UNVEILING THE CYBERSECURITY AGENDA IN LATIN AMERICA. THE ARGENTINE CASE

SECOND PUBLICATION

2

Regulatory framework

por los Derechos Civiles

Privacy Area

January 2016

https://adcdigital.org.ar

Índice

Unveiling the Cybersecurity Agenda in Latin America: The Argentine Case

Second publication: Regulatory framework*

I The project

Discussions on Cybersecurity are taking place in international contexts, as is the case with the Organization of American States (OAS) and its programs, without the participation of civil society and without considering the perspective of human rights protection. On the other hand, these discussions are also being included in national agendas, which include topics such as the State's security, intelligence mechanisms and surveillance practices.

The research projects that have been conducted on the subject matter by ADC, Derechos Digitales and other civil organizations in the region allow us to describe the following scenario: surveillance practices in the Southern Cone, especially those related to intelligence activities, are not aligned with a broad perspective of human rights, lack an adequate control and they usually constitute grounds for illegal actions that end up affecting citizens' rights or weakening the democratic system and its institutions. This is the case as there are Latin American countries that have legal frameworks allowing them to massively obtain information on their citizens; and, even worse, the organisms in charge of collecting this

*This document was produced by the Privacy Area of ADC.

information, intercepting communications and performing surveillance and cybersecurity tasks are often inherited from military dictatorships. This inheritance generally means obscure methods, disproportionate data collection, excessive secrecy, lack of transparency and a large record of human rights violations that have gone unpunished.

This second publication is part of a series of three documents that we will publish on a bimonthly basis under the framework of a research project whose findings will be published during the second half of 2016, and whose main purpose is to determine the existence and content of a cybersecurity agenda in Latin America, focusing especially on the Argentine case in order to determine its alignment with human rights protection standards and, if necessary, make the corresponding suggestions or recommendations.

In the first publication, titled "What do we understand by Cybersecurity?", we focused on defining the term at an international and national level, in order to highlight the lack of a definition despite the fact that the term "cybersecurity" is mentioned in various regulations.

In this second publication, we will analyze the regulation where the term is used and its extent in order to determine the institutional framework of this concept.

II Regulatory framework

In the previous publication, when analyzing what cybersecurity is, we mentioned that the definition may be approached from three different perspectives, which vary depending on who uses the term.

Hence, cybersecurity is referred to as:

- the protection or defense of a State's infrastructure, its networks, data and users;
- the work performed by investigation security forces, prevention and actions against crimes in the digital field (cybercrime);

- surveillance activities conducted by intelligence bodies.

These approaches can be observed in the regulatory frameworks we will analyze below.

i Critical Information Infrastructure and Cybersecurity: evolution

a Resolution by former Secretary of Public Administration N°81/00: creation of the Emergency Response Team on Telecomputing Networks of the Argentine Public Administration (ARCERT, for its acronym in Spanish)

The team was created in 1999 within the former Secretary of Public Administration, dependent on the Presidency of the Cabinet of Ministers, and was empowered to establish the policies for technologies related to computing, telecomputing or telematics, multimedia and telecommunications in regards to computing for the National Public Sector.[1]

According to the Resolution, the National State had made considerable steps towards including computing and communications technologies in its organisms, as well as their interconnection and network development, resulting in an increase of the information being transmitted through the National Public Administration networks, apart from an increase in the complexity of the interconnectivity among networks, which largely resulted from the use of the Internet. Hence, it was necessary to provide the National Public Administration with a technical service in order to address any issues occurring in its networks.

In this way, some of the ArCERT's objectives were: to promote the coordination among administration units of computer networks for the prevention, detection, management and collection of information on safety incidents; propose regulations; provide technical assistance for safety incidents in computer systems; centralize reports on safety incidents; store all information on safety incidents,

[1] http://www.infoleg.gob.ar/infolegInternet/anexos/55000-59999/58799/norma.htm

tools, defense and protection techniques, etc. The ArCERT then became part of the Critical Information Infrastructure and Cybersecurity program.

b Resolution by Presidency of Cabinet of Ministers N°580/2011: creation of the Critical Information Infrastructure and Cybersecurity – I.C.I.C.

The Resolution adopted by the Presidency of Cabinet of Ministers created the National Program of Critical Information Infrastructure and Cybersecurity (I.C.I.C.).[2]

The reasons for creating that program are outlined in the Resolution's recitals, which, among others, highlight that the digital infrastructure virtual communications depend on for their use is a critical infrastructure and, thus, essential for the operation of information and communication systems, which in turn inexorably depend on the National Public Sector and the private sector.

The resolution also stresses that the safety of the digital infrastructure is exposed to constant threats whose materialization may cause serious incidents in information and communication systems; hence, it is essential to adopt the necessary measures in order to guarantee the effective operation of critical infrastructures. For that reason, it is important to create and adopt a specific regulatory framework that makes it possible to identify and protect strategic and critical infrastructures of the National Public Sector, interjurisdictional agencies and civil and private sector organizations that so require, and to guarantee the collaboration of these sectors with a view to developing the adequate strategies and structures for a coordinated response towards the implementation of relevant technologies, among other actions.

This resulted in the creation of the I.C.I.C.,[3] whose general purpose is to elaborate a specific regulatory framework that makes it possible to identify and protect strategic and critical infrastructures of all entities and jurisdictions of the national public sector, interjurisdictional agencies and civil and private sectors that so require, as well as to promote the cooperation and collaboration of these sectors

[2] http://www.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm

[3] http://www.icic.gob.ar/

with a view to developing the adequate strategies and structures for a coordinated response towards the implementation of relevant technologies.

To that effect, the I.C.I.C. shall elaborate and propose regulations; collaborate with the private sector; manage information on safety incidents reporting in the National Public Sector and provide possible solutions in an organized and unified way; establish priorities and strategic plans in order to lead the approach to cybersecurity; warn about identification cases regarding attempts to violate critical infrastructure; coordinate the implementation of response exercises; provide technical assistance for reported safety incidents; centralize reports; store information; elaborate an annual report regarding the state of cybersecurity so that it can be published in an open and transparent way; monitor the services provided by the National Public Sector through the Internet and those identified as critical infrastructure for the prevention of potential cybersecurity failures; raise awareness about the risks posed by the use of digital media; disseminate useful information in order to increase the safety levels of networks, among others.

It is worth mentioning that, in order to participate in the Program, interested agencies, whether from the National Public Sector, interjurisdictional agencies or civil society and private sector organizations, must announce their intention to adhere to the program.

Likewise, the Resolution sets forth that the I.C.I.C. shall refrain from intercepting or inspecting private Internet or network connections under the provisions established by the Personal Data Protection Law and regulatory laws in force.

The I.C.I.C. has for group works:

1. ICIC CERT, designed to handle computing emergencies;

2. Preventive Action Group (G.A.P., for its acronym in Spanish), designed to research and analyze new technologies and computing tools;

3. Critical Information Infrastructure Group (G.I.C.I., for its acronym in Spanish), designed to identify and analyze the country's critical infrastructure, such as telecommunications, energy, oil, gas and financial services;

4. Healthy Internet, designed to raise awareness about the risks posed by the use of digital media in the national public sector.

Through the National Institute of the Public Administration (I.N.A.P., for its acronym in Spanish), the I.C.I.C. provides courses, workshops and conferences that are focused on the training strategy designed by the National Office of Information Technologies (O.N.T.I., for its acronym in Spanish). In July 2014, for example, there was a training called "Introduction to Critical Information Structure and Cybersecurity", which was conducted online and also through distance learning and was targeted at agents responsible for administrative duties in entities and jurisdictions that are part of the National Public Sector, as well as personnel of the private sector and interjurisdictional and civil agencies.

The training was divided into three modules in which, besides the theoretical grounds on the subject (What are critical infrastructures? What is cybersecurity?), specific cases were analyzed in connection with the European Union Agency for Network and Information Security (ENISA), as well as the national cybersecurity strategies of the United Kingdom, Canada, Spain, the United States and Germany.

When the I.C.I.C. was created, the enforcement authority of the I.C.I.C. program was the National Office for Information Technologies (O.N.T.I.), which depends on the Undersecretary of Technology Management of the Cabinet Secretary within the Presidency of Cabinet of Ministers. O.N.T.I.[4] is responsible for implementing innovative computing strategies for the Public Administration; developing systems that are used for management procedures; establishing the standards that must be used by public agencies when new technologies are incorporated; collaborating with other departments in order to create information and management portals; promoting the interoperability of information networks for state institutions. It also coordinates responses arising from attempted attacks and infringement of public agencies' computing networks; establishes security standards and ensures these are complied with by State systems; and implements and controls the use of the State's digital certification, which allows processing

[4] http://secretariagabinete.jefatura.gob.ar/ONTI

records electronically.

c Decree 1067/2015: creation of the Undersecretary of Critial Information Infrastructure and Cybersecurity Protection

The I.C.I.C. program led the National Executive Power to order in June 2015 the creation of the Undersecretary of Critical Information Infrastructure and Cybersecurity Protection, which depends on the Cabinet Secretary of the Presidency of the Cabinet of Ministers, whose main purpose will be to establish the national strategy of critical information structure and cybersecurity.

Decree 1067/2015[5] by the National Executive Power established the abovementioned, based on the improvement of the use of public resources with a view to substantially improve citizens' quality of life, focusing its actions on results which are collectively shared and socially valued.

To that effect, it decided to establish a new organizational structure of political levels, based on rationality and efficiency criteria which may allow a quicker response for society's demands, resulting in dynamic structures and adaptable to constant change.

This decree established that the ICIC Program should depend on the National Department for Critical Information Infrastructure and Cybersecurity, which was created under the scope of the new Undersecretary of Critical Information Infrastructure and Cybersecurity Protection.

It was then decided that the main responsibility of the Undersecretary would be to handle all aspects regarding cybersecurity and the protection of critical infrastructure, including capacity building for the detection, defense, response and recovery when faced with incidents of the National Public Sector.

To that effect, the Undersecretary must undertake similar actions to those established for the I.C.I.C. Program, such as –and just to name a few:

- Handling, assisting with and supervising all aspects connected with the security and privacy of digitalized and electronic information;

[5] http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm

- Establishing regulations and standards designed to increase efforts in order to raise the security thresholds in the resources and systems related to computing technologies;
- Defining the Sample Information Security Policy;
- Collaborating with the private sector in order to establish protection policies for digital security with regular updates;
- Establishing priorities and strategic plans in order to lead the cybersecurity approach, ensuring the latest technological advances are implemented for the protection of critical infrastructures.

Likewise, Resolution 1046/2015[6] of the Presidency of the Cabinet of Ministers created three departments and divisions that depend on the National Department for Critical Information Infrastructure and Cybersecurity.

As a result, three departments were created and they are responsible for different actions. The departments are: Department of Regulatory Elaboration and Interpretation; Technical Department for Critical Information Infrastructures and Cybersecurity and Department of Training, Awareness and Dissemination; plus two divisions: Processes and Projects Division and Development and Research Division.

ii Intelligence and Cybersecurity

a Background. Legal structure of the National Intelligence System.

The creation and evolution of the Argentine intelligence system along with its structure and legal framework were analyzed in our report "The (Non)control of Intelligence Agencies", which can be read and downloaded from our website.

The outrageous death of federal prosecutor in charge of AMIA's case, which took place on January 18 of 2015, after he was found dead with a bullet in his head

[6] http://www.infoleg.gob.ar/infolegInternet/anexos/250000-254999/251022/norma.htm

a day prior to appearing before the National Congress in order to declare for a claim he had lodged involving the highest positions in power clearly showed the pitiful and illegal operation of State intelligence and led to the amendment of the Intelligence law, which involved the creation of a new Federal Intelligence Agency.[7]

The amendment kept a regulation that we consider of utmost importance and which is supported by articles 18 and 19 of our National Constitution. Such regulation establishes that all communications, including any system of object delivery or image transmission, voices or data packages, as well as any type of information, files, records and/or private or read-only documents are inviolable, except an order or court waiver establishes otherwise.

b Decree 1311/2015. The New National Intelligence Doctrine and the Cyber-security Intelligence Operations Department.

On July 6, 2015, Decree 1311/2015[8] came into effect, which created the New National Intelligence Doctrine as a doctrinaire body, the organic and functional structure of the new organism and a new professional regime for the personnel of the Federal Intelligence Agency (A.F.I. in Spanish).

When developing the framework for the "Intelligence for the Democratic Defense and Security", Chapter I in Annex I establishes that the national intelligence is an activity included within the scope of the social and democratic Constitutional State of law that is designed to produce knowledge of any issues –risks and conflicts- involving the national defense and homeland security. The deviation in the purposes of the Argentine intelligence system made it necessary to clarify that the national intelligence must guarantee the protection and good care of Argentine citizens instead of "spying on them". Hence, the national intelligence system is organized as an "observatory" that focuses exclusively on the production and management of knowledge regarding the relevant issues on national defense and homeland security.

[7] http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm

[8] http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm

When defining the issues within the scope of Homeland Security, it establishes that these issues include criminal phenomena that violate citizens' rights and liberties as well as the social and democratic Constitutional State of law and particularly those relevant criminal phenomena of federal nature.

Then it defines the complex criminal phenomena of federal nature:

1. Terrorism and its various global and/or local, state and non-state manifestations;
2. Terrorist attacks against the constitutional order and democratic life,involving political and/or military groups or economic and/or financial groups;
3. Organized crime, particularly drug trafficking, human trafficking, economic and financial crime, arms trafficking, etc.;
4. Any actions against **cybersecurity**, crimes against confidentiality, integrity and availability of computing systems, networks or data, or a part of them, fraudulent use and illegal dissemination of contents. (bold is ours)

Chapter II in the New Doctrine, under "Extent and Activities of National Intelligence" (Annex I) establishes the extent of the national intelligence production, which includes:

1. Strategic national intelligence
2. Counterintelligence
3. Criminal intelligence
4. Strategic military intelligence

Among these four areas, cybersecurity is mentioned in the development of criminal intelligence. It establishes that criminal intelligence "includes production of intelligence regarding criminal issues and, particularly, those complex criminal issues of federal nature related to terrorism, terrorist attacks against the constitutional order and democratic life, organized crime and terrorist attacks against cybersecurity".

On the other hand, Annex II of Decree 1311/15 includes a description of the "Organic and Functional Structure of the Federal Intelligence Agency". In Section II, Chapter 4 develops the operational structure of A.F.I.'s intelligence, which includes the detailed functions and composition of the Cybersecurity Intelligence Operations Department, located at A.F.I.'s headquarters, at 25 de Mayo street, No 11, in the City of Buenos Aires.

The Cybersecurity Intelligence Operations Department is "responsible for producing intelligence in order to gain awareness of the actions taken against cybersecurity in regards to the national defense or homeland security, and of the national or foreign groups that are responsible for performing them".

The Department is composed of two additional departments:

Department of Computing Intelligence: which is responsible for producing intelligence in order to gain awareness of activities regarding risks and conflicts connected with or resulting from the use of information and communication technologies that may affect the national defense or homeland security, and of the national or foreign groups that are responsible for performing these activities.

Department of Cybercrime Intelligence: which is responsible for producing intelligence in order to gain awareness of the activities that may constitute a cyber crime in any form or kind, and of the national or foreign groups that are responsible for performing these activities.

The Cybersecurity Intelligence Operations Department "develops collection, management and information analysis activities and consists of officers and analysts who are experts in cybersecurity".

During a press conference given in July 2015 when presenting the New National Intelligence Doctrine, Former A.F.I.'s Director Oscar Parrilli informed that the Operations Department is responsible for "cyber and information crimes in the modern world, as well as the critical infrastructure in Argentina, which is part of its nuclear power plant, banks and the like and all the protection that has to be provided. In this context, there have been shocking news in the last few years:

the German parliament has been threatened and hacked and institutions have been hacked in the United States and England. In turn, in Argentina we did not have a policy to anticipate, study or undertake intelligence activities on this issue. We have created it and will launch it in the coming days. In addition, we basically pride ourselves on the fact that a very prestigious Argentine computing engineer who comes from the private business world and knows all these topics in depth will be in charge of this organism. He will provide us Argentine citizens with great support so as to avoid this type of threats and actions that may affect security and national defense".[9]

Given the short period of time following the creation of this Cybersecurity Intelligence Operations Department, we have not been able to obtain much relevant information, except for some information obtained from informative notes. In an interview that was published on December 1, 2015, the previous A.F.I. director informed that the Department had been working at full capacity for less than a month and that it was responsible for observing cyber attacks that occurred in the world, analyzing when the country could be said to be threatened and issuing the corresponding warnings if necessary; apart from participating in judicial investigations if the Federal Justice so requires.[10]

III Final comment

The initial conclusions we arrived at in the first publication focused on the difficulty and challenge involved in establishing a definition for cybersecurity, as well as on the consequences on human rights that may result from the potential adoption of a broad or narrow definition.

Given the lack of a clear terminology that will allow us to establish the extent and limitations of the actions taken by the Argentine state in regards to cybersecurity or, in other words, given the lack of a concept, we started to analyze

[9] Parrilli, Oscar. Press conference. Casa de Gobierno. July 7, 2015. Available on: http://www.casarosada.gob.ar/informacion/conferencias/28837-conferencia-del-titular-de-la-afi-oscar-parrilli-en-casa-de-gobierno

[10] http://www.pagina12.com.ar/diario/elpais/1-287308-2015-12-01.html

the regulations in force in order to determine the institutional framework of this entity so as to approach the main objective of this project, which is to determine the existence and content of Argentina's cybersecurity agenda.

2