to information and communications technologies (ICTs).

Policy and political background

Argentina is recognised worldwide for being one of the first countries to adopt biometric technologies as a form of recognition of individuals' legal identity. In the late 1800s, an Argentine police officer named Juan Vucetich established the first system of fingerprint identification[3] and started the use of fingerprint evidence in police investigations.[4]

In Argentina, the national identification document (DNI is its acronym in Spanish) is the only personal identification document individuals are obliged to have. Its format and use have been regulated since 1968 by Law No. 17671[5] for the Identification, Registration and Classification of National Human Potential, which also created the National Registry of Persons. It is issued to all people born in the country, and to foreigners who apply for a residence permit, once the National Directorate of Immigration considers that the applicant meets the necessary requirements to that end. Since November 2009, and as part of the digitalisation of national documents, a new national identification document was issued as a plastic card.

In Argentina, data protection has both constitutional and legislative protection. The constitution states in Article 43 that any person can file an action of *habeas data* "to obtain information on the data about himself, and its purpose, registered in public records or databases, or in private records or databases 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."[6]

At the same time, Law 25.326[7] on the Protection of Personal Data (2000) deals with the administration of public and private databases that include personal information. The legislation prevents any entity from handing over personal data unless it is justified by legitimate public interest. The

1 Cippolini, R. (2010, November 29). Tu software es mi biología. *Cippodromo*. http://cippodromo.blogspot.com/2010/11/tu-software-es-mi-biologia.html

2 Decreto 1766/2011. www.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm

3 Biography of Juan Vucetich, Visible Proofs. www.nlm.nih.gov/visibleproofs/galleries/biographies/vucetich.html

4 Pirlot, A. (2013, December 10). Ignoring repeated warnings, Argentina biometrics database leaks personal data. *Privacy International*. www.privacyinternational.org/blog/ignoring-repeated-warnings-argentina-biometrics-database-leaks-personal-data

5 Act Nº 17.671. infoleg.mecon.gov.ar/infolegInternet/anexos/25000-29999/28130/texact.htm

6 en.wikipedia.org/wiki/Habeas_data

7 www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

law created the National Directorate for Personal Data Protection. Legal experts consider this law an advanced one, because its regulation was prior even to some technologies being used in practice. The Argentine version of *habeas data* is considered one of the most complete to date.

However, as mentioned by the Association for Civil Rights, Argentina "also suffers from a chronic lack of control over its intelligence agencies. Every now and then, the accounts of public officials, politicians and journalists are hacked and scandal erupts. These abuses are the result of an Intelligence Law for which parliamentary oversight mechanisms simply don't work."[8]

Also relevant to the analysis is the Anti-Terrorist Act No. 26.268,[9] driven through in 2007 without parliamentary debate, which aims to punish crimes of terrorism. The Act defined a duplication of penalties for any offence contained in the Criminal Code if committed by an organisation or individual who seeks to create terror among the population or "compel a government to take action or refrain from taking it." This definition could be applied to certain labour or social-related demands. That is why human rights organisations fear that the Act serves to criminalise social protest. In addition to this legal framework that could allow the criminalisation of social protest, the biometric system could offer a tool that aggravates the risk. After the pressure and debate generated around the treatment of the Act, the executive agreed to include a point that establishes that "the aggravating circumstances provided do not apply where the act or acts in question take place in the performance of human and/or social rights or any other constitutional right."[10]

A biometric system for the identification of citizens

SIBIOS, which was developed with the technological cooperation of the government of Cuba,[11] is a centralised database that is fed by information collected by the National Registry of Persons (RENAPER - *Registro Nacional de las Personas*). RENAPER is responsible for issuing national identity documents and passports, a task which used to be the responsibility of the Federal Police. It collects the fingerprints, a photograph and the signature of every citizen who is obtaining an identity document or passport.

After that, RENAPER provides the biometric information necessary for the Automated Fingerprint Identification System (AFIS) as well as the faces used by the Federal Police to satisfy the requirement of identification made by users of SIBIOS. The AFIS started with a database of eight million biometric records collected when the police used to issue identity cards and passports.

The Ministry of Security has the authority over the application of the system, which can be used by these organs of the state: the Federal Police, the Argentine National Gendarmerie, the National Coast Guard, the Airport Security Police, the National Directorate of Immigration and the National Registry of Persons. The national government also encourages provincial entities to use the system, through the Federal Programme of Partnership and Assistance for Security.[12]

The National Office of Information Technology (ONTI), under the direction of the Chief of the Cabinet of Ministers, provides advice related to required standards, equipment compatibility and software and hardware platforms. Since 2011, the team implementing the SIBIOS system has been working closely with the National Institute of Standards and Technology (NIST) in the United States, in order to keep the Argentine software in line with NIST's standards.

The main governmental argument to justify the use of this system is that it is supposed to provide "a major qualitative leap in security in the fight against crime,"[13] a very sensitive issue for citizens these days and clearly the main issue on the public agenda.

A promotional video[14] of SIBIOS – launched by the government – highlights the importance of identity databases in a positive way. "If we know more about who we are, we can take better care of ourselves," states the introduction to the video. It argues that faces, fingerprints and signatures are three essential elements of identity and they should be managed by a very efficient system. It also mentions that in the future the system could integrate other data such as voice, iris scans and DNA.

The video describes the AFIS as a technology used to identify physical characteristics and human behaviour. It also mentions the importance of SIBIOS for the identification of people without identity

8 Álvarez Ugarte, R. (2013, October 30). Argentina's new biometric ID system ignores right to privacy. *IFEX*. www.ifex.org/argentina/2013/10/30/new_surveillance

9 infoleg.mecon.gov.ar/infolegInternet/anexos/125000-129999/129803/norma.htm

10 Act 26.734. infoleg.mecon.gov.ar/infolegInternet/anexos/190000-194999/192137/norma.htm

11 vimeo.com/77142306

12 infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/218789/norma.htm

13 Official presentation of SIBIOS. https://www.youtube.com/watch?v=9goN2MR1TR4

14 vimeo.com/77142306

documents in accidents, economic crimes including phishing, or human and – specifically – child trafficking. It also mentions that the physiognomic recognition of individual's faces that this system uses allows for the projection of how people's faces will change over time.

The government maintains that the implementation of this system also strengthens migratory controls in order to ensure that every person that enters the country is the same person that leaves it. Besides this, the system increases the chances of clarification of solving crimes, providing greater scientific support in the resolution of criminal cases.

Even though the system is considered a step forward as a government resolution to act on these sensitive matters, implementing it could entail some dangers, depending on how it is used in the future:

- SIBIOS collects information from all Argentine natural citizens, as well as foreign residents in the country, by means of the first article of Decree 1501/09.[15] Some of the data collection standards also apply to *foreign individuals who do not have a national ID* such as tourists or travellers in transit who arrive in the country. This actually means that the scope of the data collection exceeds even the 41.09 million inhabitants of Argentina.

- SIBIOS will be *fully "integrated"* with existing ID card databases, which aside from biometric identifiers include the digital image, civil status, blood type and key background information collected since the person's birth. Apparently there is an intention to increase the amount of data collected. Recently a legislator presented a bill that proposes including palm prints among the registries for the system.[16]

- The main criticism of the system is that it contradicts privacy norms and also has implications in terms of the citizens' security, since there are no clearly established mechanisms of control for the system. In this sense, the local organisation *Fundación Via Libre*, with the support of the Electronic Frontier Foundation (EFF), raised the alarm about the implementation of SIBIOS and the risk it implies for people's privacy. The EFF has been warning for a long time about how damaging it is for a free and democratic society to aspire to having "perfect surveillance". Along the same lines, the founder of WikiLeaks, Julian Assange, said that Argentina – although not on the scale of China and the United States – has "the most aggressive surveillance regime in all of Latin America."[17]

As mentioned before, the concerns in terms of SIBIOS relate not only to the power created through data centralisation, but also to different issues regarding its implementation and use. The decree that allows the implementation of SIBIOS does not include adequate mechanisms of control and protection of sensitive personal data. The functions assigned to the coordination unit created to manage the system are not clear and it is not an autonomous body.

There has also been no public discussion about the conditions under which public officials will have access to the data. Yet this type of mass surveillance can have serious repercussions for those who are willing to voice political dissent. The risk is even worse considering other public policies and private initiatives related to monitoring public spaces – such as monitoring streets using video cameras[18] in the most important cities of the country[19] or implementing a biometric system for the identification of people at football games when there is violence.[20]

According to Eduardo Bertoni, an Argentine lawyer specialised in freedom of expression and ICT issues, the deficiencies in the institutional design when it comes to implementing SIBIOS could increase the dangers already predicted by the critics of the system's implementation.[21] Another aspect highlighted by Bertoni[22] is the so-called "right to anonymity", considered as one of the basic guarantees of democracy, because it allows the expression of opinion without fear of reprisal. Consequently, this right also enables freedom of expression.

Conclusions

If we consider SIBIOS a tool implemented for the investigation of crimes, the system is a good resource. However, the issue of the sensitivity of the

15 infoleg.mecon.gov.ar/infolegInternet/anexos/155000-159999/159070/norma.htm

16 www.diputados.gov.ar/proyectos/proyecto.jsp?id=159974

17 Interview with Julian Assange by Infobae. www.youtube.com/watch?v=If7MbOvuEbg

18 Ramallo, F. (2013, August 29). Porteños bajo el foco de las cámaras de vigilancia. *Infotechnology.com*. www.infotechnology.com/comunidad/Porteos-bajo-el-foco-de-las-camaras-de-vigilancia-como-funciona-el-sistema-de-monitoreo-20130826-0004.html

19 CEMAC (Centro de Monitoreo y Atención Ciudadana) www.rosario.gov.ar/sitio/lugaresVisual/verOpcionMenuHoriz.do?id=8726&idLugar=3988

20 AFA Plus. www.afaplus.com.ar/afaplus

21 Bertoni, E. (2013, December 15). Una herramienta peligrosa. *La Nación*. www.lanacion.com.ar/1647828-una-herramienta-peligrosa

22 Interview with Eduardo Bertoni by Infobae, 24 April 2014. www.palermo.edu/derecho/up-en-los-medios/gobernanza-global-de-internet.html

data, and the ways it is used in the investigation of crimes, should be decided in a participatory way in a democratic society. The lack of legislative debate due to the fact that the creation of SIBIOS was decided by a presidential decree leaves the issue out of the reach of public opinion.

There was little consultation before the implementation of SIBIOS with non-governmental and independent entities – which is usually a positive feature of the current government when it comes to shaping policies and legislation that impact on basic human rights. Because of this, there are extremely low levels of awareness of the risks entailed in the collection of such an amount of private data that remains in the hands of the state and within the reach of public security bodies.

Even though the rights to privacy and data protection are enshrined in international law and in the Argentine constitution, national IDs and similar methods of data centralisation increase state capacity for intrusive surveillance. In this sense, the rationalisation for the collection of biometric data in a nationwide ID scheme should be examined to avoid the *unnecessary* collection, processing, retention and sharing of this very sensitive data.

Regarding transparency in the implementation of the system in Argentina, the measure was officially announced in the media at the time it was launched, described as being a technological improvement to help fight crime and as an action framed within the overall modernisation of the state. Since both arguments strike the general public as advancements, this might have negatively affected open, intensive and thought-provoking debate around the real implications of the measure.

Action steps

- In this context, the following action steps can be recommended in Argentina:
- Demand more transparency and accountability from the government in terms of the use of the biometric information, including who has access to it.
- Develop campaigns targeting legislators in order to inform them of the controversial aspects the issue raises in relation to human rights.
- Create awareness campaigns for citizens so they are informed of the risks this initiative poses when it comes to personal data, privacy and surveillance.
- Conduct comparative research on the success and failures of similar systems in other countries where they have been implemented.