# State Communications Surveillance and the Protection of Fundamental Rights in Argentina

By Verónica Ferrari and Daniela Schnidrig
*in collaboration with the Electronic Frontier Foundation*

August 2016

ELECTRONIC FRONTIER FOUNDATION

CELE
Centro de Estudios en Libertad de Expresión y Acceso a la Información

Daniela Schnidrig works for Global Partners Digital where she focuses on a project about cybersecurity policy. She was an Internet policy and human rights researcher and coordinator at the Center for Studies on Freedom of Expression and Access to Information (CELE) and an advisor in the Bicameral Commission for the Reform, Update and Unification of the Civil and Commercial Codes of the Nation for the National Congress. She has collaborated with the Association for Civil Rights and Human Rights Watch on projects related to sexual and reproductive rights. Daniela holds a law degree from Torcuato Di Tella University, in Buenos Aires.

Verónica Ferrari is an Internet policy and human rights researcher and coordinator at the CELE. Before joining CELE, she worked as a communications and press coordinator for various nonprofit organizations including the Institute of Comparative Studies in Criminal and Social Sciences (INECIP) and the Latin American Institute for Security and Democracy (ILSED). She holds a degree in communication sciences from the University of Buenos Aires.

We would like to thank Katitza Rodríguez, International Rights Director at the Electronic Frontier Foundation (EFF), for leading a substantial revision of this report; and Kim Carlson and David Bogado of EFF, for their editing and formatting work.

This report is part of a larger regional project in Latin America conducted by EFF, an international non-profit organization that has been defending freedom of expression and privacy in the digital world since 1990.

The CELE at the University of Palermo (UP, in Spanish) conducts investigations—from an academic perspective—which serve as useful tools for the defense and promotion of the rights of freedom of expression and access to information. The Initiative for Freedom of Expression on the Internet (iLEI, in Spanish) is a special program within the CELE that is devoted to the promotion of better Internet policies.

# Table of Contents

# 1.

# Normative Power of International Human Rights Treaties That May Affect Communications Surveillance

## 1.1 How Does the State Regulate its Obligation to International Cooperation in Matters of Information Exchange?

There are several international treaties that contain provisions about certain human rights that may be affected by communications surveillance. The right to privacy, which is enshrined in several different international treaties, is the primary right affected by surveillance.

For instance, Article 11 of the American Convention on Human Rights (ACHR) establishes that "No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation." Article 12 of the Universal Declaration of Human Rights (UDHR) provides a similar provision that is also in line with Article 17 of the International Covenant on Civil and Political Rights, which establishes the same, adding that "Everyone has the right to the protection of the law against such interference or attacks."

All human rights treaties that Argentina has ratified are completely binding and applicable in domestic law as was established by the Supreme Court of Justice in "*Ekmekdjian v. Sofovich*," a case on freedom of expression and the right to reply of 1992. In this case, the Court maintained that the Vienna Convention—which has been in force in Argentina since 1980—gives international law priority over domestic law and, also, that "whenever Argentina ratifies a treaty that is signed by another State, all the national administrative and jurisdictional bodies are internationally compelled to apply the provisions of such treaty, as long as they are concrete and can be applied immediately."[1]

This doctrine was explicitly adopted in 1994—the year of the last Argentinian constitutional reform—and established a constitutional hierarchy for the international human rights treaties Argentina had ratified.[2]

This means that Argentina must respect the protections against the possible interference with human rights by State communications surveillance as provided for in the treaties ratified by Argentina.

## 1.2 Are There any International Treaties that Include Dual Criminality as a Constraint for Cooperation?

Because dual criminality is a requisite condition for international legal cooperation in criminal matters, we will analyze the various treaties Argentina has signed with other countries.

Argentinian Law Nº 24,767 on International Cooperation in Criminal Matters applies to cases that involve States with which there are no cooperation treaties signed, or to issues that are not dealt with in cooperation treaties. This law establishes that a person may be extradited only if the act in question is considered a crime by both Argentinian law and the law of the requesting State, and that the criminal penalty faced is at least one year in prison.[3]

In cases where an international assistance or cooperation treaty exists, the State should comply with provisions established by such treaties. Some cooperation documents include the requisite of dual criminality, like the Treaty of Extradition between Argentina and Uruguay,[4] which outlines that crimes that result in extradition must be "classified as crimes by the laws of both parties, which are punishable with imprisonment of at least two years, whatever the denomination for such crimes might be."[5]

On the other hand, the Convention on Mutual Legal Assistance in Criminal Matters between Argentina and El Salvador,[6] establishes that "assistance shall be provided even when the act prosecuted by the requesting party is not classified as a crime by the requested party."

In short, each particular cooperation treaty should be analyzed separately, but it is imperative that a dual criminality requisite is included in the Law of International Cooperation.

# 2.

# Constitutional Framework

The Argentinian constitutional framework protects any fundamental rights that may be affected by communications surveillance.[7] As previously stated, international human rights treaties ratified by Argentina have a constitutional hierarchy. This means the human rights protections that are related to surveillance, and provided for in such treaties, are fully enforceable in Argentina's legal system.

In addition to the protections granted by international law, Argentina's national constitution provides for the protection of several related rights that might be affected by communications surveillance. With respect to the right to privacy, the national constitution maintains "The private actions of a man which in no way offend public order or morality, nor injure a third party, are reserved only to God and are exempted from the authority of judges. No inhabitant of the Nation shall be obliged to perform what the law does not demand nor be deprived of what the law does not prohibit."[8]

The constitution further establishes the inviolability of the home and of communications, since "...the home, written correspondence and private papers of inhabitants may not be violated; and a law shall determine in which cases and for which reasons their search and seizure are allowed."[9] Even though the constitution makes reference to written correspondence, the Supreme Court has extended this protection to communications transmitted via the Internet.[10] (See "Case Law.")

The concept of *habeas data* is also provided for in the constitution. This allows for "Any person" to "...file this action to obtain information on the data about himself and its purpose, registered in public records or data bases, or in private ones that aim at supplying 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."[11]

Additionally, the constitution provides for *amparo* proceedings, which can be expedited and filed "provided there is no other adequate legal remedy against any act or omission of the public authorities or individuals which currently or imminently may damage, limit, modify or threaten the rights and guarantees recognized in 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."[12] This legal tool was used by Halabi, an attorney who requested that the Supreme Court declare an article on mandatory data

retention unconstitutional since it violated privacy and professional secrecy. We elaborate on this case in the “Case Law” section.

We can conclude that Argentina's constitutional framework provides strong protections for the right to privacy, the protection of personal data, and the inviolability of communications. What follows is an analysis of this framework, which includes laws and regulations specifically related to these issues.

# 3.

# Legal Framework

## 3.1 Communications Surveillance in Criminal Matters

Argentina's criminal legislation contains several provisions regarding the interception of private communications. On one hand, the interception of private communications is considered a crime when it is conducted by a third party. On the other hand, the conditions under which the State may intercept communications are regulated in the context of a criminal process.

Provisions related to the conditions under which the State may intercept communications in the context of a criminal procedure can be found in the National Criminal Procedure Code, which was passed in November 2014.[13] This new regulation was meant to enter into force in March 2016,[14] but in December of 2015, a presidential decree postponed its implementation arguing that the application of the new Code "under present conditions might seriously jeopardize the appropriate administration of justice."[15] This decree also states that the Bicameral Commission for Monitoring and Implementing the new Code of Criminal Procedure, together with the Ministry of Justice, shall be in charge of establishing a new schedule for the implementation of this new legislation.[16]

In the section on procedural principles and guarantees, the Code establishes an obligation to respect the protection of privacy (including communications). It maintains that:

> *"The right to privacy, especially freedom of thought, home, correspondence, private documents and any type of communications of the accused and of any other individual must be respected. Only with the authorization of a judge and in accordance with the provisions laid down by this code may these rights be interfered with."*[17]

Below we further elaborate on the criminal process for ordering the interception of communications.

## 3.2 Electronic Crime and Other Types of Crimes

The Criminal Code creates the following penalties for privacy violations with regards to communications surveillance:

*"A penalty of imprisonment from fifteen (15) days to six (6) months will be imposed on those who unduly open or access an electronic communication, a letter, correspondence, a telegraphic, telephonic or any other transfers that are not addressed to him; or on those who take possession of an electronic communication, a letter, correspondence, transfer or any other private document, even when they are not closed; or on those who unduly eliminate or divert the destination of an electronic correspondence or communication that is not addressed to him.*

*The same penalty shall be imposed on those who unduly intercept or seize electronic communications or telecommunications originating from any private or limited-access system.*

*A sanction of imprisonment which ranges from one (1) month to one (1) year shall be imposed when the author of the crime also communicates to others or disseminates the content of the letter, correspondence, transfer or electronic communication.*

*Whenever the crime is committed by public officials abusing their powers, they shall be punished with twice the prison time."*[18]

There is also a penalty for those who, knowingly, through any means, and without authorization or in the abuse of their powers, access computer data or a limited-access system. This penalty is aggravated whenever the system or computer data belongs to a State agency or to a public or financial service provider.[19]

The Criminal Code also establishes sanctions against those who unduly disseminate correspondence, an electronic communication, a telegraphic, telephonic or other type of transfer that was not meant to be published, whenever it causes harm to third parties. Those who act "for the clear protection of the public interest" are exempt from this penalty.[20]

Finally, a penalty is imposed on those who "knowingly and illegitimately, or in the violation of systems of data confidentiality and security, access, through any means, a bank of personal data; or illegitimately reveal or disseminate to third parties the information registered in an archive or in a personal data bank whose secrecy must be preserved as established by the law; or illegitimately insert or have someone else insert data in an archive of personal data." This penalty is aggravated whenever these acts are conducted by public officials.[21]

In 2015, Law Nº 25,520 on National Intelligence, which is analyzed in detail in the following section, provided certain criminal provisions to punish those who, in the permanent or transitory development of the tasks regulated by this law, "unduly intercept, seize or divert telephonic, postal, telegraphic or fax communications or any other type of information,

archive, record and/or private documents whose reading is not authorized nor accessible to the public, and that have not been addressed to them."[22]

If a person is compelled, by judicial order or otherwise, to "destroy or eliminate the records of wiretaps, copies of postal, cable and fax interceptions or of any other element that accounts for the interceptions, recordings or diversions," but fails to do so, this law would consider that a crime.[23] According to this law, any public official that carries out activities that are prohibited by law is also punished.[24]

## 3.3 Communications Surveillance in Intelligence and Counterintelligence Activities

In Argentina, the regulatory framework on intelligence activities is mainly established by Law 25,520 on National Intelligence of 2001[25] and Law 27,126, which modifies the former in many substantial ways.[26] This policy framework also includes decrees that promulgate[27] and regulate[28] both laws and establish the New Doctrine of National Intelligence.[29]

Law 27,126, which was passed in 2015, modifies several aspects of the previous regulation and basically dissolves the agency in charge of intelligence activities and replaces it with the Federal Intelligence Agency (AFI, in Spanish).

According to this regulatory framework, intelligence agencies must conduct their activities in line with what is established in the national constitution and the above-mentioned treaties on human rights ratified by Argentina.[30]

"National intelligence" in Argentina is defined as an activity that deals in the "obtaining, collection, (...) and analysis of specific information related to the events, risks and conflicts that may affect national defense and the internal security of the nation."[31]

This legislative framework for national intelligence, as discussed in a recent study by the Asociación por los Derechos Civiles [Association for Civil Rights] (ADC, in Spanish), must be interpreted in tandem with national defense[32] and internal security law.[33] In the report, ADC indicates that this set of laws "aims at delineating activities and establishing clear prohibitions with the specific purpose of preventing abuses" and notes that one of their main objectives is to determine the concepts and activities related to national defense and national security.[34]

On the one hand, the national defense law regulates military intelligence activities aimed at dealing with "external aggressions." This law clearly outlines that, under no circumstances shall issues related to domestic policy be included in these activities.[35]

On the other hand, the law on internal security does not include the armed forces engaged in internal security activities. An exception arises in situations in which the executive branch determines that a certain threat cannot be combatted by internal security forces such as the federal police, the provincial police, the national gendarmerie, etc. Moreover, this law regulates the intelligence activities conducted by security and police forces.[36]

As noted above, the current regulatory framework indicates that operating intelligence systems in Argentina must strictly adhere to the provisions listed in the national constitution and in the regulations and laws in force.[37] It also establishes that no Argentinian intelligence agency shall be allowed to:

> *"Execute punitive activities, possess compulsive powers, fulfill police functions. They shall not assume functions in criminal investigations, unless a competent judicial authority issues a specific and justified request for them to do so in a particular case within their jurisdiction,[38] or unless they are authorized by law. In this case, all the pertaining procedural rules shall apply to them."[39]*

With the modifications introduced by Law 27,126, the legislative framework establishes that the highest authorities of each agency in the intelligence system must be the ones to order these activities. It indicates that in "emergency situations" these activities may be initiated, provided that they are immediately reported to the highest authorities.[40]

The Argentinian legislative framework in intelligence matters establishes that the interception and seizure of private communications may only be requested by judicial authorization.[41] The law further stipulates that this authorization "shall be submitted in writing and be justified and should contain the telephone number(s) or e-mail address(es) or any other information needed to conduct the interception and seizure of the communications transmitted through them."[42]

Although we will expand on this in later sections, it is necessary to mention a significant shifting of authority that was part of the 2015 reform of the national intelligence system. Previously the Department of Judicial Interceptions was the only Argentinian State body permitted to intercept and seize communications. The power to conduct these activities—at least those authorized or ordered by a judicial authority—was transferred to the Public Prosecutor's Office of the Public Ministry, which is an "independent body, and has functional autonomy and financial independence."[43] Through a decree of necessity and urgency in December of 2015, the then newly-elected President Macri decided to transfer this body to the Supreme Court of Justice.[44]

The Argentinian legal framework stipulates that intelligence agencies must conduct their activities in accordance with is the terms established by the Personal Data Protection Law,[45] which is analyzed further below.

The revelation or dissemination of the information obtained by intelligence agencies requires, without any exception whatsoever, a judicial order or authorization, as stated above.[46]

The law on national intelligence makes reference to the databases stored by the agencies that make up the Argentinian intelligence system. According to this law, data shall be stored in a central location—in so-called Intelligence Archives and Data Protection Banks *(Banco de Protección de Datos y Archivos de Inteligencia)*—which shall be run by an official whose job it is to oversee compliance with "the conditions and proceedings relative to the collection, storage, production and dissemination of the information obtained through intelligence activities."[47]

The legislation further establishes that these data protection banks must monitor information flow in order to guarantee their constitutionality and legality. Any data that is obtained through illegal intelligence activities must be destroyed. Moreover, these data protection banks must guarantee that no information is stored on the basis of race, religious beliefs, private actions, political activities, and membership of social organizations, among others.[48]

As previously stated, the law punishes those who are involved in intelligence activities and unlawfully intercept, seize, or divert communications that are not addressed to them.[49]

### 3.3.1 The New National Intelligence Doctrine

In 2015, Argentina's intelligence system was reformed. The State passed the "New Doctrine of National Intelligence for the Process of Reform and Modernization of the Intelligence System,"[50] which for the most part, aims to delineate the new objectives and tasks of the AFI.

This new doctrine intends to reform and modernize the National Intelligence System.[51] It includes a comprehensive definition of the notion of intelligence: The "collection, management and analysis of information."[52] The decree considers intelligence an "institutional activity that falls within the social, constitutional and democratic State, whose aim is to account for the challenges, coercive measures and conflicts that jeopardize the defense and democratic security of the Argentinian people."[53]

The first annex in the decree that establishes this doctrine indicates that intelligence activities in Argentina "are included in the specific sphere of national defense and internal

security, and they are fundamental to the stability and protection of the democratic system."[54]

It further specifies that national intelligence must ensure the protection and well-being of the Argentinian people, and refrain from "spying on them" *(quotation marks in the original).* Thus, it stipulates that the national intelligence system shall be exclusively devoted to the "production and management of the knowledge related to issues that are relevant to national defense and internal security."[55]

This new doctrine defines internal security as "the security that covers criminal acts that violate the freedoms and rights of the individuals and of the social, constitutional and democratic State."[56] Particularly, it states that the intelligence activities conducted in this sphere shall be devoted to fighting terrorism and organized crime—with a focus on drug and human trafficking.

Intelligence activities are the production of information linked to "attacks against constitutional order and democratic life." Under this new doctrine, economic or financial groups that conduct bank or currency runs, or shortages that could result in a "market coup," are considered attackers against the constitutional order and democratic life.

In line with a preliminary analysis conducted by ADC, enlarging the list of "acts of force against institutional order and the democratic system" that is already defined in the national constitution may be problematic as it "could encourage State practices that may lead to the violation of the rights of the citizenry. The attacks against constitutional order are clearly described in the constitution and the executive branch should not try to expand them by regulatory means."[57]

One of the functions of the new agency in charge of intelligence and internal security in Argentina is that it has to produce intelligence regarding complex federal crimes, for example, cybercrime and "fraudulent use and illegal disclosure of content of communications."[58]

It should be noted that many of the definitions in the doctrine are vague. For instance, the document does not clearly define cybersecurity, which is a problem given that this concept is complex and discussed in global debates on Internet regulation and governance. The doctrine fails to provide details on what type of practices are included under the wide concept of "illegal disclosure of contents." For example, can the online dissemination of content in violation of copyright law[59] be subjected to intelligence activities? All these issues might be dangerous when it comes to surveillance and the exercise of fundamental rights online.

## 3.4 Communications Surveillance in Telecommunications Legislation

### 3.4.1 Argentina Digital Law

The current regulations on telecommunications are established in the "Argentina Digital" law,[60] which was passed in December, 2014. The law was passed after a very short debate in Congress, which was held with little participation from stakeholders in this key sector.[61] This law replaces the former legislation of 1972, except for topics not at odds with the provisions established in this new law.[62]

Regarding surveillance, the "Argentina Digital" law stipulates the inviolability of communications carried out through telecommunications networks and services. Interception, and its subsequent registering and analysis may only be conducted with judicial approval.[63]

The law also lists obligations of those who use information and communication technology services. Article 60 requires that users allow employees of telecommunications services and the recently-created ENACOM [National Communications Body][64] access "in order to conduct any kind of necessary task or oversight."[65]

Some civil society organizations noted that the article's vague wording could pose a risk to users' privacy and go against the articles in the national constitution, which, as stated above, establish the inviolability of the home.[66]

### 3.4.2 Regulations on the Quality of Telecommunications Services

The other set of regulations that should be taken into account is the Regulations on the Quality of Telecommunications Services, which was drafted in 2013 by the Department of Communications.[67] In accordance with the policy framework set by Argentina Digital,[68] this agency, its functions, and its prerogatives are subject to the new enforcement authority, the ENACOM. We analyze the problems that these regulations could have with regard to surveillance in the data retention section.

### 3.4.3 Law 25.891 on Mobile Communications Services

Even though there is no implementing regulation for Law 25.891 on Mobile Communications Services,[69] it is included in the legislation in force, pursuant to the National Website for Telecommunications Users, the official website.[70]

This 2004 law establishes a register of mobile telephone users. Its' purpose? To detect illegal activities conducted on those devices. This law creates a database of lost or stolen mobile

phones, which the State can access "immediately, at any time and any day of the year," upon the request of the Judicial Branch and/or of the Public Ministry."[71]

This legislation goes against the regulations on personal data, since mobile telephone service providers are compelled to collect, retain, and disclose personal data without any limits or objectives established by law. This law, which does not specify what type of data can be requested, compels mobile telephone service providers to share "all the information about their clients and users." Due to its vagueness, this could range from a device owner's personal data to the cell phone model to information about the communications carried through it.

As previously stated, the law does not set a maximum time period for personal data retention nor does it protect against providers who may use the data for reasons that differ from the original purpose of the collection.[72]

## 3.5 Legislation on Data Retention

There is no legislation establishing mandatory data retention periods for Internet service providers in Argentina. However, there are some points worth considering in the aforementioned Regulations on the Quality of Telecommunications Services. These regulations were drafted by the Department of Communications.[73] When the "Argentina Digital" law was passed, the Department of Communications merged with the National Commission on Communications to become the AFTIC, which was then turned into the ENACOM.

Pursuant to these regulations, telecommunications service providers must give the recently-created ENACOM free access to their service equipment and systems and deliver any information that ENACOM requests by deadlines set by this body.[74]

These regulations imply that this public body, with the purpose of meeting the quality standards established in the regulations, could "request any information deemed necessary from telecommunications service providers and set a deadline for its delivery."[75] For quality assurance purposes of the system, providers must grant "full access to their networks and information" to the enforcement authority.[76]

Even though the resolution further indicates that the quality measurement of the service must be conducted in accordance with personal data protection laws,[77] these articles are, to say the least, confusing, and could result in the unlawful use of user data.[78] This could ultimately undermine the previously outlined protections involving judicial authorization.

Regarding data retention, Article 8 in the regulations requires telecommunications service providers to keep all of the data collected by their systems electronically for at least three years so that it may be used for quality assurance purposes established by this law. In addition, it stipulates that the enforcement authority may request "their partial or full delivery and store them for as long as it deems necessary,"[79] which we actually consider discretionary and potentially at odds with international standards.

## 3.6 Rules for House Searches and Computer Equipment Seizures

Rules for searches vary from province to province because the procedural codes are decided by individual jurisdictions. We will next examine the procedures outlined in the National Criminal Procedure Code, which is applicable only to federal crimes.

### 3.6.1 Search Warrant

Whenever there is a reasonable belief that evidence related to an investigation or a suspect related to a crime may be found in a certain place, upon the request, a judge shall order the search of that place, based on a properly-substantiated decision.[80]

The search may be carried out in person by the judge or—if the judge so decides it—by a representative of the Public Prosecutor's Office, by an official duly appointed by the judge, or by the police or any other security force that the judge deems appropriate.[81]

### 3.6.2 Searches

As a general rule, searches must be conducted during daylight hours. However, exigent circumstances may allow investigators to conduct the search at any time of day, as long as the extraordinary circumstances are outlined in the search warrant.[82] The search must be ordered by a judge and a warrant cannot be bypassed, even with the consent of those who reside in the premises being searched.[83]

### 3.6.3 Exceptions to the Judicial Order Requisite

A search may be conducted without a judicial order in the following cases:

- When there is a fire, explosion or flood, or any other situation that threatens the lives of the residents or the property;
- When a complaint has been made on the grounds that one or more individuals were seen entering a house or shop with clear evidence of having committed a crime, whenever it is plausible in relation to the circumstances given;
- When a suspect, who is being pursued, enters a house or shop;
- When voices coming from a house or shop cry for help or indicate that a crime is

being committed therein;
- When there are well-founded reasons to believe that a person is in danger or is being held hostage in a house or shop, the representative of the Public Prosecutor's Office must authorize the search.[84]

### 3.6.4 Requisites of the Judicial Order

The judge shall ensure that formal requisites are met and that the justification for the warrant is well-founded.[85]

The warrant must be presented in a written form and must contain:

- A description of the investigation and the context in which it is being conducted.
- The detailed description of the place(s) to be searched.
- The purpose of the search. The day on which the search is to be conducted, and, when appropriate, the time at which the search may occur.
- The description of the objects that are to be seized or the people who are to be arrested, as well as the agency that will conduct the search.

In serious or emergency cases, the investigator conducting the search can be notified by electronic means or any other adequate means, provided that the communication method used and the identification of the recipient are properly indicated.

If the request was made by telephone, the judge shall require the representative of the Public Prosecutor's Office meet certain requisites.[86]

### 3.6.5 Requirements for Search

A copy of the search warrant shall be delivered to those who reside in or occupy the place where the search will be conducted. When the residents are absent, the warrant shall be delivered to the superintendent or to any person of legal age on the premises, preferably a relative of the resident.

The official in charge of the search must identify themselves before the person being notified and invite the resident or occupant to be present during the search. If no person can be found on the premises, that fact must be placed on record.

### 3.6.6 Precautions to Take in the Context of a Search

The person(s) conducting the search should ensure the right to privacy is as minimally restricted as possible.[87] The search shall be limited to the specific place in which the sought-after objects can be found.

If, while conducting the search, other objects are found that could serve as evidence for the commission of a crime different from the evidence that prompted the search in the first place, the judge or the representative of the Public Prosecutor's Office shall be notified and decide whether it is appropriate for these objects to be seized. There should be a description of the searched property—and the way in which the seized objects were found—on record signed by the participants of the search.

## 3.7 Further Legislation

### 3.7.1 Legislation on the Protection of Personal Data

The right of Habeas Data and the protection of personal data are, as stated before, enshrined in Article 43 of the national constitution. The protection of personal data is regulated in Law 25,326. This law aims to comprehensively protect personal data that is kept in public and private databases. Its purpose is to guarantee the right to dignity and privacy, as well as a person's right to access any personal data the companies have stored on them. [88] This law, the decree that implements it[89]—and its modifications[90]—together with Law 26,343,[91] which amends one article of the former, make up the framework for the protection of personal data.

Article 2 defines personal data as “information of any kind which refers to natural persons or legal entities, either determined or determinable.” It defines sensitive data as personal data that is capable of revealing ethnic origins, political opinions, religious beliefs, union memberships, and information related to health or sex life.

Article 4 indicates that data must be stored in such a way that allows the data subject to access it. Data must be destroyed as soon as it becomes unnecessary or irrelevant to the purposes for which it was collected.

According to an ADC study, even though Argentina's legal framework offers strong personal data protections, it is “structurally weak.” The first of these weaknesses is an excessive permissiveness towards the State in relation to the storage, management, and sharing of personal data.[92]

Law 25,326 prohibits the treatment and handing over of personal data to third parties by the data controller without the subject's consent. However, Article 5 stipulates that consent may be bypassed if the data is collected “with purposes relative to the State's functions or due to a legal obligation.” In other words, the consent guarantee becomes obsolete when the State collects the information.

Article 11 prohibits the handing over of data to third parties without the consent of its subject. Nonetheless, this consent requirement may be bypassed when data is collected for purposes relative to the State's powers and functions or when the data is shared directly between departments within the State's bodies in the performance of their duties.

The personal data law allows the State to manage and share data without the owner's consent through general-term exceptions drafted within the law. This may result in the deprivation of citizens' main data privacy protections.[93]

The other issue concerning the Argentinian policy framework on personal data involves how the law is enforced. The National Department of Personal Data Protection, which operates within the Ministry of Justice and Human Rights, is a weak supervisory body and depends on the Executive Branch.[94]

### 3.7.2 Systems for the Recording and Collection of Data and Surveillance

Argentina is a pioneer when it comes to policies regarding biometrics,[95] which are techniques that allow for the automatic recognition of individuals on the basis of behavioral and physical characteristics.[96] While this is not strictly linked to communications surveillance, it is important to mention that, within the last few years, new digital systems for collecting biometric data have been implemented by the State, substantially increasing Argentina's surveillance capabilities.

Several human rights organizations have studied the trajectory of personal data collection, storage, and usage.[97] Their concerns have to do, for the most part, with the lack of transparency in the State's actions. This includes lack of information about what kind of data is collected, the purposes for collecting the data, how long the data is stored, what kind of analysis is conducted on the data, who has access to the data, and how the data is stored.[98]

These concerns are similar to the ones listed in previous sections about the law on personal data in Argentina and its two drawbacks: (i) that consent is not necessary when personal data is collected for the State's functions or legal obligation and (ii) that it enables several public agencies to exchange personal data.[99]

In the last few years, sensitive data has been inappropriately used and published without authorization and with a purpose different from the one required, which is in conflict with the law on personal data.[100]

### 3.7.3 National Identity Card

In Argentina, the National Identity Card (hereinafter DNI) is the only legal personal identification document. By law,[101] every citizen and foreign resident must have a DNI—which includes biometric data, such as a photo and a thumb fingerprint.[102] [103] In Argentina,

people are required to show this ID for all kinds of interactions: from filing paperwork with a public body to making a bank transfer or credit card purchase.

As a result of Decree 1501/2009,[104] and several resolutions by the National Registry of People (RENAPER, in Spanish),[105] Argentina began issuing the new DNI in 2009. The current DNI is produced using new computer technologies: biometric data and databases for fingerprints, and computer tools for fingerprint verification.[106]

Last year, the Minister of Internal Affairs announced it would launch a new "smart DNI" which, by employing a computer chip, would "interact with other services," such as the Unified System of Electronic Ticket (which is explained in the following section), the Social Security National Administration, and medical records of the Argentinian citizens. [107]

According to a study by Laura Siri on this "smart" ID, the Argentinian State would be able to use information more efficiently and have secure access to the information and data, which is today dispersed. Siri indicates that the Ministry of Internal Affairs and Transport, through the RENAPER, should be in charge of the collection, storage, assessment, destruction, and processing of the new DNI data.[108]

Many human rights organizations are opposed to the initiative that would allow the DNI "to become a portable and digital database containing biologic data and information about citizens' daily routines of transport and consumption, which may be updated and monitored in real time."[109]

### 3.7.4 Metro Electronic System

The Unified System of Electronic Ticket (SUBE, in Spanish) was created in 2010[110] for public transportation purposes. By issuing a card that contains personal data,[111] this system can record all the trips of its users and create a database controlled by the National Department of Transport.[112]

Among the many problems that can arise from such a system, personal data related to trips made by users is accessible to anyone with the card's number. For instance, by entering the card number in the official SUBE website—which does not require a password—anyone can access the trip record made by the user of that card. This would not align with the provisions of the law of personal data.[113]

In fact, this system has already proven itself vulnerable when it comes to the protection of the citizens' personal information.[114]

### 3.7.5 Federal System of Biometric Identification

The Federal System of Biometric Identification (SIBIOS, in Spanish) was created in 2011 by a presidential decree[115] with neither a public debate nor parliamentary discussion. The purpose of the SIBIOS, according to the decree, has to do with greater security and the prevention of crimes.

The SIBIOS, which depends on the Ministry of Security, is a centralized system of national biometric identification that allows security agencies to "cross-reference" information containing biometric and other types of data, which were originally collected by the RENAPER. The main source of information for the SIBIOS is its' database, established by Article 2 of the decree that created the system.

The SIBIOS, according to an ADC report, represents a significant change in the National Registry of Individuals. The national identity document is now key to criminal policies in Argentina. The ADC argues that, before the SIBIOS, the relation between security forces and the National Registry of Individuals was indirect: When the National Police wanted access to information in the RENAPER, they had to request it. Now, under this system, the database of the SIBIOS—as well as the National Migration Office and the RENAPER—is accessible by the federal security forces (the Police, Gendarmerie, Prefecture and Airport Police).[116]

Article 3 of Decree 1176/2011 advocates that each province join SIBIOS, which would allow all provincial security forces access to a unified database to "consult biometric data in real time."[117] According to a book about surveillance in Argentina by journalist Claudio Savoia, provincial security forces have already joined the system and are now sharing their databases among 15 Argentinian provinces. In December 2014 the system had already registered 13,2 million fingerprints.[118]

According to the ADC, SIBIOS represents the consolidation of databases that were previously scattered in various locations and greater access to data by the State's security forces.[119] This system conflicts with the protection of personal data law,which stipulates that data may not be used for purposes that are different from or incompatible with the purposes that prompted its collection.[120]

### 3.7.6 Provisions of the National Department of Personal Data

As previously stated, the National Department of Personal Data Protection (DNPDP, in Spanish), which depends on the Ministry of Justice and Human Rights, is the agency in charge of enforcing the law on personal data. The DNPDP recently published a series of regulatory standards and some of them are related to surveillance.

### 3.7.7 Collection of Personal Data Using UAVs or Drones

Provision 20/2015[121] understands that, according to the law on personal data, an image, video or audio of a person represents information that is personal and as such, must be included in that regulatory framework. This provision regulates, in particular, the capabilities of the Unmanned Aerial Vehicles (UAVs) or drones to collect information.[122] This concern has caught the attention of human rights organizations, since their usage may pose serious threats to the right to privacy, among other rights.[123]

The provision also points to the fact that UAVs or drones[124] collect personal data in a "peculiar" way, which "might pose a great risk to the rights to privacy and of informational self-determination."[125]

Annex 1 of this provision describes the "legal conditions under which personal data may be collected by drones." The first article of this annex stipulates that collecting personal data (be they pictures, videos, audio, or any other) using drones shall be legal as long as it is conducted with the consent of the data subject, pursuant to Articles 5 and 6 of the protection of personal law.

However, according to this provision, it is not necessary to obtain consent from the data subject when (i) the means to collect the information does not "disproportionally infringe upon privacy," (ii) the data is collected in a public gathering and (iii) the national State collects data "in the performance of its duties." This last item, pursuant to the National Law on Personal Data, grants excessive powers to the State and its data collection capabilities.

Article 2 of this provision, related to data collected by drones, stipulates that, to ensure the right to privacy is not adversely impacted, the collected data is proportionate, relevant, and strictly necessary to the aim for which it is being collected. Also, it adds, that in order to comply with personal data regulations, those responsible for managing or collecting the data must implement a policy on personal data management and privacy and describe, among other things, the purpose of the collection, how long the data will be retained, and the technical mechanisms employed to ensure its security and confidentiality.

Article 3 requires databases containing information collected by UAVs to be registered with the National Data Registry, however drones that are used for "recreational purposes" are exempt from this requirement under Article 5.

This provision also establishes that certain precautions must be taken in order to avoid collecting sensitive information, such as personal information obtained from health institutions, religious facilities, and political or union demonstrations.

### 3.7.8 Regulations on Video Surveillance

The Argentinian State has increasingly been using security cameras within the country.[126] For example, local authorities from Conurbano, a province of Buenos Aires, have employed approximately 12,600 cameras, according to a 2015 report.[127] Regulations on video surveillance are determined by province. Law nº 2,602 regulates video surveillance in Buenos Aires,[128] Law nº 13,164 regulates it in Santa Fe,[129] Law nº 9, 380 does so in Córdoba, Law nº 5,984 in Corrientes, and so forth.

Nationwide, the DNPDP provision establishes the conditions under which the collection and management of digital images for the purpose of security are legal.

Article 1 of the DNPDP follows the provisions in the personal data protection law by indicating that the collection of digital images through security cameras shall be legal with the consent of the subject being recorded.

However, there are loopholes in this provision. The DNPDP establishes that prior consent is not required if the collection of personal images does not represent a "disproportionate intrusion" on privacy. In other words, prior consent is not necessary when the data collection is conducted by an event host or by the State in accordance with its functions. Consent is also not required when the data is collected on private property—including spaces that are rented or leased.

Article 2 stipulates that collected images may not be used for any other reason than the originally stated purpose. Also, it dictates that the State "may only order their public disclosure when it is authorized by law or by the decision of a competent official, having a general interest in mind." And, just like the other norms enacted by this body, it establishes that the collected data must be adequate, relevant, and strictly necessary for the stated purpose, and that any restrictive measure on the right to privacy must be specifically avoided.

The provision also establishes that images that are captured in violation of individuals rights must be purged upon request of the individual whose data was collected.

Those in charge of collecting and managing digital images for purposes of security must implement a privacy and personal data management policy. The policy must establish a retention period for images, and instructions for purging the data after the period has elapsed.[130] Also, the legal conditions provided for by Law nº 25,326 must be put into practice.[131]

Similar to the information obtained by drones, the databases that store personal data collected by security cameras must be registered with the National Registry of Data.[132]

### 3.7.9 Best Privacy Practices for Application Development

The National Department of Personal Data establishes a guide of rules for the protection of personal data in the development of applications by enforcing privacy policies during app development.[133]

The guide warns about the capabilities of applications to obtain, use, and transfer personal information and emphasizes that "data" is the property of its subject, irrespective of where the data is stored or how it is used. The guide emphasizes that people have the right to control how their personal information is used.[134]

Section 2 references the principles of privacy and indicates that data management can only be legal if the data subject has given consent—unless, of course, one of the aforementioned exceptions provided for in the regulatory framework is applicable.

This guide urges app developers to be transparent about how they use data and to build their apps with *privacy by design* and *privacy by default* in mind. It also urges them to establish clear privacy policies.

Similar to the provisions mentioned above, this guide establishes that the collected data may only be used in accordance with the aim for which it was obtained. Such data must be strictly relevant to the purpose that prompted its collection, and it may not be obtained via unfair or illegal means. Finally, the data must be destroyed when it becomes irrelevant.[135]

# 4.

# Case Law

In 2009, the Supreme Court ruled on the "Halabi" case, which was and still is the most important court decision related communications surveillance.

Modifications to the Telecommunications Law were passed in 2004. In an effort to better fight crime, three articles were added, which required communications service providers to possess the necessary resources to "capture and divert communications, in order to monitor them remotely upon the request of the Judicial Branch or the Public Ministry," and to keep such data for 10 years. These articles were initially regulated by a decree, which was suspended a year later.[136] However, even though the regulations were suspended, the law on communications interception was still in force.

Attorney Ernesto Halabi filed an *amparo* action, arguing that these three articles were unconstitutional on the grounds that they violated the right to privacy and made it impossible for him to guarantee his clients professional secrecy.

The case worked its way up to the Supreme Court which ultimately ruled that communications data transmitted by appropriate means is protected under personal privacy. Such communications data is covered by the constitutional provisions that protect privacy and establish the inviolability of home, and also by the Universal Declaration on Human Rights and the American Convention on the Rights and Duties of Man.[137]

Regarding the State's powers to guarantee security and maintain public order, the Supreme Court quoted the Inter-American Court of Human Rights on the case of "Bulacio," where it was stated that State's activities are limited by the fundamental rights of individuals.[138]

The Supreme Court then maintained that intrusions into the private lives of individuals are only justified when they are provided for by law—and as long as there is a greater interest in protecting individual freedoms, social defense, public morals, or fighting crime.[139]

The Court referenced prior judgments in which a breach of the inviolability of correspondence would have been acceptable:

- When there is a law determining the "cases" and "justifications" for which the content of such correspondence needs to be known;
- When the law is based on the existence of a substantial or important aim of the

State (...)

- When such restriction is compatible with the pursued legitimate aim, and
- When the means to achieving it does not exceed what is strictly necessary. At the same time, the aims and means must compensate for the interferences they may have caused with other interests.[140]

The Court considered that the articles in question did not meet the above-mentioned requirements. The articles failed to describe the cases or circumstances in which interceptions could be conducted, and did not provide for a specific system that would protect communications.[141] For these reasons, the Court declared the articles unconstitutional.

# 5.
# Institutional Framework

## 5.1 Organizational Chart of the Bodies Involved in Criminal Prosecutions

Argentina has adopted a federal-type government structure,[142] which means more than one territorial center has the capacity to adopt laws. The unity of the State is balanced by the plurality and autonomy of the provinces.[143]

The national constitution delegates any substantive legislation to the National Congress: Civil, Commercial, Criminal, Mining, Labor, and Social Security codes. Nonetheless, it establishes that, depending on the jurisdictions to which cases or individuals belong,[144] either the federal or provincial courts are responsible for enforcing it. The goal is to maintain unity and consistency, and at the same time, respect the autonomy of each province to delineate procedural codes for the implementation of substantive law.

This means that the Criminal Code is enacted by the National Congress and applied throughout the country. Provinces cannot issue their own criminal codes, however procedural codes are promulgated by each jurisdiction.

This makes it difficult to describe all of the actors and bodies involved in criminal prosecutions in Argentina and also to outline a procedural diagram for communications interception since both vary according to jurisdiction. Thus, we look to the Federal Code of Criminal Procedure as an example, which applies to crimes under federal jurisdiction, since many provincial regulations follow the regulations in the federal code.

***Bodies Involved in Criminal Prosecutions***

*– Jurisdictional Bodies:*[145]

- Judges for review;
- Trial judges;
- Court of jurors;
- Supervisory judges;
- Enforcement judges.

*– Public Prosecutor's Office:*[146]

- Security authorities provide legal assistance to the agencies involved in criminal prosecutions.[147]

## 5.2 The Criminal Process for Communications Interception

The National Criminal Procedure Code establishes the following steps for communications interception:

- The judge may order, upon the request of one of the parties, the interception and seizure of postal or telegraphic correspondence or of any other object sent by or to the accused.[148] This procedure is similar to the one for searches.
- The interception of communications shall be an exceptional measure and may only be conducted for a maximum of thirty (30) days. This period may be renewed if there are reasons that justify the prolongation of this term given the nature and circumstances of the crime under investigation.[149]
- The communications interception request must indicate the period of time that is deemed necessary to carry out the measure according to the circumstances of the case.[150]
- The judge must consider the legality and reasonableness of the request, and make a well-founded decision whether or not to authorize it.
- Officials in charge of conducting the interception are required to respect the confidentiality and secrecy of the information obtained through such interception, except when handing it over to the authority that initially requested it. Those who failure to comply with this obligation shall be held criminally liable.[151]
- Companies that provide communications services must facilitate the immediate accomplishment of this surveillance task. Otherwise, they may also be held criminally liable.[152]
- The interception must be stopped if the reasons used to authorize the surveillance disappears, or once the time period given has elapsed or the aim has been achieved.

### 5.2.1 Seizure of Data

- The judge may order, upon the request of a party and through a warrant, the seizure of an entire or partial computer system or of data stored on a storage disk or hard drive with the purpose of seizing the elements of the system, copying the system, or preserving data or information of interest for the investigation.[153]
- The party who requests the interception of communications is responsible for examining the objects, documents and other result of the interception.[154]
- Any elements that are seized, but unrelated to the investigation shall be returned to their rightful owner and any copies that have been made shall be destroyed.[155]

- The data subject may turn to the judge to ensure that the elements are returned and that any copies are destroyed.[156]

### 5.2.2 Accessing the Intercepted Objects

- Once the correspondence or intercepted elements are ready, a representative from the Public Prosecutor's Office will open them. He or she will examine the elements and read the contents of the correspondence.[157]
- The representative from the Public Prosecutor's Office must explain to a judge, in a one-party hearing, how and why the seized objects are related and necessary to the investigation. [158]
- The judge shall keep any remaining content confidential and order its return to the data subject, his or her representatives, or close relatives.[159]

On the other hand, Law Nº 25,520 on National Intelligence establishes that the Federal Intelligence Agency has the power to conduct criminal intelligence gathering. It may occasionally request communications surveillance in connection with complex federal crimes related to terrorism, cybercrime, drugs, arms, and human trafficking, etc. It may also do so for crimes against economic and financial public order and crimes against public authorities and constitutional order. It has its own means of collection. This process is explained further below.

## 5.3 Organization Chart of Intelligence Bodies

Under Law 27,126 (which modified the Law on National Intelligence), the system of intelligence in Argentina is made up of, first and foremost, the Federal Intelligence Agency (AFI, in Spanish).

The AFI is the highest intelligence authority in Argentina and it controls the other agencies that make it up.[160] The AFI depends directly on the National Executive Branch—in fact, the highest authority in the National Intelligence System is the president of Argentina, who is in charge of shaping the National Intelligence policy.[161] The head of the AFI is its director general who has the status of a minister and is appointed by the Executive Branch with approval from the Senate.[162]

According to the New Doctrine of National Intelligence, which is the recent legislation that provides for Law 27,126 and delineates issues related to intelligence, the AFI's functions are as follows:

- To gather national intelligence by obtaining, collecting, and analyzing information related to the offenses, risks, and conflicts affecting national defense and domestic security, through the bodies that make up the national intelligence system.
- To gather criminal intelligence related to complex federal crimes of terrorism,

cybercrime, drugs, arms and human trafficking, and crimes against economic and financial order, or crimes against public authorities and constitutional order.[163]

The other agencies that make up the Argentinian intelligence system are:

- The National Department of Criminal Intelligence (DINICRI, in Spanish), which depends on the Ministry of Security.[164] The DINICRI gathers criminal intelligence,[165] unless it is related to complex federal crimes or offenses against public authorities or constitutional order. These functions were directly transferred to the AFI.[166]
- The National Department of Strategic Military Intelligence (DINIEM, in Spanish), depends on the Ministry of National Defense.[167] The DINIEM gathers the strategic operational and tactical intelligence in order to plan and conduct military operations and specific technical intelligence gathering.[168]

## 5.4 Procedures Carried out by Intelligence Bodies to Intercept Communications

Pursuant to Article 4 of Law 27,126, "intelligence activities must be ordered by the highest authorities in each agency." However, this article also adds that "in cases of emergency," these activities "can start, but they need to be immediately reported to the highest authorities in each of the intelligence agencies."

In order to intercept private communications, the AFI must request judicial authorization."[169] Such authorization, as stipulated by the legislative framework, "must be granted in writing and be justified with a detailed description on how the telephone number(s) or e-mail address(es) or any other communications are going to be intercepted or seized."[170]

The director general of the AFI, or another official shall request the judicial authorization from a federal judge with jurisdictional authority. The jurisdiction is defined according to the address of the person(s) whose communications are to be intercepted or by the place where they are held in the case of mobile or satellite communications.

Authorization to intercept communications shall be granted for a period no longer than 60 days, which shall automatically lapse, unless the director or appointed official formally requests that the period be prolonged for an additional 60 days (as long as it is absolutely required in order to complete the investigation).[171]

Once these terms have lapsed, the judge shall initiate the appropriate proceedings or, alternatively, order the destruction of all the elements that were intercepted.[172]

When Law 27,126 was adopted, the former Department of Judicial Interceptions (DOJ, in Spanish)—which was the only State body in charge of conducting communications interceptions or seizures—was transferred to the Public Prosecutor's Office of the Public Ministry an independent body that has operational and financial autonomy. After the transfer, the DOJ changed its name to Department of Interception and Recording of Communications (DICOM, in Spanish).[173]

Judicial orders for telephone communications interceptions were sent to the DICOM with precise instructions on how the interception should be conducted (for example, which numbers should be intercepted). Then, the DICOM would send the request to the telephone service provider in charge of diverting the communication.

These new regulations transferred not only the operations to the Public Prosecutor's Office, but also all the computer databases and the previous agency's documents and information about prior-conducted interceptions..

The legislation also created the *Comisión de Administración de Registros de Intervenciones Concluidas,* which was responsible for protecting any files linked to intercepted communications during the transfer.

As previously mentioned, the newly-elected President Macri decided in December 2015 to transfer the DICOM to the Supreme Court of Justice. Pursuant to this decree, the Minister of Interior[174] is responsible for criminal prosecutions and thus has a specific aim. So, in order to guarantee due process, the interception of communications should be ordered by a body that is independent from the criminal investigation process. In this case, the decree establishes that such body must be the Supreme Court.[175]

The DICOM transfer was postponed by the Supreme Court to February 2016.[176] In February, when the transfer was official, the Supreme Court renamed the DICOM the Department of Capturing of Communications of the Judiciary (DCCPJ, in Spanish) through decision No. 2/16 (*Acordada* No. 2/16).

The *Acordada* No. 2/16 states that communications interception must be conducted in line with the telecommunications framework, the National Intelligence Act, and the Argentina Digital Act mentioned above. According to this decision, the Supreme Court retains the authority to change any regulations it has over the DCCPJ.

This decision sets forth some principles which, according to the Supreme Court, should guide the interception of communications:

1. Transparency and confidentiality: An efficient oversight mechanism should be established; it must require employees working at the DCCPJ to agree to keep any information they encounter confidential. A document that guarantees the "chain of custody" which would protect the confidentiality of information gathered through the interceptions must also be created.

2. Training: Those in charge of intercepting communications must be trained to appropriately use the most efficient mechanisms and technologies for interception and evaluate the "opportunity" and duration of the interceptions. The regulation establishes that members of the DCCPJ may assist judges and prosecutors directly from their offices or "remotely."

3. Data mining: Data mining practices used for surveillance must be updated. Any attempt to discover information using "great volumes of data" should be pursued in a way that helps judges and public prosecutors.

4. New technologies: New technologies shall be pursued and the best practices of other judicial offices around the world should be studied and replicated.

5. Relationships with telecommunications companies: There shall be confidentiality agreements and shared audits of current and future technologies with telecommunications companies as well as with others who provide usable services.[177]

The DCCPJ shall remain independent from the Supreme Court, and run by a general director—who shall be a criminal judge—for one year only. Moreover, the decision states that the DCCPJ shall have a board of directors, but it is unclear as to how these board members are to be elected.

Two other bodies were created during this transfer: an advisory commission made up of experts in the field and an advisory council made up of civil society institutions and organizations in order to establish mechanisms to guarantee transparency and participation.

In the Court decision that created the DCCPJ, there is no reference to mechanisms by which civil society and academics could participate nor does it make reference to any external oversight proceedings.[178] However, there are aspects of the DCCPJ's regulation that have yet to be defined by the Court.

Pursuant to the decision, the DCCPJ shall be the only state agency in charge of conducting private interceptions and seizures of any kind, provided they are "required by the judges and the Public Ministry," and comply with the aforementioned principles. Even though several articles in the Court decision state that interceptions will be conducted when the competent

judicial authority requests them, civil society organizations have warned about the ambiguous language used in that sentence, since "it could be interpreted [as meaning] that the Public Prosecutor's Office has the authority to request the interception of a given communication directly to the DCCJP, without judicial authorization."[179] The Association for Civil Rights (ADC, in Spanish) has suggested that this segment be rephrased in order to avoid confusion, which may affect due process.

In the same document, the ADC also draws attention to the use of the phrase "data mining" [minería de datos] used in the Court decision: "The introduction of the concept of data mining is thus very revealing: it highlights practices that we suspected exist, but are not adequately regulated by any norm, of any level, which curbs a state power which, by definition, violates the rights of citizens."[180]

Taking these changes into account, the process for the interception of communications includes the following:

- Request by the AFI
- Judicial Authorization (criminal federal judge with jurisdiction)
- Department of Capturing of Communications of the Judiciary (DCCPJ, in Spanish), Supreme Court of Justice.

# 6.

# Oversight Mechanisms

## 6.1 Entities Authorized to Intercept Private Communications without Judicial Orders

According to the legislation on crime and intelligence mentioned in previous sections, the interception of communications cannot be carried out without prior judicial authorization.

## 6.2 Obligation to Submit Transparency Reports and to Implement Public Oversight Mechanisms

There is no obligation to submit transparency reports as part of the criminal process related to communications interception. In the intelligence process, intelligence agencies are compelled to submit annual confidential reports about their intelligence activities to the Bicameral Commission on the Supervision of Intelligence Bodies and their Activities.[181] The functions of this Bicameral Commission are set out below.

### 6.2.1 Bicameral Commission on the Supervision of Intelligence Bodies and Their Activities

This parliamentary supervisory body was created in 2001, when the Law on National Intelligence (№ 25,520) was passed. According to this law, the Commission shall, among other functions, supervise the various branches of the National Intelligence System, control their performance to ensure that they strictly follow legal and constitutional norms, and monitor intelligence activities.[182] Monitoring intelligence activities includes collecting, analyzing and assessing the execution of the National Intelligence Plan; assessing the Annual Report on Intelligence Activities; and elaborating and submitting a secret annual report that evaluates the activities, performance, and organization of the National Intelligence System with regard to the National Intelligence Plan to the Executive Power and the National Congress.[183] This law grants the Commission "great powers to control and investigate on its own initiative." However, the law is limited since "the access to such information will be authorized in each case by the President of the country or by the official specially appointed to do so, taking into account all the exceptions provided for by this law."[184] This provision subordinates the powers of the Commission to the will of the controlled ones.[185]

The Commission started operating in 2004, when it was given the funds it needed to operate.[186] In practice, the Commission purportedly operates in complete secrecy, even in cases that are not—or should not be—secret.[187] For instance, it does not publish information about its meetings nor agenda on its website.[188]

In December 2012, a number of civil society organizations and members of the Citizens' Initiative to Control the Intelligence System (ICCSI, in Spanish) submitted a request to access information related to the Bicameral Commission.[189] They requested information about the Commission's meetings, copies of non-secret reports it drafted, and information about whether it conducted investigations on its own initiative. Despite the fact that the request was submitted twice, the government has not yet responded.[190]

In February 2015, it was revealed that the Commission had met to analyze the reform project for the Intelligence Law.

As stated above, the resolution that created the DICOM also set up an advisory commission, made up of experts in the field. Furthermore, it urged Congress to create a Bicameral Commission in the Public Ministry to oversee the performance of the DICOM.

With the transfer of the power to intercept communications to the Supreme Court and the creation of the DCCPJ, no independent oversight mechanisms were established to guarantee transparency and accountability. However, as mentioned before, there are some aspects about this regulation that have yet to be defined by the Court.

## 6.3 Mechanisms for Deferred Notification

Both criminal and intelligence processes for communications surveillance lack procedures for deferred user notification.

In the criminal process, only in cases where computer equipments are searched and seized are the affected notified. However, the user is never informed that their private communications were intercepted if said communications are not used in a criminal proceeding.

# 7.

# Application of Surveillance Law

In the past few years, Argentina has gone through a series of situations related to the surveillance and interception of communications on public officials and journalists.

For instance, in 2006, a journalistic investigation publicly revealed that e-mails belonging to journalists and judges had been breached.[191] This impacted the subsequent enactment of Law № 26,388, which included several of the computer crimes mentioned above in the Criminal Code.

Even though there have been several similar attempts to modify the Code in order to include such crimes, it was these specific revelations that triggered the implementation of this law, since the e-mail breach was not part of the Code back then. This episode revealed loopholes in the Criminal Code for computer crimes, and soon after that the reform was passed.

## 7.1 Case on Illegal Wiretaps in Buenos Aires

This is an important case to highlight, since Buenos Aires' head of government, Mauricio Macri—who is now the president of Argentina—has been under investigation since 2010 for being a "necessary participant in an unlawful association."[192]

A Court decision holds Mr. Macri responsible for participating in the organization of a "structure of unofficial intelligence" in Buenos Aires. His former brother-in-law and leading members of the association "familiares de víctimas de la AMIA" [AMIA victims' relatives], who are opposed to the government of Buenos Aires,[193] accused him of illegally wiretapping telephones, among others things. The former chief of the Metropolitan Police of Buenos Aires has also been prosecuted and is awaiting trial in the same court case.

## 7.2 Proyecto X [Project X]

One of the biggest surveillance scandals that has occurred in the last few years is "Proyecto X." Implemented in 2005 and revealed in 2012, the National Police collected of intelligence information. This data collection violates the aforementioned legal framework and was not authorized by a judge. In addition, the activities were not reported to the Bicameral Commission, the agency in charge of monitoring intelligence activities.

Project X, which was approved by the then Minister of Security and the Chief of Gendarmerie, consisted of a database containing information about social, environmental, and human rights organizations, as well as associations related to social movements, unions, and victims of the dictatorship.[194]

The police officers worked undercover at demonstrations and protests attended by organizations opposed to the government.[195] As a result, demonstrators were prosecuted on the basis of information collected by the undercover agents.

Project X violated the above-mentioned Law on National Intelligence, which prevents security forces from producing intelligence or storing data about the political opinions of people, or their membership of social, union, political or community organizations.

Moreover, Project X was inconsistent with the legal framework established by the law on personal data protection, which prohibits data collection "through unfair or illegal means;"[196] and the storing of "sensitive data,"[197] such as "political opinions, religious, philosophic or moral beliefs and union membership."[198]

It is currently being investigated whether the activities conducted by National Police were illegal. This case is still in the preliminary investigation stage.

## 7.3 Purchase of Communications Surveillance Equipment

Thanks to a German parliamentarian's request to access information, it was revealed that Argentina bought electronic surveillance equipment from Germany. This illustrates the State's lack of transparency with regards to its surveillance activities, since, so far, the capabilities, purposes, and users of this equipment are still unknown.[199]

Furthermore, recent disclosures by WikiLeaks[200] revealed that Argentina communicated with Hacking Team, a Milan-based firm specializing in electronic intrusion and surveillance software and techniques, about possibly purchasing spy software. We can infer that the Italian company presented its products to the public agencies in charge of intelligence activities. So far there has been no concrete information or official statements regarding these interactions.

## 7.4 The Death of Alberto Nisman, Argentinian Prosecutor, and the Reform of the Intelligence System

The most recent case regarding surveillance involves the death of Alberto Nisman, which occurred in January 2015.[201] Mr. Nisman was the prosecutor in charge of the case of the bombings of the Asociación Mutual Israelita Argentina (AMIA) [Mutual Argentine-Israeli

Association] in 1994. The night before appearing before Congress to submit his charges against President Fernández de Kirchner, Nisman was found dead in his apartment.

An investigation conducted by security expert, Morgan Marquis-Boire of *The Intercept*, indicated that Nisman had downloaded spy software (malware) on his cellphone shortly before his death.[202] Marquis-Boire explains that the software was hidden in a PDF document marked "confidential," and was meant to infect his Windows computer. However, because Nisman opened the file from his Android phone, his computer was not infected.[203] According to *The Intercept*, we don't know if Nisman opened the file on his computer. Marquis-Boire adds that this attack was not an isolated event, and that the person or persons responsible for this surveillance attempt have also conducted operations in various locations in South America on other subjects, like journalist Jorge Lanata.

The aftermath of the prosecutor's death forced the Argentinian intelligence services into the spotlight and to engage in public debate.[204] Shortly after his death[205] President Cristina introduced a project to reform the intelligence system, since it had not served the "national interests."

The project paved the way for the aforementioned changes regarding surveillance: the dissolution of the Intelligence Secretariat, the creation of the Federal Intelligence Agency, the transfer of wiretaps to the Public Prosecutor's Office.

# 8.

# Does Argentina Comply with International Human Rights Standards Related to State Surveillance?

## Legality

> *This Principle establishes that any limitation to human rights must be prescribed by law and meet a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.*

Telecommunications surveillance in the criminal and intelligence fields must be conducted in accordance with the national constitution, the human rights treaties to which Argentina has subscribed, and with the provisions in the relevant laws and codes. Both normative bodies describe the procedures for conducting communications surveillance and identify the officials that may authorize them. In that sense, they comply with the requirement of legality.

Notwithstanding, the regulatory framework on intelligence includes some definitions that are vaguely defined, which can result in abuse by the State. For example, the law on national intelligence establishes that the "highest authorities" in each intelligence agency may order these activities. On the other hand, it stipulates that "in cases of emergency," such activities may be initiated, provided that they are immediately reported to the highest authorities.[206] The fact that "case of emergency" lacks an exhaustive definition in the regulatory framework could lead to actions that violate fundamental rights.

The same vagueness and lack of precise definitions can be found in the new doctrine on intelligence matters. This new doctrine was created from an Executive Branch decree and so it was not discussed in Congress or publicly debated. It elaborates on what constitutes an attacks against the constitutional order, which might be legally problematic since it is not clearly defined. The same lack of precision can be seen regarding intelligence activities in the investigation of fraudulent use or illegal disclosure of contents.

The current regulation on telecommunications also includes vague language that could unintentionally allow for communications surveillance.

The "Argentina Digital" Law, on one hand, establishes a general framework in matters related to Information and Communication Technology (ICT). On the other hand, it lays down the inviolability of communications held by telecommunications networks or services. And it indicates that communications interception, as well as its subsequent storage and analysis, may only be conducted with request of a competent judge.[207] So far, it complies with the Principle of Legality.

However, other articles establish obligations for ICT service users that might be at odds with this premise and the Principle of Legality. As seen, it stipulates that users must allow the staff of these companies and the ENACOM (formerly known as AFTIC) to access information for testing and verification purposes.[208]

Because this resolution is very broad, it may be problematic for the Principle of Legality. For example, telecommunications service providers must guarantee "full access to their networks and information" to the public agency in charge of enforcing the telecommunications framework and provide all the requested information that said agency deems "appropriate."[209]

The same applies to Law 25,891 on Mobile Communications Services. This law compels mobile service providers to collect, retain, and disclose personal data without clearly delineating the limits to or purposes of the collection, or the type of data being collected. It just imposes the obligation to share "all information about clients and users."

The fact that these regulations are not clear—that they are too broad and lack precision—leaves room for potential abuse by authorities which conflicts with the international standards on privacy.

### Legitimate Aim

> *Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.*

In principle, the Argentinian law that provides for the interception of communications complies with this requirement, since it establishes that interceptions must be conducted in exceptional circumstances, with an aim to prove the commission of a crime or to protect national defense and domestic security.

However, as we have analyzed, the new framework that regulates intelligence activities in Argentina extends the list of offenses that could be considered at odds with institutional order and democratic practices. As such, it could be subjected to intelligence activities. This could trigger new State practices that are dangerous to human rights and challenge the Principle of Legitimate Aim.

With regards to the telecommunications framework, the requirement that service providers must retain information is not duly justified.[210] Neither does the legislation adequately describe the aims.

Similarly, telecommunications legislation does not comply with this principle. This law compels users to allow authorities to access information so they can conduct "all kinds of tasks and necessary verifications" without specifying the kind of task, the type of verification or their purposes.[211] It also compels mobile service providers to report "all information" about users and clients, without specifying the purposes that justify such measures.[212]

The new systems for data collection analyzed in this report, like the SUBE, SIBIOS, and the DNI, which all originated from prior legislation and were not publicly discussed, do not abide by this principle, as their aims are not duly justified. With the broad idea of providing more security, preventing crime, and simplifying paperwork, [213] biometric and biographic data and information about the citizens' daily movements and routines are being collected with very little transparency.

This happens despite the fact that personal data and intelligence legislation do not allow agencies to obtain information, produce intelligence, or store people's data on the basis of race, religion, and political opinions or activities. However Project X included practices that were implemented by the Argentinian security forces and in conflict with this provision.

### Necessity

> *Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. This means that Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when it is the means least likely to infringe upon human rights.*

The criminal procedure for communications interception establishes the exceptional nature of communications interception, as well as the judge's duty in making sure that the interception request complies with the Principle of Legality and Reasonableness.

The legal framework for national intelligence stipulates that whenever intelligence activities are deemed "necessary" to intercept communications, judicial authorization must be

requested.[214] However, there are no further specifications as to when it is "necessary" to turn to this measure, or as to whether there are other, less intrusive methods to achieve the same aims when the request is submitted. In this regard, this does not comply with this principle.

Notwithstanding, the intelligence framework establishes provisions linked to this principle, since communications surveillance may only be carried out with a written judicial order describing in detail the phone numbers or e-mail addresses that are going to be intercepted or recorded.[215] The national intelligence law also stipulates that intelligence activities must be conducted in accordance with the policy framework for the protection of personal data in Argentina,[216] establishing a maximum time period for the communications surveillance to occur.[217]

The legal framework for telecommunications abides by the Principle of Necessity as it highlights the concept of the inviolability of communications and that surveillance may only be carried out with a judicial order.[218] However, some regulations that make up this legislative framework go against this principle, as they establish that service providers must deliver user data upon the request of law enforcement and for as long as the authority deems necessary.[219]

### Adequacy

> *Any instance of Communications Surveillance authorized by law must be appropriate to fulfill the specific Legitimate Aim identified.*

Communications surveillance conducted through the criminal process must demonstrate that the interception is useful in determining that a crime has been committed.

Moreover, intelligence regulations comply with the Principle of Adequacy by establishing that any data collected through intelligence activities that is unrelated to the aims set out in the regulatory framework must be destroyed. This law further establishes that information may not be stored on the basis of race, religion, private actions, political activities, and membership of social organizations, among others.[220]

Telecommunications legislation, as we have previously seen, does not completely comply with this principle, since it does not establish a maximum time period for personal data retention.[221] This is at odds with the personal data provisions in the law, which, in Article 4, stipulate that data must be stored in such a way that it allows for the data subject to access their own data. It also must be stored in a way that it can be destroyed when the data becomes unnecessary or irrelevant to the aims for which they were first collected.

## Proportionality

*In order for communications surveillance to be proportional, it is necessary for the State to establish certain requisites to a competent judicial authority, prior to conducting communications surveillance:*

1. *There is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out.*

This requisite is not met in the criminal legislation, as it solely requires that interception be useful to ascertain that a crime has been committed, without specifications regarding the severity of the crime.

For intelligence activities, national intelligence bodies must seek judicial authorization to intercept communications in order to investigate risks to domestic security and national defense, or complex federal crimes, like drug trafficking.

2. *There is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought.*

This requisite is neither met in the criminal process nor in the framework that regulates intelligence activities. The criminal process solely demands that information be useful; it does not require there be concrete proof leading to the necessary evidence. As mentioned, communications surveillance can be requested in the context of intelligence activities. It should be noted that there is a wide variety and of intelligence activities that may be problematic.

3. *Other less invasive techniques have been exhausted or would be futile, such that the technique used is the least invasive option.*

Even though the criminal legislation specifies that communications surveillance must only be carried out in certain, extenuating circumstances it does not explicitly state that other, less invasive techniques should first be exhausted in the investigation prior to turning to communications surveillance. Likewise, the legislation on intelligence doesn't specify that other, less invasive techniques should be used first.

4. *Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged.*

Criminal legislation with regards to communications surveillance establishes the obligation to limit the seizure exclusively to the elements that are related to the sought-after object. Regulations on intelligence activities comply with this principle.

5. *Any excess information collected will not be retained, but instead will be promptly destroyed or returned.*

The criminal system provides for confidentiality and secrecy when it comes to communications surveillance, and in the case of data seizures, it provides for the return of information or elements that have no relation to the process. Intelligence regulations establish a maximum time period that the interception of communications may be conducted as well as an obligation to destroy collected data that is not necessary for the purposes established in the framework that regulates these activities.[222]

6. *Information will be accessed only by the specified authority and used only for the purpose and duration for which authorization was given.*

Criminal legislation provides for these requisites, since it establishes that any data collected must be returned and surveillance must stop once the time period has elapsed or the aim has been achieved.

Intelligence legislation complies with this principle, as it establishes that the staff in charge of intelligence activities, documents and intelligence agencies' data banks "shall be assigned the appropriate security clearance in the interest of domestic security, national defense and the nation's foreign affairs. Access to such information shall be authorized in each case by the president of the country or the official appointed specially to conduct such activity, with the provisions established by this law."[223]

Moreover, it complies with this principle because it indicates that data cannot be collected on the basis of race, religion, private actions, political activities, and membership of social organizations, among others.[224]

7. *That the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.*

Criminal regulations provide for the protection of privacy by imposing a duty of confidentiality on the officials who conduct the surveillance.

The national intelligence law, as previously explained, establishes penalties for those who work for intelligence agencies and unduly intercept, record or divert communications that are not addressed to them.[225]

The regulations that do not have a maximum data retention period allow collected information to be used for purposes other than the ones for which it was collected.

### Competent Judicial Authority

> *This principle establishes that determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. This authority must be separate and independent from the authorities conducting Communications Surveillance, conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights, and have adequate resources in exercising the functions assigned to them.*

This requisite is met, both in criminal and intelligence legislation. Article 5 of the Argentina Digital law also complies with this principle by stating that communications surveillance may only take place with a judicial authorization.

However, some aspects of the laws that make up the telecommunications policy framework circumvent this principle, like the aforementioned rules for Quality of Telecommunications Services and the law on mobile communications services.

### Due Process

> *Due process requires that States respect and guarantee individuals' human rights. They must ensure that everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law. Only in cases of emergency when there is imminent risk of danger to human life will it be possible to do without the judicial order. In such instances, retroactive authorization must be sought.*

In general terms, the State of Argentina guarantees due process. However, in certain cases, the system allows for the possibility of searches without a judicial order. These are cases in which there is a threat to life or when "one or more individuals have been seen entering a house or shop, with concrete evidence of the commission of a crime." This exception is not completely clear and could result in a misinterpretation.

Communications surveillance in the context of intelligence activities provides for due process since it may only be carried out with a judicial authorization. However, it is necessary to remember that the policy framework enables these intelligence activities to be initiated in "cases of emergency"—which must be immediately reported. This could leave room for possible human rights violations.

The intelligence framework establishes a maximum time period for the authorization of communications interceptions. Such authorization may be extended for a maximum additional 60 days, as long it's required to complete the investigation.[226]

Data retention, pursuant to some laws and resolutions that make up the policy framework for telecommunications, does not completely comply with this principle. Even though the Argentina Digital law stipulates that all interceptions of communications must be conducted with a judicial order, other laws enable one part of the Executive Branch to access personal data, request information about users and, among other things, store it for as long as it deems necessary. All these issues violate this principle.

### User Notification

> *Those whose communications are being surveilled should be notified of a decision authorizing Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies. Delay in notification is only justified when it would seriously jeopardize the purpose for which the Communications Surveillance is authorized, or there is an imminent risk of danger to human life, the authorization to delay notification is granted by a Competent Judicial Authority, and the user affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.*

Argentina does not comply with this principle since it is not provided for in the criminal normative framework nor in the legislation on intelligence activities. There is no obligation to notify the individual, not even when the interception is over.

If elements relevant to the criminal or intelligence investigation emerge from said interception, the subject might eventually learn about it, provided that such elements are used as evidence in the criminal process. However, surveillance often produces elements that are irrelevant to an investigation. In these cases, an individual would never discover that their communications were surveilled.

### Transparency

> *In order to comply with the principle of transparency States should be transparent about the use and scope of Communications Surveillance. They should publish, at a minimum, aggregate information on the*

*specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each.*

Again, this principle is not met in Argentina. Although intelligence agencies are required to submit reports to the Bicameral Commission, such reports are not public. Thus, there is no official, publicly available data about communications interception activities.

### Public Oversight

*This principle lays down that States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.*

The existence of the Bicameral Commission on the Supervision of Intelligence Bodies and their Activities is a good thing since its supervisory powers ensure that the agencies that conduct intelligence activities abide by constitutional norms and respect human rights. However, civil society organizations have criticized the Commission for its secrecy and lack of transparency. They have yet to hear a response to their requests for information about the Commission's operations.

Nonetheless, the Court has not yet established regulations for this agency since the *acordada* that creates the DCCPJ fails to establish external oversight mechanisms—it only makes reference to the fact that there shall be an oversight body in charge of the Court, but fails to provide more details.

Aside from this, there is no provision about any additional independent mechanism to oversee intelligence activities.

### Integrity of Communications and Systems

*In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes.*

Service providers should never be compelled preserve or collect data. The aforementioned resolution establishing the Rules for the Quality of Telecommunications Services, drafted by the Communications Secretariat, might be at odds with this principle.

These rules outline that telecommunications service providers must preserve, in electronic form, for at least three years, all the data collected by their systems that may be used as a quality indicator according to the law. Authorities may later request such data. Even though the collected data shall only be used as a quality indicator, we think that this power might go against this principle.

Although the guide on best privacy practices for application developers is non-binding and only a guide for the National Department of Personal Data (DNDP), it is a positive step towards complying with this principle, since it encourages app developers to be clear about their use of data and to practice the principles of *privacy by design* and *privacy by default*.

### Safeguards for International Cooperation

> *This principle establishes that the agreements entered into by States should ensure that, where the laws of more than one state could apply to Communications Surveillance, the available standard with the higher level of protection for individuals is applied. The principle of dual criminality should also be included in such agreements.*

Even though all cases should be analyzed individually, due to the lack of a specific cooperation agreement, the international cooperation law in criminal matters lays down that the principle of dual criminality applies in order for an individual to be extradited.

### Safeguards against Illegitimate Access

> *States should enact legislation criminalising illegal Communications Surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected.*
>
> *States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.*

It is encouraging that both the criminal and intelligence legislation create penalties for illegal communications surveillance or intelligence activities—penalties that are aggravated in cases where they are committed by public officials.

In regards to the protection of whistleblowers, criminal legislation that criminalizes the disclosure of private communications provides an exception for those who disclose communications "with the clear purpose of protecting a public interest."[227]

This year, the National Intelligence Law (№ 25,520) incorporated criminal sanctions for those who, permanently or transitorily participating in the activities regulated in this law, "unduly intercept, record or divert telephone, postal, telegraphic or fax communications or any other system of delivery of objects or transmission of images, audios or data packets, as well as any other type of information, file, record, and/or private document or documents with classified access that are not addressed to them."[228]

This law also establishes it is a crime when a person, acting under a judicial order, "fails to destroy or eliminate the records of wiretaps, the copies of postal, cable and fax interceptions or of any other element that accounts for the interceptions, recordings or diversions."[229] According to this law, any public official that carries out activities that are prohibited by law is also subject to prosecution.[230]

On the other hand, the legislation on national intelligence does not include protections for intelligence agents that publicly disclose information about the practices that violate fundamental rights.[231]

# 9.

# Recommendations

### Legality

- The framework that regulates intelligence activities should specify certain definitions with respect to the attacks against the constitutional order in order to prevent surveillance practices that go against international standards.
- Regarding telecommunications, the regulations and articles in the Argentina Digital law that would allow for the unlawful use of users' personal data should be revised.

### Proportionality

- It is necessary for communications surveillance to be confined, as established by the Principle of Proportionality, to serious crimes and to explicitly establish that all other, less invasive investigation techniques must be exhausted first.

### Due Process

- It is necessary to narrow down the situations in which a search with no judicial authorization may be conducted. Vague exceptions distort due process.

### User Notification

- One of the most imperative reforms is implementing some sort of user notification process for those whose communications are intercepted.

### Transparency

- There is no official public data on communications interception activities. It is essential that States publish, at minimum, aggregate information on the specific number of approved or rejected requests, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each.
- To this end, it is necessary to implement the oversight and supervisory mechanisms provided for in the legislative framework for intelligence activities.
- Even though this goes beyond communications surveillance, it is important to make the data collection—such as SIBIOS, SUBE, and the DNI—more transparent. So far, we know little about how the State uses collected data, or who has access to it, or how data is cross-referenced and for how long it is preserved, etc.[232] These questions are related to the comments made in previous sections about the law on personal data in Argentina and its two drawbacks: that consent is not necessary when

personal data is collected in the exercise of the State's functions or a legal obligation and that it enables several public agencies to exchange personal data.[233]

### Public Oversight

- The Bicameral Commission on the Supervision of Intelligence Bodies and their Activities needs to be more transparent about non-confidential affairs. Other independent oversight mechanisms should be implemented.

### Safeguards against Illegitimate Access

- In light of situations like the Snowden revelations, it is essential for national intelligence legislation to include protections for intelligence agents who publicly disclose information about practices that violate fundamental rights.[234]

# 10.
# New Developments Adopted by President Macri

August 2016

The original Argentina report was completed in October 2015. Since then, a lot has changed. Towards the end of that month, the first round of the presidential elections took place. Two candidates came out as the front-runners—Daniel Scioli, governor of the Province of Buenos Aires and member of the ruling party, and Mauricio Macri, mayor of Buenos Aires and leader of an opposition coalition. On November 22, 2015, Mauricio Macri was elected president with 51 percent of the popular vote. An updated version of the Argentina report, as well as this addendum, was completed in August 2016.

He took office on December 10, 2015, while Congress was on its summer recess.[235] During the first few weeks of his term, President Macri made several executive decisions—mostly through presidential decrees—which altered the normative framework described in Argentina's report. This brief addendum presents and, when relevant, analyzes these changes vis-à-vis the International Principles on the Application of Human Rights to Communications Surveillance.[236]

## Suspension of the Code of Criminal Procedure

The new Code of Criminal Procedure was adopted by Congress on November 9, 2014. In June of 2015, Act No. 27.150 established a gradual process for its implementation, which was to be accomplished by March 1, 2016. President Macri suspended the Code arguing that the conditions for its full implementation had "not been met." Instead of setting a new date, President Macri decided—through a decree of *necessity and urgency*—that a Bicameral Commission in Congress, with the agreement of the Ministry of Justice, would decide when the new Code would go into effect.[237]

Therefore, the analysis conducted in section 3.6 of the report loses its relevance. The section covers the ways searches are to be conducted (3.6.1 and 3.6.2) and the cases in which a judicial warrant is not required (3.6.3). It also covers the formalities judicial warrants must follow (3.6.4) and the formalities that must guide their execution (3.6.5 and 3.6.6). Because the new Code of Criminal Procedure has not gone into effect, today's regulations are to be found in the previous Code of Criminal Procedure of 1991. The way both codes deal with searches and seizures do not vary significantly.

In the Code of Criminal Procedure of 1991, judges are in charge of conducting criminal investigations. They can, however, delegate searches and seizures to public prosecutors if they so choose.[238] Both the order for the search and the procedure need to be outlined in an official document, which must follow certain formal requirements.[239]

Even though a judicial warrant is required, the Code establishes that it is not necessary in cases of fire, explosion or flood in which the life of the inhabitants of a given property might be at risk (Article 227.1). A warrant would also not be required if "strange persons" were seen going into a property when there is suspicion that a crime might be occurring (227.2). Similarly, one would not be required if a suspect who is being pursued enters a building (227.3) or when someone is asking for help (227.4). Finally, a warrant is not required when there is suspicion that a victim of human trafficking is inside a building to be searched (227.5). The inhabitants of the property shall be notified immediately at the moment the search warrant and the procedure are registered. If the inhabitants are not present at the time of the search, such fact must be noted in the official document.

Section 5.2 should also be revised; it currently describes the process through which communications are intercepted. In that sense, the Code of 1991 currently in force limits interceptions to "postal mail and telegraphic communications."[240] A more precise regulation can be found in the old Telecommunications Act of 1972 (No. 19.798) which was repealed by the Argentina Digital Act only with regard to those articles that conflicted with the new regulation.[241] Therefore, Act No. 19.798 still controls the process through which telecommunications are to be intercepted. Articles 18-21 establish the need for a judicial warrant (Article 18) and state that those who work in telecommunication services must keep the confidentiality of communications (Article 20), an obligation which is extended to "any person" who learns about their content (Article 21).

The New Code of Criminal Procedure, now suspended, included an article (144) that allowed for the search of computers in order to seize data. The rules for proceeding with the search are the same that apply to personal domiciles. However, the regulation also included a provision which guaranteed that any data that is not relevant to the investigation shall be returned to its owner and any copies that State has of it shall be destroyed.

From the standpoint of the International Principles on the Application of Human Rights to Communications Surveillance, the regulation currently in place also presents problems in terms of the precision of the language used.[242] In that sense, the current legal regime also allows for searches without judicial warrants under exceptional circumstances, including some—such as when persons were seen entering someone's domicile—which are excessively vague and prone to misuse.

## Transfer of the Authority to Intercept Communications

The National Intelligence Act of 2001 (No. 25.520) is the main legal framework for the surveillance activities of the State. On March 5, 2015 the Act was reformed by Act No. 27.126. Besides changing the name of the main intelligence agency (from Secretariat of Intelligence to the Federal Agency of Investigations, AFI in Spanish) the law introduced one major reform: it moved the body in charge of intercepting communications (DICOM) from the Executive Branch to the Public Ministry, a body which, since 1994, has been independent.[243] The DICOM is the office in charge of intercepting communications at the request or with the authorization of a judge.[244] Moving this body to the Public Ministry was arguably a decision that increased transparency and independence: the DICOM was traditionally perceived as being responsible for an entrenched practice of political espionage at the behest of the President.[245]

On December 24, 2015 by decree 256/2015, President Macri decided to move the DICOM from the Public Ministry to the Supreme Court.[246] The decree through which this was accomplished argued that the Public Ministry was not the right institutional body for the DICOM to function within, as it is the prosecuting party in criminal procedures where interceptions are used as evidence. Therefore, the power to intercept communications should lie—according to the decree—in an authority "that is not part of the criminal investigation."

It should be noted that both Act No. 27.126 and decree 256/2015 are rather imprecise regarding the authority of the DICOM. According to the National Intelligence Act, all communications interceptions fall within the scope of the DICOM and require judicial authorization, that is, those that are conducted for purposes of criminal investigations and those that are conducted for intelligence purposes, including foreign intelligence. However, both Act 27.126 and decree 256/2015 use language which suggests that the DICOM is only involved in criminal investigations. That is not the case, for it is also in charge of interceptions related to general intelligence gathering, including foreign intelligence.

Decree 256/2015 states that the Supreme Court will establish an internal regulation for running the DICOM, which will be in charge of a judge of a Criminal Court of Appeals who would be selected by lot and would last in his or her position for one year. However, the Supreme Court refused to take up the new responsibility immediately. In a decision made on December 29, 2015, the Court unanimously decided that in order to receive the DICOM, a bureaucratic structure to deal with it must be created.[247] Therefore, the Supreme Court decided to postpone the reception of the DICOM until February 15, 2016. On that date, the Court issued *Acordada* No. 2/2016 through which it created the Department of Capturing of Communications of the Judiciary (DCCPJ, in Spanish).[248] The regulation clarified the regulatory framework controlling the interception of communications: it mentions the Telecommunications Act of 1972 (No. 19.798), the National Intelligence Act

of 2001 and the Argentina Digital Act of 2015.

The new Department will have managerial autonomy from the Supreme Court, and will be in charge of a federal judge. The Supreme Court, however, retains the authority to change the regulation of the DCCPJ at any time. The *Acordada* sets forth a few principles, which should guide communications interception:

- Transparency and confidentiality: It states that an efficient oversight mechanism "is to be established" and mandates a duty of confidentiality for the employees working at the DCCPJ. It also orders the development of a document meant to guarantee the "chain of custody" which would protect the confidentiality of the information gathered through the interceptions.
- Training: The Court ordered that those in charge of intercepting communications must be trained so that they may make informed decisions regarding the most efficient mechanisms and technologies to be used for interception and evaluate the "opportunity" and duration of interceptions. Relevantly, the regulation establishes that the members of the DCCPJ might assist judges and prosecutors directly on their offices or "remotely."
- Data mining: The regulation mandates that an *update* to data mining practices is needed. In particular, it states that attempts to discover information in "great volumes of data" are to be pursued as a way of helping judges and public prosecutors.
- New technologies: The regulation establishes that new technologies are to be pursued and that the best practices of other judicial offices around the world are to be studied and copied.
- Relationships with telecommunications companies: The *Acordada* establishes that confidentiality agreements will be signed with telecommunications companies as well as with others who provide "usable services."

The DCCPJ will be formed by a general director, who will be a criminal judge and in office for one year only. Furthermore, the DCCPJ will have a board of five directors, but the *Acordada* does not clarify how the members of the board are to be elected.

Civil society organizations that have been working on the issue of intelligence reform for the last few years expressed concern with the new regulation. The Association for Civil Rights (ADC, in Spanish) reminded the public that many doubt the constitutionality of moving the DICOM to the Judiciary.[249] Furthermore, ADC warned about the use of vague language that does not clarify, with sufficient precision, when and how interceptions will be conducted and by the request of whom. Regarding the *data mining* section of the *Acordada*, ADC questioned the very existence of a database to be mined.

> *"If the body in charge of intercepting communications has created a data base that can be mined, citizens should know about the details of said database. What kind of information does it hold? How is the information collected? Are there any procedures for checking the accuracy of the data and which weighs in on the legality of its retention? Do the guarantees established in the Data Protection Act apply? The introduction of the concept of data mining is thus very revealing: it highlights practices we suspected exists but which are not adequately regulated by any norm, of any level, which curbs a state power which by definition violates the rights of citizens."*[250]

From the standpoint of International Principles on the Application of Human Rights to Communications Surveillance, placing the DICOM under the authority of the Supreme Court creates a lack of additional oversight and accountability measures.[251] Indeed, while the DICOM under the Public Ministry lacked an independent oversight mechanism, the same can be said for the DICOM under the authority of the Supreme Court, even though internal rules are yet to be established.

## Changes in Telecommunications Authority

The report mentions Argentina Digital Act of 2014, which was partially changed by decree 267/2015 of December 29, 2015. This decree does not fundamentally alter the law, but it does fuse its administrative authority (AFTIC) with the broadcasting authority (AFSCA) established by Act 26.522 of 2013. The changes introduced by the decree do not touch on the regulations that were considered in Argentina's report. It does, however, fundamentally change the rules against media cross-ownership, it authorizes telecommunication companies to access and provide broadcasting services and it eliminates both the broadcasting and the telecommunications authorities in order to create a new, encompassing agency called the ENACOM.

## Conclusion

The suspension of the New Code of Criminal Procedure was done mainly because it proposed a controversial change: it was going to transfer the authority of conducting criminal investigations from judges to public prosecutors. This is the main reform, which is now in standby. Regarding the actual rules which control the investigation of crimes, changes between the New Code and the Code of 1991 were not as radical, as we saw in the overview—and can be seen in the comparative table. The law remained more or less the same, even though certain updates that the New Code proposed—such as including explicitly electronic communications and the seizure of electronic data—are not in the law books yet.

On the other hand, moving of the department in charge of intercepting communications from the Public Ministry to the Supreme Court should be read as being motivated by the same reasons that were behind the suspension of the New Code of Criminal Procedure. The head of the Public Ministry is a controversial figure who was perceived by the ruling party to be too close to the previous administration. Hence, transferring the DICOM to the Supreme Court can be seen as an effort of keeping the DICOM independent but, at the same time, curtailing the powers of the Public Ministry. In any event, the regulation proposed by the Supreme Court seems indeed problematic. As ADC pointed out, several of its details are troublesome, such as the directive to increase data mining capabilities. At the same time, the DICOM—both under the Public Ministry and the Supreme Court—still lacks an independent oversight mechanism. It remains to be seen if, under the new political landscape, the legislative oversight mechanism established in the National Intelligence Act of 2001 works as it is supposed to or, as it has been the case for the last decade, remains incapable of effectively controlling intelligence activities (ADC, 2015).

| Previous framework: New Code, now suspended | Current rules (Code of 1991) |
|---|---|
| In the New Code (now suspended), public prosecutors were in charge of conducting searches and seizures, and—generally—of directing criminal investigations (Article 132 of the New Code). | The Old Code (currently in place) states that judges are to conduct searches, even though they can—if they choose so—let a public prosecutor conduct a search (Article 224 of the Code of 1991). |
| The New Code (now suspended) outlines that the name of the public prosecutor in charge of a search must be stated in the official document of the proceedings (Article 132 of the New Code). | The Old Code does not include that requirement (article 224). |
| The New Code (now suspended) allows for the interception of postal mail, telegraphic or electronic communications or any other forms of communications (Article 143). | The Old Code (now in place) only mentions postal mail and telegraphic communications (Article 234). |
| The New Code (now suspended) has some regulations in terms of how data gathered during a search is to be seizure. In that sense, a judge could issue a warrant to search a computer, with the goal of keeping the data. The same rules for the search and seizures of documents apply. Those elements which are not related to the criminal investigation will be returned to the owners, who can demand the destruction of the data which is not related to the investigation (Article 144). | No similar rule exists in the Old Code (now in place). However, it should be noted that the Supreme Court considered that metadata is in itself a "document" for constitutional purposes, and the State can only gather it under the same conditions which apply for the search and seizure of a document. Hence, the gathering of metadata in Argentina does require a judicial warrant. |
| The DICOM, the body in charge of intercepting communications, was under the Public Ministry. | President Macri transferred the DICOM to the Supreme Court, which renamed it DCCPJ. |
| AFSCA was the broadcasting authority and AFTIC was the telecommunications authority under the previous regime. | President Macri fused both authorities, which were eliminated in order to create one encompassing agency called ENACOM. |

1 Supreme Court of Justice, "Ekmekdjian, Miguel Ángel v. Sofovich, Gerardo et al.," July 7, 1992.

2 Article 75 subsection 22 includes the following treaties on human rights, ratified before 1994: American Declaration of the Rights and Duties of Man; the Universal Declaration of Human Rights; the American Convention on Human Rights; the International Covenant on Economic, Social and Cultural Rights; the International Covenant on Civil and Political Rights and its Optional Protocol; the Convention on the Prevention and Punishment of the Crime of Genocide; the International Convention on the Elimination of all forms of Racial Discrimination; the Convention on the Elimination of all forms of Discrimination against Women; the Convention against Torture and Other Cruel, Inhuman or Dreading Treatment or Punishment; the Convention on Child Rights. This article provides for a proceeding in Congress in order to incorporate the treaties subsequently signed.

3 Law Nº 24,767 on International Cooperation in Criminal Matters, Official Journal of January 16, 1997, article 6.

4 Law Nº 25,304, Official Journal of September 7, 2000.

5 *Ibid.*, article 2.1.

6 Law Nº 25,911, Official Journal of September 13, 1996.

7 In accordance with the International Principles on the Application of Human Rights to Communications Surveillance, the term "Communications" includes activities, interactions, and transactions transmitted through electronic mediums, such as content of communications, the identity of the parties to the communications, location-tracking, information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications; and "Communications surveillance" in the modern environment encompasses the monitoring, intercepting, collecting, obtaining, analyzing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future.

8 National Constitution, article 19.

9 *Ibid.*, article 18.

10 CSJN, "Halabi, Ernesto c/ PEN law 25,873 and decree 1563/04 on an amparo complaint," sentence of February 24, 2009. Available at: http://www.cij.gov.ar/nota-615-La-Corte-reconoce-accion-colectiva-y-da-alcance-general-a-un-fallo.html

11 National Constitution, article 43.

12 Ibid.

13 Law Nº 27,063 of December 9, 2014 passed it. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239340/norma.htm

14 Law No. 27,150, passed on June 17, 2015, establishes a gradual process for its implementation. As of March 2016, the Code was meant to enter into force in the sphere of national justice. Regarding federal justice, this Code was supposed to enter into force in accordance with a schedule for its gradual implementation established by a Bicameral Commission for Monitoring and Implementing the New National Code of Criminal Procedure. Visit the Bicameral Commission's webpage, available at: http://www.senado.gov.ar/parlamentario/comisiones/info/379

15 Decree No. 257/2015. Available at: http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=257347

16 Since the new Code of Criminal Procedure has not been repealed, we will refer to it throughout this report. In Annex I, you will find a table comparing the old Code of Criminal Procedure (in force at the moment of writing this report) and the new policy framework, currently suspended, in relation to communications interception.

17 Article 13. Emphasis added.

18 Criminal Code, article 153.

19 *Ibid.*, article 153 bis.

20 *Ibid.*, article 155.

21 *Ibid.*, article 157 bis.

22 Law Nº 25,520 on National Intelligence, Official Journal of December 6, 2001, article 42. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm

23 *Ibid.*, article 43.

24 *Ibid.*, article 43 b.

25 Law Nº 25,520 on National Intelligence, supra note 19.

26 Law Nº 27,126 on the creation of the Federal Intelligence Agency, Official Journal of March 05, 2015. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm

27 Decree Nº 337/2015 enacting Law Nº 27,126, Official Journal of March 3, 2015. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243822/norma.htm

28 Decree Nº 950/2002, Official Journal of June 06, 2002. Available at: http://www.infoleg.gov.ar/infolegInternet/anexos/70000-74999/74896/norma.htm

29 Decree Nº 1311/15, Official Journal of July 6, 2015. Available at: http://www.infoleg.ov.ar/infolegInternet/verNorma.do?id=248914

30 Law Nº 25,520 on National Intelligence, *supra* note 19, article 1.

31 *Ibid.*, article 2.

32 Law Nº 23,554 on National Defense, Official Journal of April 13, 1988. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm

33 Law Nº 24,059 on Internal Security, Official Journal of January 17, 1992. Available at: http://www.infoleg.gov.ar/infolegInternet/anexos/0-4999/458/texact.htm

34 Asociación por los Derechos Civiles [Association for Civil Rights], "Quién vigila a quienes vigilan. Estudio comparativo sobre sistemas de control de los organismos de inteligencia" [Who Surveils those who Surveil? Comparative Study on the Oversight Mechanisms for Intelligence Organisms], 2014, pp. 5 and 6.

35 Law Nº 23,554 on National Defense, article 15.

36 Law Nº 24,059 on Internal Security, article 8, section 2.

37 Law Nº 25,520 on National Intelligence, *supra* note 19, article 3.

38 This aspect has been criticized by human rights organizations. For instance, the Center of Legal and Social Studies (CELS, in Spanish) has stated that "this article has enabled the Intelligence Secretariat to penetrate in any legal case to assist the judiciary, which fostered promiscuous relationships with important areas of the federal justice. If this possibility is constant, the objectives of the reform will not be met." See more on the Center of Legal and Social Studies, "Ley de Inteligencia: las reformas al proyecto no solucionan problemas de fondo" [Law on Intelligence: Bill Reforms do not Solve Core Problems], February 7, 2015. Available at: http://cels.org.ar/comunicacion/?info=detalleDoc&ids=4&lang=es&ss=46&idc=1896

39 Law Nº 25,520 on National Intelligence, *supra* note 19, article 4.

40 *Ibid.*, article 5 bis.

41 *Ibid.*, article 18.

42 *Ibid.*

43 *Ibid.*, article 41.

44 Decree 256/2015. available at: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257346/norma.htm

45 Law Nº 25,326 on Personal Data Protection. Official Journal of April 13, 1988. Available at: http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

46 Law Nº 25,520, *supra* note 19, article 16 c., incorporated by article 13 of Law Nº 27,126.

47 *Ibid.*, article 16 d., incorporated by article 14 of Law Nº 27,126.

48 Law Nº 25,520, *supra* note 19, article 16 e., incorporated by article 15 of Law Nº 27,126.

49 *Ibid.*, article 42.

50 Decree Nº 1311/15, Official Journal of July 6, 2015. Available at: http://www.infojus.gob.ar/descarga-archivo?guid=noprstuv-wnov-edad-esde-ci31120l5pdf&name=dec13112015.pdf

51 *Ibid.*

52 Under the new doctrine of national intelligence, "intelligence information" covers "a series of observations and readings obtained or collected by public or reserved sources, referred to a specific relevant event or issue regarding national defense or internal security, or that have an impact on these areas."

53 *Ibid.*

54 Decree Nº 15, supra note 46, Annex I. Available at: http://www.boletinoficial.gov.ar/Displaypdf.aspx?s=A&tid=49218l1&i=1

55 *Ibid.*

56 *Ibid.*

57 Asociación por los Derechos Civiles [Association for Civil Rights], "Observaciones al decreto 1311/15" [Comments on Decree 1311/15], July 9, 2015, p. 2. Available at: http://www.adc.org.ar/wp-content/uploads/2015/07/Apuntes-sobre-el-decreto-1311-15.pdf

58 Decree Nº 1311/15, *supra* note 46, Annex I.

59 It is necessary to note the Argentina has a very restrictive regulatory framework in relation to copyright provided by the Law on Intellectual Property Nº 11,723 of 1933, to which more restrictive amendments were introduced.

60 Law Nº 27,078, Argentina Digital, Official Journal of December 19, 2014. Available at: http://www.infoleg.gov.ar/infolegInternet/anexos/235000-239999/239771/norma.htm

61 See more at Fontanals, Gustavo, "La política detrás de AFTIC" [Politics behind AFTIC], *Bastión Digital*, July 13, 2015. Available at: http://ar.bastiondigital.com/notas/la-politica-detras-de-aftic and Massare, Bruno and Pautasio, Leticia, "Argentina Digital en detalle: qué cambios plantea la nueva ley de telecomunicaciones" [Argentina Digital in Detail: Changes in the New Telecommunications Law], *Info-technology*, May 8, 2015. Available at: http://www.infotechnology.com/internet/Argentina-Digital-en-detalle-que-cambios-plantea-la-nueva-ley-de-telecomunicaciones-20150508-0008.html#sthash.UuPMbB3U.dpuf

62 Article 89 of Argentina Digital Law indicates that Law Nº 19,798 and its modifications will only persist "with respect to those provisions that are not opposed to the provisions of this Law."

63 Law Nº 27,078 Argentina Digital, *supra* note 56, article 5.

64 Through another presidential decree (267/2015) two public bodies, one in charge of broadcasting—the Federal Authority for Audiovisual Communication Services (AFSCA, in Spanish)—and the other in charge of telecommunications—the Federal Authority for Information Technology and Communication (AFTIC, in Spanish)—were fused into a new agency called National Communications Body (ENACOM, in Spanish). Apart from this, this decree does not alter the telecommunications framework in relation to the aspects analyzed in this report.

65 *Ibid.*, article 60, section d.

66 Asociación por los Derechos Civiles [Association for Civil Rights], "Alerta de la ADC sobre el proyecto de ley Argentina Digital" [ADC Warns about the Argentina Digital Law], November 16, 2014. Available at: http://www.adc.org.ar/alerta-de-la-adc-sobre-el-proyecto-de-ley-argentina-digital/

67 Department of Communications, Resolution Nº 5/2013, July 1, 2013. Available at: http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm

68 Law Nº 27,078 Argentina Digital, supra note 56, article 87.

69 Law Nº 25,891 on Mobile Communications Services, Official Journal of April 28, 2004. Available at: http://infoleg.mecon.gov.ar/infolegInternet/anexos/95000-99999/95221/norma.htm

70 Portal Nacional de Usuarios de Telecomunicaciones [Website for Telecommunications Users]. Autoridad Federal de Tecnologías de la Información y las Comunicaciones (AFTIC) [Federal Authority on Information and Communication Technologies]. Available at: http://www.quenosecorte.gob.ar/

71 Law Nº 25,891 on Mobile Communications Services, article 3.

72 Vargas, Paula, "Vigilancia masiva de las comunicaciones: inconstitucionalidad de la Ley 25.891" [Massive Communications Surveillance: Unconstitutionality of Law 25,891], *Internet Right and Communication Technology Blog*, August 12, 2015. Available at: http://www.ditc.com.ar/2015/08/12/397/

73 Ministry of Federal Planning, Public Investment and Services, Department of Communication, Resolution Nº 5/2013, July 1, 2013. Available at: http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm

74 *Ibid.*, article 2.

75 *Ibid.*, article 3.

76 *Ibid.*, article 5, section 2.

77 *Ibid.*

78 Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) [Center of Studies in Freedom of Expression and Access to Information, "Internet en Argentina: ¿cómo estamos hoy?" [The Situation of the Internet in Argentina Today], p. 18. Available at: http://www.palermo.edu/cele/pdf/investigaciones/Mapping-ARG-CELE.pdf

79 Ministry of Federal Planning, Public Investment and Services, Department of Communication, Resolution Nº 5/2013, July 1, 2013, article 8.

80 National Criminal Procedure Code. Article 132.

81 *Ibid.*

82 National Criminal Procedure Code, article 133.

83 *Ibid.*

84 *Ibid.*, article 135.

85 *Ibid.*, article 137.

86 Requisites established in article 136: a) The concrete identification of the place(s) to be searched; b) The purpose of the search, specifying the objects to be seized and the people to be arrested; c) The name of the representative of the Public Prosecutor's Office in charge of overseeing and conducting the measures, the motives that justify the necessity of the measure and the prima facie evidence that supports it; d) When necessary, the motives that justify the need to conduct the measure after daytime hours; e) The signature of the representative of the Public Prosecutor's Office who requests the authorization.

87 National Criminal Procedure Code, article 139.

88 Law Nº 25,326 on Personal Data Protection, *supra* note 41, article 1.

89 Decree Nº 1558/2001, Official Journal of November 29, 2001. Available at: http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70368/texact.htm

90 Decree Nº 1160/10, Official Journal of August 11, 2010. Available at: http://www.infoleg.gov.ar/infolegInternet/anexos/170000-174999/170508/norma.htm

91 Law Nº 26,343, Official Journal of January 9, 2008. Available at: http://infoleg.mecon.gov.ar/infolegInternet/anexos/135000-139999/136483/norma.htm

92 Asociación por los Derechos Civiles [Association for Civil Rights], "El Estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos" ["Collection by the State. A Study of Argentina and the Personal Data of its People"], 2014, p. 3.

93 *Ibid.*, pp. 3 and 4.

94 *Ibid.*, p. 3 and Torres, Natalia, *Acceso a la información y datos personales: una vieja tensión, nuevos desafíos [Access to Information and Personal Data: Old issue, New Challenges]*, CELE, Universidad de Palermo [Palermo University]. Available at: http://www.palermo.edu/cele/pdf/DatosPersonales_Final.pdf

95 *See* Asociación por los Derechos Civiles [Association for Human Rights], "Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina" [If we get to know one another, we can take better care of one another. Report on Argentinian Biometrics Policies], May, 2015, p. 5. Available at: http://www.adc.org.ar/wp-content/uploads/2015/05/InformeBiometriaADC2015.pdf and Fascendini, Flavia and Roveri, Florencia, "Tu software, mi biología. Sistemas de vigilancia masiva en Argentina" [Your software, my biology. Massive Surveillance Systems in Argentina], *GISWatch Report*, 2014. Available at: http://www.giswatch.org/node/4951

96 Savoia, Claudio, *Espiados [Spied on]*, Buenos Aires, Publishing House: Planeta, 2015, p. 333.

97 Madres de Plaza de Mayo Línea Fundadora, Fundación Vía Libre, Liga por los Derechos del Hombre y otros [Mothers of the Plaza de Mayo Founding Line, Free Pass Foundation, League for Man's Rights, among others] "Los DNI electrónicos violan nuestros derechos" [Electronic IDs Violate our Rights], October 6, 2014. Available at: http://www.pensamientopenal.org.ar/dni/

98 Siri, Laura, "El Documento Nacional de Identidad Argentino: una "caja negra" y una política de veridicción" [The Argentinian ID: a "Black Box" and a Veridiction Policy], 3rd International LAVITS Symposium: Surveillance, Tecnopolitics and Territories. May 13-15, 2015. Rio de Janeiro, Brazil. Latin American Network of Surveillance, Technology and Society Studies (LAVITS), p. 3.

99 *Ibid.*

100 *See also* Villa, Emiliano and Álvarez Ugarte, Ramiro, "Las fotos de los argentinos, al mejor postor" [Pictures of Argentinians to the Highest Bidder], Bulletin of *Digital Rights*, November 22, 2013. Available at: http://www.digitalrightslac.net/es/las-fotos-de-los-argentinos-al-mejor-postor/

101 Law Nº 17,671 on Identification, registry and classification of the national human potential, Official Journal February 29, 1968. Available at: http://www.infoleg.gov.ar/infolegInternet/anexos/25000-29999/28130/texact.htm

102 Siri, Laura, *supra* note 94, p. 2.

103 ADC, *supra* note 91, p. 8.

104 Decree Nº 1501/2009, Official Journal of October 20, 2009. Available at: http://infoleg.mecon.gov.ar/infolegInternet/anexos/155000-159999/159070/norma.htm

105 RENAPER, Resolutions Nº 585/2012 and 797/2012.

106 ADC, *supra* note 74, p. 9.

107 "Randazzo anunció nuevo DNI inteligente que incorpora un chip" [Randazzo Announced the Launching of a New Smart DNI with a Built-in Computer Chip], Audiovisual Télam, June 27, 2014. Available at: http://www.telam.com.ar/multimedia/video/5091-randazzo-anuncio-nuevo-dni-inteligente-que-incorpora-un-chip/

108 Siri, Laura, *supra* note 77, p. 5.

109 Mothers of the Plaza Mayo Founding Line et al., *supra* note 76.

110 Department of Transport, Resolution 162/2010 of October 27, 2010. Available at: http://infoleg.mecon.gov.ar/infolegInternet/anexos/170000-174999/170118/norma.htm

111 It is possible to use the card without being registered but there is no way to claim back the credit left in it, for example, if it gets lost. Moreover, its use is not mandatory but, the price of the fare is higher if it is not used.

112 Fundación Vía Libre [Free Pass Foundation], "Con SUBE sí vas a pagar más caro: el fin de la privacidad" [You *are* Going to Pay more Using SUBE: The End of Privacy]. Available at: http://www.vialibre.org.ar/2012/01/27/con-sube-si-vas-a-pagar-mas-caro-el-fin-de-la-privacidad/

113 Law Nº 25,326 on Personal Data Protection, *supra* note 41, article 9.

114 "Exponen en la Red los registros de viajes de la tarjeta SUBE" [Records of Trips made with the SUBE Card Revealed], *La Nación*, January 30, 2012. Available at: http://www.lanacion.com.ar/1444623-exponen-en-la-red-los-registros-de-viajes-de-la-tarjeta-sube and "Anonymous SUBE viajes" ["Anonymous" Reveals SUBE Trips], *Página 12*, January 31, 2012. Available at: http://www.pagina12.com.ar/diario/cdigital/31-186566-2012-01-31.html

115 Decree Nº 1766/2011.

116 ADC, "Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina" [If we get to know one another, we can take better care of one another. Report on Argentinian Biometrics Policies], 2015, p. 18.

117 Decree Nº 1176/2011, article 4.

118 Savoia, Claudio, *supra* note 92, p. 335 and 336.

119 ADC, 2015, "Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina" [If we get to know one another, we can take better care of one another. Report on Argentinian Biometrics Policies], p. 17 and 18.

120 Tordini, Ximena, "El triunfo final sobre el anonimato" [The Final Triumph over Anonymity], Magazine Crisis, Number 8, February-March, 2012. Available at: http://www.revistacrisis.com.ar/el-triunfo-final-sobre-el.html

121 National Department of Personal Data Protection, Provision Nº 20/2015, Official Journal of May 27, 2015.

122 The National Civil Aviation Administration has issued a general regulation on unmanned aerial vehicles. *See* ANAC, Resolution N° 527/2015, Provisional Regulation on Unmanned Aerial Vehicles. Available at: http://www.anac.gov.ar/anac/web/index.php/1/1196/noticias-y-novedades/reglamento-provisional-de-los-vehiculos-aereos-no-tripulados-vant

123 For instance, organizations of the region made presentations on the use of drones and the impact on human rights in the Americas in a hearing before the Inter-American Commission on Human Rights in 2013.

124 Annex 2 of this provision defines UAVs or drones as artifacts "equipped with cameras, microphones, gps or any other kind of sensor, which has the ability to collect data from people, such as images, videos, conversations, geolocation, and so on. It

can also fly, allowing it to access places that the human eye cannot reach; and the possibility to operate without being detected."

125 National Department of Personal Data Protection, Provision Nº 20/2015, Official Journal of May 27, 2015. Available at: http://www.jus.gob.ar/media/2898655/disp_2015_20.pdf

126 Ministry of Justice and Human Rights, National Department of Personal Data Protection, Provision 10/2015, Buenos Aires, February 24, 2015. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243335/norma.htm

127 Savoia, Claudio, *supra* note 92, p. 318.

128 Law Nº 2,602, December 6, 2007.

129 Law Nº 13,164.

130 *Ibid.*, article 3.

131 *Ibid.*, article 7.

132 *Ibid.*, article 6.

133 Ministry of Justice and Human Rights, National Department of Personal Data Protection, Provision 18/2015, Buenos Aires, April 10, 2015. Available at: http://infoleg.mecon.gov.ar/infolegInternet/anexos/245000-249999/245973/norma.htm

134 *Ibid.*, Introduction

135 *Ibid.*, Annex 1, Section 3.

136 Decree Nº 357/2005 suspended the application of Decree Nº 1563.

137 Halabi, recital 23.

138 *Ibid.*, recital 24.

139 Halabi, recital 24.

140 *Ibid.*, recital 25.

141 *Ibid.*, recital 26.

142 National Constitution, article 1.

143 Gelli.

144 National Constitution, article 75, subsection 12.

145 National Criminal Procedure Code, article 52.

146 National Criminal Procedure Code, article 88.

147 National Criminal Procedure Code, article 90.

148 National Criminal Procedure Code, article 143.

149 *Ibid.*

150 *Ibid.*

151 *Ibid.*

152 *Ibid.*

153 National Criminal Procedure Code, article 144.

154 *Ibid.*

155 *Ibid.*

156 *Ibid.*

157 National Criminal Procedure Code, article 145.

158 *Ibid.*, article 145.

159 *Ibid.*

160 Law Nº 27,126 creating the Federal Intelligence Agency, *supra* note 23, article 7.

161 Decree Nº 1311/15, *supra* note 46, Annex I, Chapter III.

162 Law Nº 27,126 creating the Federal Intelligence Agency, *supra* note 23, article 8.

163 *Ibid.*

164 Presidency of the Argentine Republic. Ministry of Security. Available at: http://www.minseg.gob.ar/

165 Decree Nº 1311/15, *supra* note 46, Annex I, Chapter III, page 27.

166 Law Nº 27,126 creating the Federal Intelligence Agency, *supra* note 23, article 7.

167 *Ibid.*

168 Decree Nº 1311/15, *supra* note 46, Annex I, Chapter III, page 28.

169 Law Nº 25,520 on National Intelligence, *supra* note 19, article 18.

170 *Ibid.*

171 *Ibid.*, article 19.

172 *Ibid.*, article 20.

173 Public Prosecutor's Office, Nº 2067/15, July 7, 2015.

174 The Public Ministry is a fundamental part in the administration of justice and is made up of the Judiciary, the Public Prosecutor's Office and the Public Defender's Office. Together, they represent the three fundamental parts of the legal process. Moreover, the Public Ministry is an independent body in the system of the administration of justice. It is in charge of the Prosecutor General, who is suggested by the Executive Branch and appointed by the National Congress. The Public Ministry is even independent from the Judiciary (led by the Supreme Court of Justice). Such independence springs from the Constitutional Reform of 1994, which established the autonomy of the Public Ministry. In regards to criminal matters, the Prosecutor General in charge of the Ministry has the power to decide how to deal with certain crimes that may have a greater relevance in relation to the defense of the general interests of society. For instance, crimes against life, humanity, drug-related crimes, institutional violence, and money laundering, to name a few. Hence, the Public Ministry is made up of special units whose aim is to improve the the accomplishment of such job. The Public Ministry is, according to the regulation that creates it, an autonomous body, independent from the Executive Power. *See also* Organic Law No. 27,148 of the Public Ministry, June of 2015. Available at: http://www.infojus.gob.ar/27148-nacional-ley-organica-ministerio-publico-fiscal-lns0006116-2015-06-10/123456789-0abc-defg-g61-16000scanyel

175 Decree 256/2015. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257346/norma.htm

176 Supreme Court of Justice, *Acordada* No. 45/2015, December 29, 2015. Available at: http://old.csjn.gov.ar/docus/documentos/verdoc.jsp?ID=96663

177 Supreme Court of Justice, *Acordada* No. 2/16, February 15, 2016. Available at: http://old.csjn.gov.ar/docus/documentos/verdoc.jsp?ID=96793

178 For more information on this, see Asociación por los Derechos Civiles, "Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones" ["Thoughts on the Creation of the Department of Capturing of Communications," by the Association for Civil Rights.] February 19, 2016. Available at: https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-de-comunicaciones/

179 *Ibid.*

180 *Ibid.*

181 Law Nº 25,520 on National Intelligence, *supra* note 19, article 13.9.

182 *Ibid.*, article 32.

183 *Ibid.*, article 33.

184 *Ibid.*, article 16.

185 Asociación por los Derechos Civiles [Association for Civil Rights], "Quién vigila a los que vigilan" [Who Surveils those who Conduct Surveillance?], p. 15.

186 *Ibid.*, p. 14.

187 Di Santi, Matías, "Marcelo Fuentes: 'Las funciones de la Comisión están claras y su trabajo también'" [Marcelo Fuentes: The duties and tasks of the Commission are Clear], *Chequeado.com*, February 3, 2015. Available at:

http://chequeado.com/ultimas-noticias/marcelo-fuentes-las-funciones-de-la-comision-estan-claras-y-su-trabajo-tambien

188 See the website of the Permanent Bicameral Commission on the Supervision of Intelligence Bodies and their Activities - Law 25,520. Available at: http://www.senado.gov.ar/parlamentario/comisiones/proyectos/104

189 "Cuestionan a la Comisión Bicameral de Inteligencia" [Bicameral Intelligence Commission Questioned], *La Nación*, February 25, 2014. Available at: http://www.lanacion.com.ar/1667003-cuestionan-a-la-comision-bicameral-de-inteligencia

190 Citizens' Initiative to Control the Intelligence System.

191 "Espían y roban correos electrónicos de un juez y de un periodista de Clarín" [Spied on and Stolen E-mails of a Judge and a Clarín Journalist], *Clarín*, May 11, 2006 and Sued, Gabriel, "Espían e-mails de políticos y periodistas" [Spied on E-mails of Politicians and Journalists], *La Nación*, May 23, 2006. Available at: http://www.lanacion.com.ar/808286-espian-e-mails-de-politicos-y-periodistas

192 *See also*, Smink, Veronica, "Procesan al alcalde de Buenos Aires por caso de espionaje" [Mayor of Buenos Aires Prosecuted for Espionage], *BBC Mundo*, available at: http://www.bbc.com/mundo/america_latina/2010/05/100514_2318_macri_proceso_buenos_aires_jg.shtml and Hauser, Irina and Kollmann, Raúl, "El día que Macri quedó Procesado" [The Day Macri was Prosecuted], *Página 12*, May 15, 2010. Available at: http://www.pagina12.com.ar/diario/elpais/1-145731-2010-05-15.html

193 "Escuchas ilegales: la Cámara Federal confirmó el procesamiento de Macri" [Illegal Wiretaps: The Federal Court Confirmed the Prosecution of Macri], *Perfil*, July 15, 2010. Available at: http://www.perfil.com/politica/Escuchas-ilegales-la-Camara-Federal-confirmo-el-procesamiento-de-Macri-20100715-0019.html

194 See, "Una denuncia contra la Gendarmería" [Lawsuit against National Gendarmerie], *Página 12*, November 22, 2011. Available at: http://www.pagina12.com.ar/diario/elpais/1-181754-2011-11-22.html; Thieberger, Mariano, "Proyecto X: Cómo espió la Gendarmería a más de mil organizaciones" [X Project: Gendarmerie Spied on more than a Thousand Organizations], *Clarín*, October 10, 2013. Available at: http://www.clarin.com/zona/espio-Gendarmeria-mil-organizaciones_0_880112088.html; Riera, Ariel and Tarricone, Manuel, "CFK: "Quisieron montar (...) que había una suerte de espionaje de la Gendarmería, Proyecto X, inexistente" [Cristina Fernández de Kirchner: They Made up (...) that there was a sort of Espionage Conducted by Gendarmerie, called X Project, which does not Exist] Available at: https://eff.org/r.ktax; "Un escándalo que reveló la cara oculta de la política de seguridad" [A Scandal that Unveiled Security Policies], *Clarín*, October 10, 2013. Available at: http://www.clarin.com/zona/escandalo-revelo-oculta-politica-seguridad_0_880112093.html

195 One can realize that the scope of the X Project was extensive by looking at the complete list of organizations in the country that were subjected to intelligence activities conducted by National Gendarmerie. *See*, Savoia, Claudio, *supra* note 92, p. 341-383.

196 Law on Personal Data, article 4.

197 *Ibid.*, article 7.

198 *Ibid.*, article 2.

199 Interview with Beatriz Busaniche, from Fundación Vía Libre, "Acá se vigila a quienes interpelan al poder" [Only those who Interpellate the Authority are surveilled], Perfil, January 2, 2015. Available at: http://www.perfil.com/elobservador/Aca-se-vigila-a-quienes-interpelan-al-poder-20150102-0062.html, Santoro, Daniel, "El Gobierno compró equipos para espiar mails y llamados" [Government Buys Spy Equipment to Use on E-mails and Calls], *Clarín*, November 15, 2014. Available at: http://www.clarin.com/politica/Organismos_de_inteligencia-vigilancia-SIDE-espionaje_0_1249075526.html and Savoia, Claudio, *supra* note 92, p. 220.

200 "Hacking Team," July 8, 2015. Available at: https://wikileaks.org/hackingteam/emails/emailid/4517

201 See more in "Hallan muerto al fiscal Alberto Nisman en su departamento de Puerto Madero" [Prosecutor Alberto Nisman Found Dead in his Apartment in Puerto Madero], *La Nación*, January 19, 2015. Available at: http://www.lanacion.com.ar/1761270-hallan-muerto-al-fiscal-alberto-nisman-en-su-departamento-de-puerto-madero and "AMIA Special Prosecutor Alberto Nisman found dead in his Puerto Madero home", *Buenos Aires Herald*, January 19, 2015. Available at: http://www.buenosairesherald.com/article/179900/amia-special-prosecutor-alberto-nisman-found-dead-in-his-puerto-madero-home

202 Marquis-Boire, Morgan, "Inside the Spyware Campaign Against Argentine Troublemakers", *The Intercept*, April 21, 2015. Available at: https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/

203 In that regard, the local legal experts stated that the software found "only works in computers." See more at: Hauser, Irina, "Una lupa sobre el celular y la notebook" [Magnifying Glass on Cellphone and Laptop], *Página 12*, June 8, 2015. Available at: http://www.pagina12.com.ar/diario/elpais/1-274433-2015-06-08.html and "Peritos dictaminaron que el virus en el celular del fiscal no sirve para espiar" [Legal Experts say the Virus in Nisman's Phone Cannot be Used to Spy], *Perfil*, August 26, 2015. Available at: https://eff.org/r.8rvv

204 *See*, O'Donnell, Santiago, "Caso Nisman. Pruebas y sospechas" [Nisman Case: Evidence and Suspicion], *Magazine Revista Anfibia*. Available at: http://www.revistaanfibia.com/ensayo/pruebas-y-sospechas/ and Budassi, Sonia and Fidanza, Andrés, "El rompecabezas Nisman" [The Nisman Puzzle], *Magazine Revista Anfibia*. Available at: http://www.revistaanfibia.com/cronica/el-rompecabezas-nisman/

205 *See*, Smink, Verónica, "Por qué Argentina tiene un problema con sus servicios de inteligencia" [Reasons why Argentina has Problems with its Intelligence Services], *BBC Mundo*, January 27, 2015. Available at: http://www.bbc.com/mundo/noticias/2015/01/150126_argentina_nisman_espias_vs and "Macri reclamó que la muerte de Nisman sea 'un antes y un después'" [Macri Demanded that Nisman's Death be a Turning Point], *Clarín*, January 19, 2015. Available at: http://www.clarin.com/politica/Macri-reclamo-muerte-Nisman-bisagra_0_1288071426.html

206 Law Nº 25,520 on National Intelligence, *supra* note 19, article 5 bis.

207 Law Nº 27,078 Argentina Digital, *supra* note 56, article 5.

208 *Ibid.*, article 60, section d.

209 *Ibid.*, article 5, section 2.

210 Communications Secretariat, *supra* note 62, article 8.

211 Law Nº 27,078 Argentina Digital, *supra* note 56, article 60, section d.

212 Law Nº 25,891 on Mobile Communications Services, *supra* note 64, article 8.

213 *La Nación*, "Florencio Randazzo anunció un nuevo DNI, con chip inteligente" [Florencio Randazzo Announces the Launching of a New Smart DNI with a Built-in Computer Chip], June 27, 2014. Available at: http://www.lanacion.com.ar/1705106-florencio-randazzo-anuncio-un-nuevo-dni-con-un-chip-inteligente.

214 Law Nº 25,520 on National Intelligence, *supra* note 19, article 18.

215 *Ibid.*, Title VI, article 18.

216 Law on Personal Data Protection, Nº 25,326.

217 Law Nº 25,520 on National Intelligence, *supra* note 19, article 19.

218 Law Nº 27,078 Argentina Digital, *supra* note 56, article 5.

219 Communications Secretariat, *supra* note 62, article 8.

220 Law Nº 25,520 on National Intelligence, *supra* note 19, article 16 e.

221 *See*, Communications Secretariat, *supra* note 62 and the law on mobile communications services, *supra* note 64.

222 Law Nº 25,520 on National Intelligence, *supra* note 19, article 20.

223 *Ibid.*, article 16.

224 Law Nº 25,520 on National Intelligence, *supra* note 19, article 16 e.

225 *Ibid.*, article 42.

226 *Ibid.*, article 19.

227 Criminal Code, article 155.

228 Law Nº 25,520 on National Intelligence, *supra* note 19, article 42.

229 *Ibid.*, article 43.

230 *Ibid.*

231 *See*, Bertoni, Eduardo, "Ley de inteligencia, oportunidad perdida" [Intelligence Law, Lost Opportunity], Bastión Digital, February 19, 2015. Available at: http://ar.bastiondigital.com/notas/ley-de-inteligencia-oportunidad-perdida#sthash.Td5djgJU.dpuf

232 Siri, Laura, *supra* note 77, p. 3.

233 *Ibid.*

234 *See*, Bertoni, Eduardo, "Ley de inteligencia, oportunidad perdida" [Intelligence Law, Lost Opportunity], Bastión Digital, February 19, 2015. Available at: http://ar.bastiondigital.com/notas/ley-de-inteligencia-oportunidad-perdida#sthash.Td5djgJU.dpuf

235 In Argentina, Congress holds ordinary sessions between March 1 and November 30. The National Constitution allows the President to call Congress for extension sessions or extra-ordinary sessions (Article 99.9). This is an authority President Macri chose not to exert during the first few weeks of his term. In February 2016, he did call Congress to meet but only to deliberate a limited set of issues, none of which included the decisions and decrees discussed in this document.

236 International Principles on the Application of Human Rights to Communications Surveillance, available at: https://en.necessaryandproportionate.org/text.

237 Decree 257/2015. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257347/norma.htm. This presidential power does not exist in other presidential democracies such as e.g., the United States. It was included in the 1994 constitution, when it was amended. Article 99.3 grants this authority to the President in the following terms:

"The President of the Nation has the following powers: ...3. He takes part in the making of laws according to the Constitution, promulgates them and has them published. The Executive Power shall in no event issue provisions of legislative nature, in which case they shall be absolutely and irreparably null and void. Only when due to exceptional circumstances the ordinary procedures foreseen by this Constitution for the enactment of laws are impossible to be followed, and when rules are not referred to criminal issues, taxation, electoral matters, or the system of political parties, he shall issue decrees on grounds of necessity and urgency, which shall be decided by a general agreement of ministers who shall countersign them together with the Chief of the Ministerial Cabinet. Within the term of ten days, the Chief of the Ministerial Cabinet shall personally submit the decision to the consideration of the Joint Standing Committee of Congress, which shall be composed according to the proportion of the political representation of the parties in each House. Within the term of ten days, this committee shall submit its report to the plenary meeting of each House for its specific consideration and it shall be immediately discussed by both Houses. A special law enacted with the absolute majority of all the members of each House shall regulate the procedure and scope of Congress participation."

238 Code of Criminal Procedure of 1991, Article 224.

239 Code of Criminal Procedure of 1991, Articles 224, 138 and 139.

240 *Code of Criminal Procedure of 1991, Article 234.*

241 *See* Argentina Digital Act, Article 89.

242 *See the analysis in the report, subsection on Due Process.*

243 Article 120 of the Argentina Constitution establishes the following:
"The Public Ministry is an independent body with functional autonomy and financial independence, with the function of promoting the participation of justice for the defense of the legal character of the general interests of society, in coordination with the other authorities of the Republic. It is composed of an Attorney General of the Nation and a General Defender of the Nation, and such other members as the law may establish. Its members enjoy functional immunities and intangibility of remunerations."

244 On this point, *see* ADC, "¿Quien vigila a quienes vigilan? Estudio comparativo sobre sistemas de control de los organismos de inteligencia," Policy Paper (Buenos Aires: Asociación por los Derechos Civiles, May 2014) and ADC, "El (des)control democrático de los organismos de inteligencia en la Argentina," Report. (Buenos Aires: Asociación por los Derechos Civiles, January 2015.)

245 *See* ADC, 2015, p. 7.

246 Decree 256/2015. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257346/norma.htm.

247 See Supreme Court, Decision (Acordada) No. 45/2015, December 29, 2015.

248 *See* Corte Suprema de Justicia de la Nación, Acordada No. 2/16 of February 15, 2016.

249 Asociación por los Derechos Civiles. Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones. February 19, 2016. Available at: https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-de-comunicaciones/.

250 Id.

251 See the analysis in the report, subsection on Public Oversight.