SURVEILLANCE AND INTELLIGENCE IN THE LATIN AMERICAN CYBERSECURITY AGENDA

COMPARATIVE REPORT: CHILE - ARGENTINA

por los Derechos Civiles

Privacy Area

October 2016

https://adcdigital.org.ar

Surveillance and Intelligence in the Latin American Cybersecurity Agenda

Comparative report: Chile - Argentina*

I Introduction

Under a project developed by The Citizen Lab, this report was made jointly by the Asociación por los Derechos Civiles and Derechos Digitales in order to perform a comparative analysis of the results obtained in previous research on intelligence and surveillance in Chile[1] and Argentina,[2] two countries that are essential to understanding the subject at a Latin American level.

The major goal of the project is to describe the most relevant aspects of cybersecurity in the field of online intelligence and surveillance from a perspective of human rights and public interest coming from civil society and aimed at influencing discussions over these topics both in national and international forums.

Cybersecurity programs are being developed in these discussion spaces and, unfortunately, they lack meaningful participation from the civil society and a human rights perspective. In the Latin American context, this has occurred in the Organization of American States (OAS, for its acronym in Spanish) and in internal discussions of some countries in the continent.

In this respect, it is interesting to observe how discussions and regulations on cybersecurity have evolved in the countries analyzed herein; taking into account they share a recent past shaped by a

*This report was produced by Leandro Ucciferri, Lawyer and Research of the Privacy and Freedom of Expression Areas at Asociación por los Derechos Civiles, and Paula Jaramillo, Senior Researcher and General Counsel at Derechos Digitales.

[1] Vigilancia en Chile: hacia una Política Nacional de Ciberseguridad [Surveillance in Chile: towards a National Cybersecurity Policy], Derechos Digitales, July 2016. Available at (PDF): https://derechosdigitales.org/wp-content/uploads/Politica-Nacional-de-ciberseguridad.pdf

[2] Cybersecurity in the Mass Surveillance Age, ADC, May 2016. Available at (PDF): https://adcdigital.org.ar/wp-content/uploads/2016/09/Cybersecurity-Argentina-ADC.pdf Spanish version available at (PDF): https://adcdigital.org.ar/wp-content/uploads/2016/06/ciberseguridad-argentina-ADC.pdf

democratic rupture and long dictatorship periods. This characteristic has determined the way we understand the powers the State has to monitor its citizens, carrying a legacy that is hard to change regarding the human rights perspective (or the lack of it) in the development of military surveillance and intelligence policies and their subsequent expansion into the digital environment.

This legacy bears defects regarding the transparency of the methods used and the lack of proportionality in data collection, and unfortunately it also involves a record of human rights violations, most of them unpunished.

The work done under this project is expected to serve as a contribution by addressing cybersecurity not only from a historical perspective, but also with an outlook to the future based on the present; and by analyzing those current cases related to the subject, despite the fact that the discussion and treatment of this subject are underway.

In this report we did a comparative work in four main areas:

1. Verification and content of a cybersecurity concept both in Argentina and Chile;
2. The institutions and agencies responsible for the work related to that activity, including the level of specificity the subject has reached in each of the countries under analysis;
3. Applicable laws designed to address online surveillance work or work related to it, even when no specific reference is made. In the last section we mention what happens in both countries regarding the cybersecurity agenda or policies and describe the evolution of that particular process.
4. Finally, relevant cases in both countries to show how cybersecurity issues have been handled when it conflicts with certain human rights.

Finally, this joint exploration will translate into a series of recommendations and suggestions resulting from the studies conducted in parallel.

II Concepts

Based on the research carried out in the respective countries, the first observation is that the subject of surveillance and cybersecurity goes hand in hand with concepts that are unknown to the general public. Regarding human rights, this creates a difficulty for the civil society when communicating, in clear terms that may be understood by all citizens, how these concepts impact their daily lives.

This led us to analyze the regulations in each country in order to understand how various concepts are used and what their implications are. Both the Chilean and Argentine legislations establish similar concepts for intelligence and counterintelligence.

Regarding intelligence, both legislations establish that its purpose is to obtain, systematize and analyze information that is useful for knowing the risks and conflicts that may jeopardize the defense and security of the Nation. On the other hand, with respect to counterintelligence, both countries highlight that it must be aimed at circumventing intelligence activities that may pose a threat or risk to the security of the State. The Chilean legislation provides a more detailed definition as it sets out who the objects of counterintelligence are: other States, individuals, foreign organizations or groups, or their local agents. Such explanation does not exist in the Argentine legislation.

One of the concepts lacking a definition in the Chilean and Argentine legislations is that of surveillance or "surveillance activities". The parallel concept in cyberspace -that of "cybersurveillance"- lacks a definition too.

Regarding the concept of cybersecurity, in the Argentine case we concluded that, at a state level, there is yet no consensus on what cybersecurity is or a unanimous definition. However, despite the lack of definition, the term cybersecurity appears in some regulations and has been used more frequently in the last years.

In Chile, the situation is just the opposite. After the Inter-Ministerial Committee for Cybersecurity was created, which is composed of representatives from the main undersecretariats of the central Government and the National Intelligence Agency, it was discovered that the definition adopted by the Chilean government for cybersecurity involves a condition of reduced risk and the means to reach such condition technology wise.

Regardless of the cybersecurity definition developed by a country, as is the case with Chile, the respective studies allowed identifying various attempts by non-governmental agencies to provide a conceptual framework of what cybersecurity is, what it involves and how it must be approached. Both the United Nations' International Telecommunications Union and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights have published reports in this regard.

III Institutionality

The intelligence system of each country emerged in different periods and contexts. In Chile, its background dates back to Colonial times, in the middle of the 18th Century, and to the War of the Pacific, by the end of the 19th Century. Meanwhile, in Argentina, the intelligence services emerged after the Second World War as part of a global trend to defend the Nation and its interests. Both countries share an obscure past, with the respective intelligence agencies being used as tools to systematically violate citizens' human rights.

In Chile intelligence agencies were created under some branches of the Armed Forces or the Corps of Carabiniers (Cuerpo de Carabineros, in Spanish) during the civic-military dictatorship led by Augusto

Pinochet. The first one was the Military Intelligence Service, which participated in the preparations for the State overthrow and up until the beginning of 1974; the other branches of the Armed Forces also had intelligence services, such as the Naval Intelligence Service, the Carabiniers Intelligence Service and the Intelligence Service of the Air Force.

The Intelligence Military Service was replaced with the National Intelligence Directorate (DINA, for its acronym in Spanish), a secret police directly linked with the Governing Body that was exempted from controls and which had powers to arrest, torture and elicit information under pressure or to imprison persons in its operating centres during the state of exception.

In Argentina, the main national intelligence agency, the former Secretariat of State Intelligence (SIDE, for its Spanish acronym) –currently the Federal Intelligence Agency- was run through secret decrees from the Executive Power for many years until the National Intelligence Law was passed in order to define intelligence activities, narrow the scope of action and establish control mechanisms. The SIDE was closely linked with the dictatorships ruling Argentina during the decades of 1950 and 1970. It carried out internal intelligence activities under supervision of the military and in conjunction with the intelligence departments of the various armed forces, going as far as to run a clandestine detention centre.

The current structure of the Chilean intelligence system is composed of agencies that may be classified into three categories: (a) political intelligence: in charge of the National Intelligence Agency (ANI, for its Spanish acronym), subordinate to the Presidency of the Republic; (b) police intelligence: made up of the Police Intelligence Directorate of Carabiniers and the National Head Office of Police Intelligence; and (c) military intelligence: in charge of the Department of Intelligence of the National Defense General Staff and the Intelligence Directorates of the Armed Forces. In the first two cases, the abovementioned bodies are under the Ministry of Interior and Public Security; in the last case, it is subordinate to the executive power through the Ministry of National Defense.

In Argentina, the National Intelligence System is made up of: (a) the Federal Intelligence Agency, which is the highest body and director of the other agencies. It is subordinate to the Executive Power; (b) the National Directorate of Criminal Intelligence, subordinate to the Interior Security Secretariat of the Ministry of Security, as the superior authority of the criminal intelligence areas of the Federal Police, National Gendarmerie, Naval Prefecture, Airport Security Police and Penitentiary Intelligence of the Federal Penitentiary Service; and (c) the National Directorate of Strategic Military Intelligence, subordinate to the Ministry of Defense, as the superior authority of the intelligence areas of the Armed Forces.

In the context of criminal investigations, the specialized units from the Order and Security Forces are responsible for conducting online surveillance and security tasks in both countries.

In Chile there is the Cybercrime Investigation Squad, subordinate to the Investigation Police, and the Office of Criminal Organizations, subordinate to the Caribiniers. Both the Caribiniers and the

Investigations office are subordinate to the Government through the Ministry of Interior and Public Security.

In Argentina, both the Federal Police, with national jurisdiction, and the Metropolitan Police, with jurisdiction over the City of Buenos Aires, have specialized divisions in cybercrimes. There is the Cybercrime Specialized Prosecution Unit under the scope of the General Prosecutor's Office and the Cybercrime Specialized Prosecutor's Office under the scope of the City of Buenos Aires.

There is a substantial difference regarding the institution that is in charge of cybersecurity public policy-making. Unlike Argentina, Chile is formally transitioning towards the elaboration of a Cybersecurity National Policy, where various agencies are participating: the Department of Organized Crime, Studies Division and the IT Division, both being subordinate to the Ministry of the Interior, which also counts with the collaboration of the Defense Under-Secretariat of the Ministry of Defense and the Ministries of Transport and Telecommunications; Economy, Development and Tourism; Foreign Affairs; General Secretariat of the Presidency; University of Chile; the National Institute of Normalization; the Public Ministry and the Judicial Power.

However, a series of measures were taken in Argentina to reorganize part of the structure of the different ministries after the change of administration and the arrival of the new authorities in the National State. Some of these changes include the creation of the Ministry of Modernization and the Under-Secretariat of Technology and Cybersecurity, which is subordinate to it.

This is the central agency coordinating the various state departments that were working on cybersecurity. The under-secretariat is subordinate to the National Office for Information Technologies (ONTI, for its Spanish acronym), the National Directorate of Technology Infrastructure and Operations and the National Directorate for Critical Information Infrastructure and Cybersecurity. The Under-Secretariat is now responsible for developing a cybersecurity national strategy and has the power to coordinate all agencies in charge of collaborating with the development of said strategy.

IV Legal Framework

In this section of the joint report we will describe the comparative results obtained when contrasting the general characteristics of the current legal framework of both countries as well as the agendas and national policies on cybersecurity.

Regarding the first aspect, it is worth mentioning that one of the noticeable differences between the Argentine and Chilean legal framework concerns the position adopted by each. In the Argentine case, the legal framework clearly focuses on organic and institutional matters of cybersecurity while Chile's legal framework markedly focuses on matters of substantive nature.

In the Argentine case, this perception changed throughout the course of the respective research, as indicated by one of the interviewees, the expert Iván Arce:

"From an institutional viewpoint, the efforts made throughout the last years are a step towards the right direction, but it remains to consolidate that in a national strategy, address conceptual loopholes, narrow down or add what is lacking. [Cybersecurity] is not only a matter of security, defense and intelligence; it involves many things more, such as economic, social and business matters. We are lacking regulatory and technological development aspects, as well as a sustainable cybersecurity environment. We must think of it in holistic terms."

In this respect, it is worth noting that the bodies in charge of cybersecurity tasks have achieved a higher level of expertise, which, at first sight, seems to be greater than that of Chile. In the latter case, the focus has been on the other end of the spectrum: the substantive laws instead of the creation of bodies responsible for them.

This is clearly evidenced when verifying that the legal framework has laws involving privacy protection from the Constitution to more specific laws on surveillance and cybersecurity. These are specially related to the protection of said fundamental right in contexts such as criminal investigation procedures, telecommunications, access to public information, surveillance in public and private spaces, just to name a few.

However, there are some pending issues regarding the creation of specialized bodies in charge of this matter: to date, only one inter-ministerial committee has been created for the elaboration of a national cybersecurity policy, while the other bodies have generic jurisdiction regarding security and surveillance matters, to which they have added activities belonging to cyberspace. In addition, the need to strengthen the incident response centre (CSIRT-CL) has been expressly acknowledged in connection with international reports and the proposal of a national cybersecurity policy.

There is also a remarkable difference concerning the legal framework for the protection of personal data in both countries: In Chile there have been various unsuccessful modification processes in this matter, which resulted in one of the most vulnerable data protection applicable laws in Latin America. On the other hand, in Argentina the problem is different, but unfortunately, in both cases, it has created similar negative results. In effect, Argentina acknowledges that, based on a European regulatory model, the legal standards of privacy protection are high, especially in connection with personal data. Nonetheless, the Achilles' heel lies on the prohibition to process and transfer personal data without the consent of the data holder, unless the databases belong to state agencies.

Hence, the wide scope of the law allows various state agencies to treat personal data beyond what is strictly necessary and proportionate. As a result, the cybersecurity work done by the State is made easier to the detriment of the necessary protection owed to fundamental rights.

In regards to the national or political agenda on cybersecurity, we can affirm Chile has an edge, as

it has a concrete proposal that is publicly known and which has involved citizen participation. It should materialize shortly with the publication of a formal policy.

All in all, the process is underway, despite criticism leveled at the proposal. Generally speaking, such criticism questions the excessive scope of the proposal and the lack of depth in the treatment of the topics that are part of it, as we have mentioned in previous reports.

As for the Argentine case, even though there have been public announcements about the elaboration and, in parallel, the adoption, of a future public policy, the findings of previous reports prove that this has not yet materialized. In this sense, the performance of the National Program of Critical Information Infrastructure and Cybersecurity (ICIC, for its Spanish acronym) has not met expectations as it has worked behind citizens' back and failed to develop and publish the expected products.

There are various reasons to account for this phenomenon, some of which include the lack of budget to carry out the goals initially set out and the lack of guidelines needed for a long-term policy.

In the Argentine case, in the absence of a cybersecurity policy, advances were made through initiatives such as "*Internet Sano*", carried out by ICIC and "*Con Vos en la Web*" from the National Directorate for the Protection of Personal Data. Despite the fact both initiatives were well received and considered a contribution for training purposes regarding technologies and human rights, they are now inactive and nothing has been said about their continuity.

V Cybersecurity and surveillance: cases

In both countries there have been cases related to cybersecurity that may shed some light on how surveillance manifests itself in cyberspace in Latin America. Most of these cases have emerged and been handled by the press, lacking the seriousness they could have enjoyed had there existed a formal and current cybersecurity policy with a perspective of the human rights involved in those cases. In Argentina, it is interesting to see that the only strictly formal information is found in the report "Cybersecurity and Critical Infrastructure in the Americas" from 2015, which was done by Trend Micro Inc. along with the OAS. However, the conclusion resulting from this information only casts more doubts.

The report comments on the work done by ICIC to help pass legislation related to cybercrime and allow for the "successful investigation and prosecution of several cyber-criminal cases", without providing more information on concrete cases for its identification.

Meanwhile, in Chile we have compiled cases dating back many years, in many of which Derechos Digitales has directly participated by conducting concrete work to correct some anomalous behaviors

regarding surveillance displayed by the bodies responsible for the investigation and prosecution of crimes, with diverse results.

It is shocking to verify how these events have affected different ethnic groups, such as the mapuche, as well as university students, whose rights were violated when their social media privacy was disturbed. The extent of the surveillance actions adversely affecting rights in cyberspace seems to be on the increase in a democratic society with a rule of law.

In the Chilean case, the attempts made to this effect become evident in the numerous bills drafted to regulate activities taking place on the Internet or involving technology use that violate fundamental rights.

One last example given as an update of the information contained in the final report on the Chilean case concerns the ruling issued by the Supreme Court at the beginning of June 2016 entering a final decision on the outcome of the telesurveillance balloons installed in two neighborhoods of the capital. In the decision, the Court finally allowed for the cameras installed in these devices to continue working, while openly acknowledging that they do violate citizens' privacy and setting out some conditions for their use (which, based on the analysis done by Derechos Digitales, are very little realistic).[3]

Finally, we should mention the most relevant and notorious case in the last years regarding surveillance in cyberspace, which reached the whole Latin American continent. The case concerns the Italian malware company "Hacking Team", which markets spyware and applications for remote access to electronic devices. Ironically, the company was hacked, unveiling its business relationships with various governments. In the Argentine case, its influence only reached exploratory stages with a view to a potential business. However, the preliminary reports of this investigation informed of the presence of another well-known company marketing surveillance and communication interception software in that country: the American company Blue Coat.

For its part, Chile was proven to be a client of the Italian company, and it became publicly known that the Investigation Police had acquired its software for a considerable amount of money. This purchase was secretly made using state funds. It has yet not been possible to determine how this technology has been used nor who are the citizens being monitored. However, it has been guaranteed that all the applicable legal requirements are being fulfilled.

After analyzing the case in an extensive report done by Derechos Digitales, it has been concluded that, even if the law is being observed effectively when the malware is used, this may prove insufficient, given the scope and context of the legal provisions authorizing the use of surveillance for intelligence or criminal investigation purposes. Such legal provisions were not created for a technological platform specifically, and as a result, the privacy of the individual directly monitored may be violated, as well as that of their contacts in an indirect manner.

[3] For more information please see (in Spanish): http://bit.ly/2dXQHgC

VI Conclusions and Recommendations

Given the lack of international consensus regarding the definitions and scope of cybersecurity, Latin America still has time to advance to a new definition that is not exclusively of military nature or uses intelligence language, but one that is aligned with the acknowledgment and respect of fundamental rights and the international standards of human rights.

Even though there are regional studies on the status of cybersecurity in various Latin American countries, it is essential to highlight the need to conduct more analyses ideally by local working groups rather than by international agencies that tend to echo the responses of state agencies. This way, we could develop policies that help create a healthy cybersecurity environment. It is crucial to assess the scenario to act accordingly.

In Argentina, the initiatives of the last years regarding cybersecurity were on the right track, with the State focusing its work through goals and tasks that were adequate for the development of a cybersecurity agenda. In practice, nothing came out. Chile shows a more developed scenario from a legal standpoint. However, the status of cybersecurity in Chile is not mature enough, as the proposal for a cybersecurity national policy (PNCS, for its acronym in Spanish) involved many topics. As a result, the proposal was not profound enough and it lacked a clear direction, having been designed to bridge other gaps of public policies in other related areas.

There is a substantial difference concerning the way in which cybersecurity has been addressed in both countries. While Chile chose a citizen-oriented process through an open consultation, in Argentina the State approached cybersecurity lacking transparency in its actions, work and results and it has excluded the technical community and the civil society from the discussion, as it lacks a model of multiple interested parties that may be able to provide a broader perspective on how to improve the proposed policies.

Yet, in both countries it is necessary to promote an open debate on surveillance and cybersecurity at a national level involving all the actors of the society in order to guarantee the full development of public policies that necessarily count with an holistic view and reach all strata of society, while creating a social culture with a greater awareness about the importance of privacy.

As a result, based on our joint efforts, we would like to make the following recommendations:

- It is necessary to agree on the elements or axes that will be used to address or narrow down the definition of cybersecurity from a regional perspective, taking into account the Latin American record of democratic ruptures which generally associate said concept with military intelligence and surveillance work. In regards to this point, the vision must be expanded by giving it an adequate perspective of human rights.

- Promote the development of more studies on cybersecurity from and for Latin America taking into account the institutional and regulatory aspects involved in each country of the region.
- Take steps to foster debates on cybersecurity among citizens and the civil society, taking into account their concerns and opinions as part of the process for developing a national cybersecurity policy or agenda and their subsequent assessment.

Based on the respective studies, it was concluded that Chile and Argentina include the debate on cybersecurity in their public agendas as part of an international trend and not based on a real, assessed and concrete need to be faced, and as a result, not even the respective States have a definite idea on how to address or treat the topic correctly, which is an issue that requires a prompt solution.

Finally, it is necessary to mention that, at the beginning of 2016, a group of organizations of the Latin American civil society, including Derechos Digitales and Asociación por los Derechos Civiles, signed a declaration on digital security which establishes ten fundamental points which we understand must be promoted locally in our countries in order to align cybersecurity policies with a human rights perspective.[4]

[4] Latin American Civil Society Declaration on Digital Security, April 2016, available (in Spanish) at: https://adcdigital.org.ar/2016/04/06/oea-declaracion-sociedad-civil-latinoamericana-seguridad-digital/


por los Derechos Civiles