State Communications Surveillance and the Protection of Fundamental Rights in Colombia

By Juan Camilo Rivera and Katitza Rodríguez

March 2016

Fundación Karisma
www.karisma.org.co

ELECTRONIC FRONTIER FOUNDATION

Comisión Colombiana de Juristas

Juan Camilo Rivera is a lawyer at the Universidad del Rosario (Bogota), where he teaches Theory of Law. He has a master's degree in law from Universidad de los Andes (Bogota). He has worked for the Colombian Commission of Jurists, a Colombian NGO, conducting strategic litigation in human rights cases. Currently, he is a legal advisor for the Colombian National Senate.

Katitza Rodríguez is the international rights director at the Electronic Frontier Foundation. She concentrates on comparative policy of international privacy issues, with an emphasis on law enforcement, government surveillance, and cross border data flows. Katitza holds a Bachelor of Law degree from the University of Lima, Peru.

We would like to thank human rights experts, Carolina Botero and Juan Diego Castañeda, both members of *Fundación Karisma,* and Mateo Gómez of *Comisión Colombiana de Juristas,* for their substantial contributions to this report. And to Kim Carlson and David Bogado of *EFF* for their copyediting and formatting contributions.

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

Table of Contents

I. Introduction.....4

II. Constitutional Legal Framework on the Protection of Fundamental Rights vis-à-vis State Communications Surveillance in Colombia.....7

2.1 International Treaties on Human Rights that can be Affected by State Communications Surveillance.....8

2.2 Safeguards for State Communications Surveillance in International Human Rights Law....10

2.3 Constitutional Safeguards for State Communications Surveillance.....11

III. Legal Framework of State Communications Surveillance in Colombia.....13

3.1 State Communications Surveillance in Criminal Legislation.....14

3.2 State Communications Surveillance in Intelligence and Counterintelligence Activities.....17

3.3 State Communications Surveillance in Telecommunications Legislation.....20

IV. Does Colombian Legislation Comply with the International Standards on Human Rights When it Comes to State Communication Surveillance? Recommendations for Improvement.....21

4.1 Adaptation of National Regulations to the International Principles on the Application of Human Rights to Communications Surveillance.....21

V. Recommendations for Improvement.....32

VI. Conclusion.....34

I.
Introduction

Nowadays, States have an increased technological capacity to conduct surveillance on all communications. As stated by the UN Special Rapporteur for Freedom of Expression in his 2013 report, the States have an unprecedented capability to conduct simultaneous, invasive, targeted, and large-scale surveillance activities due to technological advances.[1] This represents a threat to several rights recognized in State constitutions and by international human rights treaties that have been ratified by various States. These rights include privacy, since private information may be accessed without the owner's authorization; freedom of association, since the activities of a group of people may be surveilled; freedom of expression, since communications surveillance may lead to self-censorship or repression; and access to information, since information collected and stored by way of surveillance may be hidden from its owner and used for unknown purposes.

State response to protect these threatened human rights has not always stayed on pace with the advancement of State communications surveillance.[2] Colombia is no exception to this pattern. Colombian legislation on communications surveillance is vague and incomplete. Several laws, decrees, regulations, and international treaties on human rights are included in the Constitution. In some cases, regulations have been passed and implemented after the execution of certain surveillance techniques and strategies. For example, Colombian intelligence services did not have a comprehensive set of regulations to limit their functions and scope for nearly sixty years,[3] until said regulations were established by Act 1621 in 2013.[4]

The lack of a clear and comprehensive normative framework to limit the use of State communications surveillance makes it difficult for the general public to carry out public oversight, especially since many surveillance activities are being carried out surreptitiously, steeped in a culture of secrecy. The absence of regulations may represent the States' lack of awareness about the obligations they have when signing international treaties: under the treaties, States must enact legislation to protect the rights they outline.[5]

State communications surveillance regulation is an issue that is taken seriously in Colombia due to the many related public cases the country has seen over the last few years. Between 2003 and 2008, intelligence services conducted arbitrary acts in a systematic and generalized manner in order to track and surveil journalists, members of the opposition, human rights defenders, high court judges, and individuals who were considered government policy opponents.[6] Most recently, the Colombian media revealed that the country's intelligence service carried out widespread surveillance of key NGOs, journalists, and leftist politicians, including their own governmental team responsible for negotiating a peace agreement with

the Colombian guerrilla, the Revolutionary Armed Forces of Colombia (FARC, in Spanish) in Havana, Cuba,[7] in an operation called "Andrómeda." Moreover, there was an information intelligence leak in the last presidential election in Colombia.[8]

In December 2015, the Colombian press revealed that some national journalists had been subjected to State communication surveillance, denouncing the National Police as one of the institutions conducting it.[9] The complaint is part of a broader context in which it was revealed that the police had acquired new surveillance equipment to carry out massive and intrusive surveillance, as shown by two reports published in mid-2015 by the British NGO Privacy International.[10] Moreover, recent news in the Colombian press shows the Colombian Prosecutor's concern about the potential indiscriminate use of new surveillance technologies by the Colombian Government in cases where the "invasion of fundamental rights is not even necessary in the fight against crime."[11]

This reports aims to analyze current State communications surveillance law and practices in Colombia and to recommend improvements to these regulations and practices, which prioritize human rights to the maximum extent possible. In order to achieve this general aim, the report has two specific goals.

First: To identify and explain Colombian legislation relating to current State communications surveillance, in order to facilitate understanding about the legal framework of surveillance, the institutional oversight mechanisms, and the rights that are guaranteed to an individual. Specifically, this paper describes one particular issue with communications surveillance: how may the State access people's communications? When dealing with State communications surveillance, it's especially important to analyze domestic law with regard to the protection of human rights in order to establish limits for State institutions that conduct surveillance.

Second: To present the international standard on human rights, which should serve as a parameter for State communications surveillance regulations. This report will also assess the extent to which Colombia currently observes such international standards by looking at national regulations and practices. These international human rights standards apply at a domestic level by virtue of the constitutional block—which allows the State to legally invoke treaties at a domestic level in order to protect the rights of those affected by State communications surveillance; and to help draft communications surveillance legislation that better protects human rights.

International human rights law is important to reference when proposing limits to State communications surveillance. In recent years there have been important statements by international bodies about the interpretation and guidelines to define the instances in which a State must comply with its international human rights obligations when

conducting communications surveillance.

Due to the complexity of the technical and legal aspects of this topic, we will use the following terms throughout the document as explained in the International Principles on the Application of Human Rights to Communications Surveillance.[12]

- "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.
- "Communications" include 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.
- "Protected Information" is information that includes, reflects, arises from, or is about a person's communications and that is not readily available and easily accessible to the general public.

II.
Constitutional Legal Framework on the Protection of Fundamental Rights vis-à-vis State Communications Surveillance in Colombia

Communications surveillance is often at odds with several fundamental rights recognized by the Constitution and many international human rights treaties. The most obvious right when speaking about communications surveillance is the right to privacy. There exist many national and international laws that regulate the content of this right. Some of these laws are general, but some are specific and take into account concrete consequences. Either way, as briefly stated in the introduction, the right to privacy is not the only right that's threatened by State communications surveillance. There are other rights at odds with communications surveillance, such as freedom of expression, access to information, freedom of association, and due process. These rights are also regulated by general constitutional provisions. Others are of a legal or regulatory type, which are more specific about the scope and content of each one.

All of these regulations make up the legal framework to protect human rights against State communications surveillance. To apply this framework, it is necessary to address the main provisions regulating individuals' privacy.[13] This report first covers the provisions about communications surveillance that are found in the Political Constitution, where the essential safeguards with regard to communications surveillance are established.

This report includes a contrasting analysis between the provisions in international human rights law and those outlined in the constitution, since the Colombian legal system recognizes the normative nature of international human rights treaties in domestic law. This normative power is not always consistent. Therefore, it is necessary to make some distinctions. As such, this report briefly presents the doctrine of the Constitutional Court on the constitutional block, which specifically focuses on explaining the normative power granted to certain international human rights documents, which are, by nature, the same as some that have studied the application of human rights to communications surveillance in the last few years.

2.1 International Treaties on Human Rights that can be Affected by State Communications Surveillance

Several international documents and declarations made by international bodies reference the rights that can be affected by State communications surveillance. It is essential to include them in the legal framework of communications surveillance in Colombia since, by virtue of the Constitution, international regulations have normative power on the domestic legal system. According to what has been clarified by constitutional jurisprudence, some provisions are binding while others have interpretative power.

The normative power of some of these international law provisions in the domestic system finds its legal basis in the Constitution; it establishes various explicit clauses referencing international law in Article 53, about international job agreements; Article 93, about treaties and regulations on human rights; and Article 214, about international humanitarian law.

Article 93 contains general rules regarding the treaties and regulations on human rights that are valid in domestic legislation. According to this article, there are international treaties—ratified by Colombia and which cannot be suspended in a state of emergency—that possess the same binding characteristics as the Constitution. Others have interpretative power, meaning they may be used to determine the scope and content of the rights recognized in the Constitution.[14]

Abiding by these regulations since 1995,[15] the Constitutional Court has maintained that some of the treaties on human rights and on international humanitarian law, together with the articles in the Constitution, make up the constitutional block. In other words, the regulations with constitutional power are both the ones mentioned in the Constitution and the ones established by international treaties on human rights.[16]

On this basis, the Constitutional Court has allowed declarations made by international bodies like the Inter-American Commission on Human Rights,[17] the Inter-American Court of Human Rights,[18] and the United Nations Human Rights Bodies[19] to influence domestic legislation.

The Constitutional Court has also given domestic normative power to international documents other than international treaties, like the declarations of principles made by the United Nations' institutions.[20] On other occasions, some documents drafted by experts have been used and the Constitutional Court has maintained that they are important for the interpretation of the obligations to human rights undertaken by virtue of the ratification of international treaties that make up the constitutional block.[21]

This constitutional block is important to understand when interpreting the Colombian legal framework in relation to communications surveillance and its respect for human

rights. Due to technological advances in communications surveillance, there are new legal challenges. These challenges have, in part, been dealt with in the past few years by international bodies and experts who have worked to show how international human rights law applies to the context of State communications surveillance. The most important among them is the United Nations' Resolution on the Right to Privacy in the Digital Age,[22] the report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism,[23] the Inter-American Commission on Human Rights about the impact of the Internet on freedom of expression,[24] the report of the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,[25] the report of the United Nations High Commissioner for Human Rights on the scope and protection of the right to privacy in the digital age,[26] and the two newest reports of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on Anonymity, Encryption, and the Protection of Whistleblowers.[27]

Similarly, it is necessary to mention that experts from civil society and the academic world have undertaken the study of the application of international human rights law to State communications surveillance. As a result, principles that establish the regulations and the existing jurisprudence on this subject have been developed. The best example of these types of initiatives is the International Principles on the Application of Human Rights to Communications Surveillance, drafted by several academic experts and activists.

International bodies have already recognized them as authoritative guidelines for the interpretation of the meaning and scope of human rights to communications surveillance.[28] Taking into account the aforementioned Constitutional Court case law, as these principles interpret rights included in treaties that make up the constitutional block—like the American Convention on Human Rights or the International Covenant on Civil and Political Rights—they represent a relevant doctrine for interpreting these rights, regardless of the fact that some of these principles have greater normative power because they replicate existing regulations in treaties that make up the constitutional block.

Finally, the Constitutional Court also recognizes the importance of decisions that were made in various other treaties that Colombia has not signed, but whose content is similar to the ones it did—like, for example, the European Court of Human Rights, which uses the European Convention for the Protection of Human Rights and Fundamental Freedoms. According to the Constitutional Court, the declarations made by the European Court of Human Rights are relevant to Colombian legislation for at least two reasons: first, because national and foreign case law is always a source of interpretation for legal provisions; and second, because, although Colombia has not participated in the European Convention on Human Rights, several of its provisions are replicated in treaties that Colombia has signed. Therefore, its provisions are “useful criteria for understanding the content and scope of

Colombian international agreements on human rights." It is essential to mention the relevance of this body for our analysis, since the European Court of Human Rights has made important decisions related to State communications surveillance, which may provide more reasonable legal solutions for the challenges that it poses.

2.2 Safeguards for State Communications Surveillance in International Human Rights Law

Multiple international treaties that make up the constitutional block include safeguards for individuals' rights against State communications surveillance. Article 11.2 of the American Convention on Human Rights established 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."

According to the Inter-American Court of Human Rights, even when it is not explicitly established in Article 11.2 of the American Convention, the right to privacy also protects telephone conversations and "can even include both the technical operations designed to record this content by taping it and listening to it, and any other elements of the communication process; for example, the destination or origin of the calls, the identity of the speakers, the frequency, time, and duration of the calls, and other aspects that can be verified without the need to record the content of the call by recording the conversation."[29]

According to this court, in order for an interference not to be arbitrary or abusive, it must a) be provided for by law, b) pursue a legitimate aim, and c) be adequate, necessary, and proportionate.[30] These limitations have been generally defined by the Inter-American Court, but are also found in detail in the European Court of Human Rights. The latter has stipulated that surveillance measures, among others, must be based on a particular and precise law, mainly due to the implicit risk of abuse any surveillance system poses and to technological advances that make it easy to carry out these practices.[31] As such, surveillance legislation that is general and vague does not meet the legality criterion.

Similarly, the International Covenant on Civil and Political Rights protects the right to privacy in Article 17, which protects individuals against arbitrary and illegal interference on their private lives. The Human Rights Committee, in charge of interpreting this right, has established that in order for an interference not to be considered arbitrary or illegal, it must be a) provided for by law, b) consistent with the provisions, purposes and aims of the Covenant, and c) reasonable in light of the circumstances of each particular case.[32] Similar to the Inter-American Court, the Human Rights Committee has maintained that not only does this right protect the inviolability of communications, but it also outlaws surveillance activities and other types of interferences on an individual's private life. In this sense, the Human Rights Committee has supported that the right to privacy implies that

"surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping, and recording of conversations should be prohibited."[33]

Safeguards under international human rights law that consider valid limits to the right to privacy are detailed in the International Principles on the Application of Human Rights to Communications Surveillance. Not only do these principles state that interference with the right to privacy, or any human right, must be necessary and proportionate and provided for by law, but they also explain in detail the scope of these safeguards. For example, they mention that in order for a measure to be proportionate, it must a) pursue a legitimate aim, b) be adequate for this aim, c) be necessary, and d) be strictly proportionate, for which they specify a series of burdens of proof on the State in order for communications surveillance to be considered legitimate.

2.3 Constitutional Safeguards for State Communications Surveillance

Article 15 of the Colombian Political Constitution establishes the general legal framework of the right to privacy, specifying its scope and the way in which it may be interfered with. This article recognizes three different rights: the right to privacy, the right to a good name, and the right of habeas data. The Constitutional Court has maintained on repeated occasions that these three rights are autonomous, since they protect different spheres of an individual's life and, as a consequence, require different safeguards.

In general terms, Colombian case law has defined the scope of the protection of these three rights as follows:[34] The right to a good name "refers to the image that members of society have about an individual and his or her behavior, integrity, decorum, qualities, human and professional conditions, and criminal records."[35] In order to illustrate the content of the right to privacy, there is the metaphor "private sphere," which is "exempt of State intervention or arbitrary social interferences," whose protection is deemed necessary to allow full personal, individual, and cultural growth.[36] Finally, habeas data refers to the right to know, update, and rectify any personal information contained in databases and private entities.

From the viewpoint of the Constitutional Court, defining the content of these rights is essential to understanding when they are violated and how their protection may be requested from the authorities. For instance, interference with these rights may occur for several reasons relating to the manipulation of a person's information. In general terms, the right to a good name is violated when a person's data is false or erroneous; the right to privacy is violated when the data references facts that belong a person's private sphere; and the habeas data right is violated when an individual's personal information that's contained

in databases is collected illegally, when it's erroneous (false or out of date), and when it relates to aspects of an individual's private life.[37]

The right to privacy, like any other fundamental right, is likely to be interfered with.[38] Article 15 of the Political Constitution points out that generally, "Correspondence and other forms of private communication shall not be violated," but it specifies that communications may only be intercepted or recorded i) with a court order and ii) in cases and following the formalities established by law. In other words, the Constitution demands legal and judicial safeguards for the interference to the right of privacy. Moreover, Article 28 of the Constitution establishes that every individual is free and thus his or her home may not be searched "except with written order from a competent judicial authority, subject to the legal procedures, and for reasons previously defined by law."

This general rule has a specific exception, also established in the Political Constitution: The Office of the Attorney General has the power to conduct "searches, house visits, seizures and interceptions of communications" without a prior judicial decision. As mentioned above, this is the only circumstance in which the government is permitted to interfere with the right to privacy without a judicial decision. The following is a detailed explanation of the legal regulations on this subject matter.

III.
Legal Framework of State Communications Surveillance in Colombia

Before proceeding to the analysis of the Colombian legal framework on state surveillance of communications, we'll summarize some of the surveillance systems currently known in the country. A report called "Shadow State," published by Privacy International in August 2015, reveals the details of the main platforms for surveillance of communications in Colombia. They include:[39]

- Esperanza (*Hope* in English): This system is used against an individualized person who is under suspicion, and the system is managed by the Prosecutor's office. According to the report, Esperanza is "used to obtain evidence for judicial prosecution on a case-by-case basis." Other safeguards built into Esperanza include "an electronic warrant submission system and supervisory judges." However, according to the report, Esperanza "suffered from various security vulnerabilities and its restriction to accessing data only for pre-defined individual targets on the basis of a warrant was a point of friction for other law enforcement agencies."[40]
- The Single Monitoring and Analysis Platform (PUMA) is presented as a system of telephone and Internet monitoring directly linked to the network infrastructure, managed and funded by the police and managed by the Directorate of Criminal Investigation and Interpol (DIJIN), the unit in charge of the judicial administration. According to the report, the service providers in Colombia not only "know" about the existence of PUMA but have "collaborated in the installation"; however, they are "excluded from its daily operations."[41]
- The Integrated Recording System of the Directorate of Police Intelligence (DIPOL): The DIPOL acquired its own state surveillance of communications technologies since 2005. According to the report, the system was built in order to demarcate their surveillance activities from the Prosecutor's system, Esperanza. The software of DIPOL enables the processing of massive and widespread amount of data, from publicly available information published on social networks to sensitive data such as biometric information. These systems can analyze data and create profiles that determine certain patterns of behavior over time. According to the report, the system "can collect 100 million call records per day and intercept 20 million of SMS messages daily." This data can be combined with biometric data, images, and video, among others. According to Colombian law, the DIPOL are not allowed to engage in "interception" without the supervision of the Prosecutor.[42]

- Hacking tools: The report reveals that DIPOL acquired malicious software (malware) that can infiltrate and control a phone, computer or device remotely. DIJIN is not authorized to engage in "interception" without the supervision of the prosecutor according to Colombian law.

These surveillance systems have been used to surveil the Directorate of Police Intelligence (Dipol) and even Colombian journalists. A recent case (March 2016), which is still under investigation after the publication of this report by a presidential commission, the Attorney General's Office, and the Attorney General's Office, involves journalists reporting on an alleged male prostitution ring that operated within the National Police dubbed "The Fellowship of the Ring."[43] The case involves lieutenants, politicians, and top police commanders and has already led to the resignations of Rodolfo Palomino, Director of the National Police, and Carlos Ferro, Deputy Interior Minister.[44]

In mid-December 2015 journalist Vicky Dávila reported that she was being surveilled and that her coworkers were also having their conversations monitored.[45] In reference to these cases, the Attorney General asked *Fundación Karisma* for a copy of "A Shadow State," the investigation conducted with Privacy International that revealed the use of malware in the country.[46]

Taking into account what is established in Article 15 of the Political Constitution, Article 11 of the American Convention on Human Rights, and Article 17 of the International Covenant on Civil and Political Rights, below you will find an explanation of the Colombian legislation that regulates multiple circumstances in which State authorities may record or access an individual's private communications.

3.1 State Communications Surveillance in Criminal Legislation

Colombian criminal legislation regulates State communications surveillance in two ways: First, criminal procedure law establishes that in order to conduct communications surveillance, it must be for the sole purpose of collecting evidence for a criminal investigation. Second, the criminal legislation outlines a series of behaviors related to communications surveillance that it considers to be illegal and punishable.

According to Article 250 of the Political Constitution, the Office of the Attorney General must take possession of the evidence in the framework of a criminal investigation. It specifies that "when additional measures that imply the infringement of fundamental rights is required, the appropriate authorization must be obtained from the judge responsible for the control of guarantees in order to proceed." In the same way, it stipulates that the Office of the Attorney General may "conduct searches, house visits, seizures, and interceptions of communications" without prior judicial decision, but must get subsequent permission of a

judge within thirty-six (36) hours.

While interpreting these two provisions, the Constitutional Court has stated that the general rule in the Colombian legal system is that the decisions that interfere with the fundamental rights of those being investigated or accused must be provided for by law (legal safeguard) and must be a prior authorization of a judge (judicial safeguard).[47] Exceptionally, the Office of the Attorney General is given the power to interfere with an individual's rights, with the purpose of collecting information relevant to criminal investigations, subject to a subsequent judicial review by a judge. This exception only applies in the cases of searches, house visits, seizures, and interceptions of communications. And these cases are justified only because the evidence is prone to tampering.[48]

The above-mentioned exception must be strictly interpreted so that the safeguard of a prior judicial authorization is not bypassed. Under this rule, for example, the Constitutional Court has held that practices like selectively searching a database for an accused person's confidential information is not one of the activities that may be conducted by the sole request of the Office of the Attorney General of the Nation subject to subsequent judicial review by a judge.[49] Therefore, the Court has demanded that, in order to proceed with such searches, there must be prior judicial authorization.

However, the Office of the Attorney General is allowed to intercept communications; seize data storage devices and mechanisms; and track individuals, objects, or places involved in a criminal investigation without prior judicial authorization, but with subsequent judicial control. The Criminal Procedure Code establishes the cases and the procedures in which the Office of the Attorney General may make use of this power. It indicates that the interception of communications (i) may take place to search for material elements of evidence transmitted through any type of communication that are important to the criminal investigation, (ii) must be justified in writing, (iii) must not be conducted on the communications of the accused and his or her defense lawyer, (iv) must have a maximum validity of three months, and (v) must be subjected to judicial control within 36 hours.[50]

Criminal procedure legislation also stipulates that "competent authorities" shall be in charge of the technical proceedings for the interception and its processing. Despite the vagueness of the law in relation to the authorities in charge of conducting the proceedings, the Constitutional Court endorsed it. The Court argued that the law does specify which authority gives the order and conducts the interception—the Office of the Attorney General of the Nation—and grants this office the power to determine which authorities conduct the interception and processing.

Moreover, even though the law does not specify who these "competent authorities" are, they may be determined through a systematic interpretation of the regulations related to the

technical proceedings of communications interceptions. In Article 46 of Act 938 of 2004, the Court lays down that the aforementioned competence devolves upon the judicial police authorities—currently, those that fulfill these functions are the Technical Corps of the Judicial Police and the National Police.[51]

The Office of the Attorney General also has the power to order the retrieval of information from Internet logs or other similar technologies of the accused person in a criminal investigation, as long as the following are met: (i) the Attorney must have reasonable, well-founded motives to assume that information useful for the investigation has been transmitted through the Internet or similar technological means by the accused; (ii) the Attorney may order the seizure of computers and servers, as well as physical storage devices, that the accused may have used; (iii) the seizure shall be exclusively limited to the time needed to capture the searched data; and (iv) there must be judicial authorization within 36 hours following the seizure.[52]

Moreover, the Office of the Attorney General has the power to conduct surveillance on an accused person during a criminal process. In order to make use of this power, the following must be met: (i) there must exist a prior authorization from the National Directorate or the Sectional Director of the Office of the Attorney General; (ii) there must exist reasonable, well-founded motives to assume that the information of the accused person is useful to the investigation; (iii) the tracking will last for a limited time period; (iv) if there are no results during the year following the issuing of the surveillance order, the surveillance order must be canceled, but it may be issued again when new motives arise; (v) during surveillance, any type of sensible technical means may be used; (vi) surveillance shall have the purpose of collecting information relevant for identifying and individualizing of the perpetrator or any participants, their social relations, the places they frequent, and similar aspects, without unnecessarily affecting the privacy of the accused or third parties; and (vii) there must be subsequent judicial authorization within 36 hours.

Furthermore, there is a law separate from the Criminal Procedure Code that regulates communications interception, but solely when it is related to a very specific situation: when there is a serious disruption of public order.[53] It is the statutory law that regulates the state of emergency (Act 137 of 1994), which allows the national government to intercept or record communications during situations of internal disturbance "with the sole purpose of finding judicial evidence or preventing the commission of crimes," as long as there is judicial authorization.[54]

As stated above, the Colombian criminal legislation provides for a series of crimes related to illegal communications surveillance. Thus, communications interception without judicial authorization is considered a crime—except, of course, in the case of the Office of the Attorney General, as stated in Article 250 of the Constitution. In this regard, Article 296C

of the Criminal Procedure Code establishes that "Anyone who intercepts computer data without prior judicial authorization at its origin, destination, or inside the computer system, or the electromagnetic emissions springing from a computer system shall be punished with imprisonment for a time period ranging from thirty-six (36) to seventy-two (72) months."

Moreover, a new addition was made when reforming the Criminal Code in 2009 which was aimed at protecting information and personal data. Stipulated crimes in the reform include abusive access to a computer system, illegal hindering of computer systems or telecommunications networks, interception of computer data, computer damage, use of malicious software, violation of personal data, and website spoofing for seizure of personal data.[55]

3.2 State Communications Surveillance in Intelligence and Counterintelligence Activities

Separate from criminal prosecutions, the law has provided for the ability to interfere with an individual's rights by conducting communications surveillance through intelligence and counterintelligence activities. On several occasions, the Constitutional Court has deemed the interference with certain rights, like the right to privacy or freedom of expression, legal. Intelligence and counterintelligence activities are aimed at collecting, analyzing, and disseminating information that aids lawmakers and other entities in deciding which measures are suitable for the protection of national security.[56] Hence, they resort to communications surveillance, with the purpose of obtaining information that might threaten national security. Due to the aim these activities pursue, the fact that they interfere with individuals' rights has been deemed legal so long as certain criteria are met. According to the Constitutional Court, "the powers of the intelligence and counterintelligence organizations must be strictly conducted in the framework of the Constitution, international human rights law, and international humanitarian law."[57] Thus, in order to determine the criteria that allows for intelligence and counterintelligence activities, it is important to consult not only the Colombian Constitution, but also international treaties and the provisions contained in international documents.

In this regard, the Constitutional Court has maintained that intelligence activities must (i) be clearly and specifically established by law, which must explain in detail the proceedings to conduct them, the officials who may authorize them and the motivations underlying the authorization; (ii) pursue constitutionally legitimate aims, like the protection of constitutional democracy, national security and national defense; (iii) be necessary, i.e. be strictly required to fulfill this responsibility; and (iv) incorporate elements of accountability, such as periodic intelligence and counterintelligence reports and records of authorized and conducted activities.[58]

International human rights law includes safeguards that are similar to the ones established by the Constitutional Court for conducting intelligence and counterintelligence activities. For instance, the Inter-American Court of Human Rights has pointed out that these activities must meet the criteria that authorize the interference of human rights, which implies that in order to respect the right to privacy, these activities must meet the following requirements: a) they must be provided for by law; b) they must pursue a legitimate aim; and c) they must be adequate, necessary, and proportionate.[59] In addition, "specially strict" controls must be carried out, since the confidentiality under which these mechanisms work may result in the commission of human rights violations and criminal offenses.[60]

The International Principles on the Application of Human Rights to Communications Surveillance outline that the measures that involve communications surveillance must be stipulated by law; pursue a legitimate aim; be adequate, necessary, and proportionate; establish institutional and non-institutional public oversight mechanisms; and guarantee due process and transparency.

The Intelligence and Counterintelligence Law (law 1621 of 2013) enables security agencies to conduct certain activities that pose a potential violation of individuals' rights. This law establishes which agencies can carry out intelligence and counterintelligence in Colombia. According to Article 3 of this law, that function is carried out by units of the Armed Forces and the National Police organized for this purpose, the Unit of Information and Financial Analysis, and others that enforce the law. According to this article, these are the only bodies that can carry out intelligence and counterintelligence.

Among the agencies that carry out intelligence work in Colombia are the following: the National Intelligence Agency, created in 2011 to replace the Administrative Department of Security (DAS); Chief of Joint Military Intelligence and Counterintelligence, under the General Command of the Armed Forces; the Directorate of Police Intelligence (DIPOL), a unit of the National Police in charge of the function of producing strategic intelligence; the Chief of Naval Intelligence; the Chief of Intelligence and Counterintelligence of the National Army; and Headquarters Air Intelligence. It can also perform as a military intelligence in "units or special units" created by the General Command, the National Police, the Army, Navy or Air Force, through an administrative act Forces.[61]

In particular, Act 1621 enables security agencies to conduct the following activities that interfere with individuals' rights: (i) monitor the electromagnetic spectrum (*espectro electromagnético in Spanish*) and (ii) request information from the telecommunications companies to help identify and locate users of these services. This act does not enable communications interception, since it explicitly claims that interception is exclusively regulated by the Political Constitution and the Criminal Procedure Code. As mentioned above, the disclosure of an individual's private information interferes with the fundamental

right to privacy. The following is a detailed explanation of the activities that are allowed by intelligence agencies and how they may affect individuals' private lives.

The Colombian legislation, thus, distinguishes between communications interception and the monitoring of the electromagnetic spectrum. The latter is, according to the Constitutional Court, a "random and indiscriminate tracking activity," and implies "the incidental collection of communications which reveal circumstances that allow the prevention of attacks and the control of risks to the Nation's defense and security. Technically, it is a sort of tracking of shadows, images and sounds represented by electromagnetic radiation and radio waves."[62] That is, the norm creates a legal difference between monitoring communications aimed at national security and intercept communications under the rules of criminal procedure. It is worth mentioning that this definition of "monitoring of the spectrum" corresponds to a judicial interpretation by the Constitutional Court, and that the law does not stipulate any specific views on the definition.

On the other hand, the law defines communications interception as an individualized tracking of a person's communications, with the purpose of collecting evidence for a criminal prosecution, as regulated by the constitutional and criminal legal frameworks.[63]

However, it can be argued that the application of the intelligence legal framework suggests that the "monitoring of the spectrum" (*monitoreo del espectro electromagnético, in Spanish*) is performed in a much broader way that the one defined by the Constitutional Court. As detailed in the report by Privacy International, various agencies in Colombia, as the Directorate of Police Intelligence (DIPOL); the Criminal and INTERPOL Research (DIJIN); and the DAS, until its dissolution, have used "devices for the interception of communications mobile (known generically as IMSI catchers) that allow localized indiscriminate interception of all mobile phone calls and text messages in a specific place." These tasks are far from the "incidental interception"[64] which is how the Court understands the monitoring of communications.

Another key aspect of the Law on Intelligence and Counterintelligence involves the regulation of encrypted voice messages. Paragraph 2 of Article 44 of this law states that operators of telecommunications services must offer intelligence agencies encrypted voice calls. The article adds that this service will be exclusive to high government and intelligence agencies, which can be interpreted as prohibiting the use of encrypted voice messages to those who are not part of high government or intelligence agencies.

3.3 State Communications Surveillance in Telecommunications Legislation

Colombian telecom legislation compels Internet and communications service providers to make their technical infrastructure available for State surveillance in cases relating to "national defense, prevention of states of emergency, and public safety."[65]

So the government adopted a decree that compels Internet and communications service providers to implement and guarantee the technological infrastructure to provide interconnection points and access to communication traffic, so competent authorities can conduct surveillance activities with prior authorization from the Office of the Attorney General of the Nation.[66]

According to this decree, companies are also compelled to give the Office "or any other competent authority"[67] subscriber data such as his or her identity, billing address, and type of connection. The decree stipulates that "network providers and telecommunications service providers must keep their users' information up-to-date and stored for at least five years."

Moreover, intelligence law stipulates that intelligence agencies have the power to request from telecommunications companies information about a) conversation history of connected telephones, b) technical data on the identification of the users involved in an intelligence operation, c) the location of cell towers, and d) any other type of information that contributes to location.[68] In other words, this information does not relate to the content of communications, but to the technical data about them (metadata), which often itself reveals the content of communications or even more sensitive information. Metadata may include information about a person's identity, information about their cellphones and their interactions, or their location and destination. It can show visited web pages, books or sources that were read, the persons with whom an individual interacts, browsing history, technological resources used, and place, time, and proximity to other persons.[69]

This provision in intelligence law compels companies to deliver technical data on the information mentioned therein, setting a maximum time limit of five years. Interestingly, it stipulates that its application should be "technically feasible." That is to say, this provision does not explicitly impose a data retention obligation on companies, but if companies already have the data, the government may request access to it for a time period of up to five years. This suggests that companies must voluntarily implement data retention practices in order for this law to work.

IV.
Does Colombian Legislation Comply with the International Standards on Human Rights When it Comes to State Communication Surveillance? Recommendations for Improvement

The Colombian legislation outlined in the previous section may be at odds with the human rights standards specified at the beginning of this report. In several cases, there is a lack of compliance with multiple international standards on State communications surveillance. These standards aim at protecting, to the maximum extent possible, human rights that may potentially be affected by surveillance activities. What follows is an analysis of the regulations stipulated in the International Principles on the Application of Human Rights to Communications Surveillance—hereafter the Principles. There follow recommendations for improvement so that the regulations are aligned with the Principles. This is particularly relevant since the respect for human rights in all areas is a duty that the Colombian State has agreed to through the signing of international treaties on this subject matter.

4.1 Adaptation of National Regulations to the International Principles on the Application of Human Rights to Communications Surveillance

Legality

According to the Principles, any communications surveillance measure that poses a limitation to human rights must be prescribed by law. Moreover, State communications surveillance must meet a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Finally, the principle of legality states that laws that limit human rights should be subjected to periodic review by means of a participatory legislative or regulatory process for the updating of regulations on State communications surveillance.

In accordance with the Colombian regulations mentioned, the principle of legality has been established in a general way by the Constitutional Court through the doctrine of legal specificity (*reserval legal in Spanish*), which lays out that the decisions that restrict the human rights of those under investigation must be provided for by law. This Principle is, in

practice, respected when it comes to criminal legislation that deals with communication surveillance.

However, when it comes to some situations regarding intelligence activities and regulations on telecommunications, the Principle of legality is not fully complied with.

This Principle has also been mentioned in the decision made by the Constitutional Court about the scope of intelligence activities, demanding that they, as well as their proceedings, the officials in charge, and their motivations, be prescribed by law in a clear and precise way. Nonetheless, intelligence law is vague and ambiguous when regulating a wide range of subjects; activities that limit individuals' rights must be clear and precise, as established by the Principle of legality.

In particular, the motives that justify conducting intelligence and counterintelligence activities—such as the protection of national security, democratic institutions, and national defense, among others—are not clear. The Colombian legislation does not provide examples of the issues that the intelligence and counterintelligence services will be responsible for. This may lead to a situation where intelligence agencies are interpreting and determining when to execute intelligence and counterintelligence activities when, in fact, this should be the lawmaker's job.

Intelligence and counterintelligence law also fails to regulate classification of information. It is the government that does so by decree.[70] The Constitutional Court approved this by arguing that, in all cases, the law provides criteria for the fulfillment of the regulations.[71] By giving the government power to determine classification levels of information, the executive branch may define criteria to classify intelligence information, and it is the intelligence and counterintelligence agencies that must apply this criteria in practice.[72] It is ignored that the secrecy of information, whenever it entails a limitation to the right to access to information, should be clearly defined by law in accordance with the Principle of legality.

Additionally, an important gap contained in this the law was to not specifically define the activities that can be carried out by the intelligence agencies. Especially regarding the monitoring of the electromagnetic spectrum, this is a power that intelligence agencies have and is restricted to monitoring the set of all wavelengths of electromagnetic radiation.[73] In Colombia, this power does not have a legal definition, (there is only one definition of interpretation by the Constitutional Court tied to the electromagnetic spectrum).

In our opinion, the lack of precision in Colombian law partly explains the controversy that has arisen in Colombia in recent years about the legal basis for starting to use massive interception of communications, that will be carry out by intelligence agencies through the systems such as the Single Monitoring and Analysis Platform (PUMA) and the Integrated

Digital Recording System (sigD). The legality of the use of these tools has been questioned by the Public Prosecutor.[74] Disputes of this kind can be avoided by clear and specific laws that indicate precisely the kind of work that can be undertaken and monitoring specific parties authorized to undertake them.

The intelligence legislation must in any case take into account the constitutional rule according to which the interception of communications of people can only be done individually, in the context of criminal proceedings, and with the participation of Public Prosecutions of the Nation and national judicial authorities.

Communications companies' duty to deliver user information to the authorities that fulfill the functions of judicial police is not provided for by law, nor available to the public. It is a decree that compels Internet and communications service providers to deliver user information. Thus, this decree does not have legal standing from the democratic body nor is it published like typical laws. Besides not having the authority of a law, it is not specific enough since it does not specify the circumstances in which its application is appropriate.

Furthermore, it fails to clarify the scope of the regulations on telecommunications that compel Internet and communications service providers to retain user information in the criminal context: it does not specify whether this information should be about users' identification—such as their ID numbers, or mailing address—or whether it should be about the usage of these services—date, time and duration of communications, browsing history, persons with whom they communicate, etc.

This vagueness exists because Decree 1704 from 2012 does not exhaustively prescribe what type of users' information is to be kept by Internet and telecommunications service providers, for it refers in general terms to user information that allows the identification of the users, and it provides few examples of this type of information.

Legitimate Aim

With regard to human rights, the Principles specify that laws should only permit State communications surveillance to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.

In Colombia, the criminal procedure law complies with this Principle by establishing the proceedings that must be followed in order to conduct communications surveillance, with the sole purpose of collecting evidence for a criminal process.

Similarly, the Principle of a legitimate aim has been expressed in the decision made by the Constitutional Court about the limits to intelligence activities, demanding that they pursue constitutionally legal aims, such as the protection of constitutional democracy, national

security, and national defense.

When it comes to telecommunications, the data retention obligations of service providers are not justified by the power that the State has to request it for reasons of "national defense, prevention of states of emergency and public safety."

Necessity

This Principle establishes that the regulations applicable to State communications surveillance must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim.

The Colombian criminal law complies with this Principle, since the Office of the General Attorney is allowed to intercept communications, seize equipments and data storage devices, and track any individual who is involved in a criminal process or the like, with the sole purpose of finding material evidence and physical evidence transmitted through any communications network and which is relevant for a criminal investigation. It must be expressed in writing and may not be used on communications between the accused and his or her lawyer. Moreover, these activities must be carried out over a limited time period—a maximum of three months—and must be subjected to prior or subsequent judicial control.

Likewise, legislation on intelligence and counterintelligence enshrines the Principles of adequacy, necessity, and proportionality. In relation to the necessity Principle, it points out that "intelligence and counterintelligence activities must be necessary to achieve constitutional aims, i.e. they may be resorted to whenever there are no other less detrimental activities available to achieve these aims."[75] Similarly, the decision made by the Constitutional Court about the limits to intelligence activities demands that they be limited to those which are strictly necessary to achieve the specified legitimate aim.

Regarding surveillance regulations on telecommunications, it's been established that Internet and telecommunications service providers must have the technological infrastructure in place to ensure they can access the communications that are sent through their networks. There is no additional regulation that specifies what kind of use they will give to the surveillance technology, nor a rule that describes that the technology that is implemented should be as invasive as possible.

Adequacy

This principle stipulates that any instance of communications surveillance authorized by law in each country must be appropriate to fulfill the specific legitimate aim.

The adequacy Principle is recognized in intelligence and counterintelligence legislation. Article 5 of Act 1621 of 2013 outlines: "Intelligence and counterintelligence activities must

make use of measures that are adequate for the aims defined in Article 4 of this Act; that is to say, the most adequate measures for the fulfilling these aims are to be used, and any others should be discarded." In this provision, the law establishes that the information collected through activities related to monitoring the electromagnetic spectrum (*espectro electromágnetico in Spanish*) that is useless for the objective of the investigation must be destroyed and not stored in databases.[76] Furthermore, intelligence law stipulates that each organization in charge of fulfilling these functions must create a committee to update and eliminate intelligence data and information.

The committees shall respect that information collected for anything other than intelligence activity "must be eliminated from their databases and records; and it shall be stored in a historical archive until the Commission for the classification of information (*Comisión para la depuración*) submits its report on recommendations."[77]

Proportionality

The observance of these Principles requires that regulations on communications surveillance must include mechanisms that protect human rights violations against authorized communications surveillance measures. Akin to the assessment of whether the mechanisms outlined in the regulations are efficient at verifying if interference is limited and reasonable in relation to the specified legitimate aim is the preservation of human rights to the maximum extent possible.

The proportionality Principle can be seen in Colombian criminal legislation, since whenever the Office of the Attorney General of the Nation requires the seizure of equipments of the information produced while surfing the Internet or similar media of an accused individual during a criminal investigation, the Office must prove that it has reasonable, well-founded motives to conclude that the accused individual has been transmitting information that is useful to the investigation. Said procedure must be conducted in the necessary amount of time required to seize the desired information, and there must be subsequent judicial control within 36 hours following the request for the seizure of equipments.[78]

This is also explicitly provided for by the legislation on intelligence and counterintelligence. Article 5 of Act 1621 of 2013 outlines: "Intelligence and counterintelligence activities must be proportionate to the pursued aims and their benefits must exceed the restrictions imposed on other principles and constitutional values. Particularly, the means and methods used must not be disproportionate in relation to the pursued aims."

On the contrary, in the legislation on telecommunications, mandatory data retention has been vaguely regulated and may be highly disproportionate. It is not clear whether Internet and communications companies must exclusively retain subscriber information, or data about a person's use of the services—date, time and duration of a communication, browsing

history, etc. Mandatory data retention of metadata and subscriber information is absolutely a clear disproportional infringement on the right to privacy, as argued by the European Court of Justice when analyzing the European directive on data retention.[79]

According to the European Court of Justice, mass data retention exclusively conducted for a limited time period is a disproportionate infringement on the right to privacy, for (i) it encompasses the entire population of a nation, any means of communication and all data traffic without limitation, differentiation or exception; (ii) it does not have an objective criterion to determine the circumstances for when data can be accessed or a procedure for this to happen; and (iii) it does not distinguish the duration of data retention or the usefulness of the retained data.[80] The International Principles on the Application of Human Rights to Communications Surveillance point to the same direction, as they dictate that mass data retention that is not relevant to face a specific threat is an infringement on the right to privacy.

Competent Judicial Authority

The observance of the Principles regarding this subject matter in order to protect human rights to the maximum extent possible is guaranteed by the authorization for a communications surveillance measure from a competent judicial authority, who shall be impartial, independent, and also versed in technology and shall have the appropriate resources to fulfill his or her functions on this matter.

In Colombia, the Constitutional Court has established the rule of judicial safeguard, which implies that the general principle in the Colombian legal system is for decisions that infringe upon human rights of those being investigated must involve judicial authorization.

According to Article 250 of the Political Constitution, the Office of the Attorney General must take possession of the evidence during a criminal investigation, and it also states that "when measures that could infringe upon fundamental rights are necessary, the appropriate authorization must be obtained from a judge in order to proceed." In the same way, it stipulates that the Office of the Attorney General may "conduct searches, house visits, seizures and interceptions of communications" without prior judicial authorization, but must subsequently get authorization from a judge is needed within thirty-six (36) hours. This exception only applies in the cases of searches, house visits, seizures and interceptions of communications. These are only justified because they factual information which is prone to sudden changes and easy to alter, which would be detrimental for the criminal investigation.[81]

The judicial control of intelligence activities is limited to communications interceptions, and does not apply in cases of communications monitoring.

Finally, the regulations on telecommunications do not mention the existence of a judicial order as a requirement for the delivery of users' identification data, which ignores the safeguards for individuals' rights, made up by the judicial revision of legality and proportionality of the measure taken.

Due Process

In order to protect human rights that are affected by surveillance, the Principles require that the authorization of a communications surveillance measure be conducted in the framework of due process, which provides for a public hearing for the individual affected, within a reasonable time period (prior or subsequent to the authorization of the measure) in an independent, competent and impartial tribunal. Additionally, there must be opportunities for remedy.

As has been discussed, when a suspect's right to privacy is interfered with in a criminal investigation, a judge must intervene either before or after the measure is taken. In communications interception and correspondence searches, the person on whom such measures were taken should be allowed to know the results and be allowed to participate in a hearing—once there has been a formal accusation in the process—or to request a hearing in order to ask for evidence produced through surveillance to be excluded.[82]

User Notification

One of the safeguards provided by the Principles is that all individuals subject to communications surveillance should be notified and allowed to challenge the decision. In criminal law, this Principle is guaranteed since an individual who has been surveilled has the opportunity to question the legality of the measures taken against him or her in a hearing. Depending on the stage where in which the criminal procedure is, the accused may have the ability to intervene in a hearing about the legality of the tracking measures or to request a new hearing to ask for the exclusion of evidence.

Intelligence regulations do not provide for user notification of communications surveillance, which is a State duty that may only be suspended—though not obviated—when certain circumstances arise, according to what is established by the Principles. In Colombia a person may not know whether there have been intelligence activities carried out against him or her in present time, or in the past. They may not ask for correction, nor is there a judge who controls certain intelligence activities that can have an impact on an individual's human rights.

Transparency

The Principles require the implementation of transparency measures in the regulations on communications surveillance. The State should publish, at 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. The goal is to provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance.

The Transparency Principle has been recognized in the decision made by the Constitutional Court about the scope of intelligence activities, demanding that they include elements for accountability, such as the submission of periodic intelligence and counterintelligence reports and a record of the authorized and conducted activities.

However, intelligence law does not provide for a public mechanism to oversee intelligence activities. Instead, it establishes internal and external controls of intelligence activities. Among the external ones, we find judicial intervention—limited to communications interception: It does not apply in cases of communications monitoring—and public control, in charge of the Legal Commission for the Monitoring of Intelligence and Counterintelligence Activities. This Commission has three main functions: to conduct political follow-up and oversight, to verify the efficient use of resources, and to confirm the legality of intelligence services actions. The powers of this Commission are devoted to inspecting the functioning of the oversight mechanisms of intelligence activities.

The first paragraph of Article 22 says that the Legal Commission shall be able to meet with the Joint Intelligence Committee, have access to the annual reports form inspectors, request additional information from the inspectors and the internal control offices, summon the chiefs and directors of the intelligence agencies and be acquainted with the national intelligence aims outlined in the Colombian National Plan of Intelligence. Thus, in order to verify the legality of the actions conducted by intelligence and counterintelligence agencies, the Legal Commission shall be limited to judge on the basis of the information that the agencies themselves provide, which is especially critical when it comes to secret activities, since those who conduct them may, as an excuse, say that information is confidential in order hide their actions.

In criminal law, transparency on State surveillance measures is promoted due to the fact that the criminal proceedings are governed by the principle of publicity. In the application of this principle, the hearings in which the legality of communications interception and other surveillance measures are verified are open to public scrutiny. In any case, the principle of publicity of judicial acts admits exceptions enshrined by law to protect fundamental rights and to develop constitutional principles and values. Specifically, Article 18 of Act 906 of 2004 stipulates that the judge may limit the publicity of the procedures when he or she considers that "it jeopardizes the victims, juries, witnesses, judicial experts and other participants; national security is affected; it inflicts psychological damage upon

the underage involved; the right to a fair trial for the accused is diminished; or the success of the investigations is seriously compromised."

Integrity of Communications and Systems

The observance of this Principle requires that the national authorities refrain from demanding that communications service providers or hardware and software providers develop the capability to surveil, collect, or retain certain information exclusively for State surveillance purposes. *A priori* data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users

In this regard, the Colombian legislation on telecommunications establishes that the State may intervene in the area of information technologies and communications so that the Internet and communications service companies provide their services and allow the use of their infrastructure, as long as the intervention is carried out for purposes such as "national defense, prevention of states of emergency, and public safety."[83]

In using this legal power, the government issued a decree requiring Internet and communications service providers to implement and guarantee the necessary technological infrastructure to allow competent authorities, with a prior authorization from the Office of the Attorney General, to conduct interception of communications.

Act 1621 relating to intelligence activities enables security agencies to request information that helps to identify and locate users from the telecommunications companies. However, the limits to these activities are the regulations provided for by the Political Constitution and by the Criminal Procedure Code.

Those provisions seriously affect the Principle of Integrity of Communication System.

Safeguards for International Cooperation

The Principles take into account the existence of international mutual legal assistance treaties (MLAT) applying to communications surveillance, in order to guarantee the highest level of protection for individuals in each of the countries. Additionally, this Principle stipulates that whenever the States seek assistance for internal law enforcement purposes, the principle of dual criminality should be applied.

There is a Colombian-French agreement on information exchange about transnational organized crime.[84] Article 2 of this agreement provides for regulations on the processing of identification data transmitted from one country to the other as a result of the agreed upon assistance. The communication of data must be conducted explaining which specific purposes it has and its period of use. When this period has finished, the data must be

destroyed. The types of transnational crime considered for information exchange are: terrorism, asset laundering, drug trafficking, arms trafficking, counterfeit money, human trafficking, illicit trafficking of cultural property, industrial and intellectual property infringements, and illegal trafficking of natural resources.

Colombia has signed a treaty on security cooperation aimed at exchanging intelligence information with the North Atlantic Treaty Organization (NATO).[85] This Agreement establishes measures for the exchange and protection of the information shared between the parties. Some of these measures include the protection of and safeguards for the information and material exchanged between the parties, which implies the observance of mutual security proceedings, as well as the commitment of confidentiality in relation to third parties, unless there is consent from the party originating such information.

There is also an agreement between Colombia and the European Police Office.[86] Among other sorts of cooperation, this agreement is based on the exchange of information regarding serious international organized crime investigations, such as drug trafficking, crimes related to nuclear materials, illegal immigration, human trafficking, crimes related to motorized vehicles, counterfeit money and money laundering. The agreement provides for a series of provisions related to the purpose of exchanging information, the way of transmission and preservation, as well as the possibility to classify its level of confidentiality and the measures devoted to limiting and protecting the use of the exchanged information.

The International Convention for the Suppression of Terrorist Bombings[87] provides for some multilateral agreements on information exchange. This Convention requests that the States exchange information related to the location of the individuals responsible for an offense and immediately take the necessary measures—which ought to be in accordance with national legislation—required to investigate acts related to terrorist bombings. It further establishes that any person who is taken into custody or has been involved in any other measures or proceedings shall be guaranteed fair treatment, including enjoyment of all rights and guarantees in accordance with the law of the State in the territory of which that person is present and applicable provisions of international law, including international human rights law.

A bilateral agreement between the Government of the Republic of Colombia and the Government of the Federative Republic of Brazil on Cooperation on Security matters also exists.[88] The aim of this agreement is to promote cooperation between Colombia and Brazil on security matters, especially in investigation, logistic support, aviation, maritime and land industry, knowledge exchange about experiences and expertise, and mutual training activities, in order to enhance the responsiveness of national authorities in both countries and to increase the exchange of experiences, expertise and strengths in the many areas. The parties in this agreement are committed to keeping the confidentiality of the information

and material exchanged between them.

Safeguards against Illegitimate Access and Right to Effective Remedy

The Principles establish that States should enact legislation criminalizing illegal communications surveillance by public or private actors, in order to protect communications privacy. Moreover, it stipulates that the law should provide avenues for redress by those affected.

The Colombian criminal legislation provides for criminal penalties for illegal communications surveillance. Communications interception without a judicial decision is a crime—except for the case of the Office of the Attorney General of the Nation, according to what is established in Article 250 of the Constitution. In 2009, the types of crime related to the abusive access to a computer system were added, as well as the illegal hindering of computer systems and telecommunications networks, the use of malicious software, violation of personal data, and the website spoofing of websites for the seizure of personal data.[89]

On the other hand, intelligence and counterintelligence law does not provide for a remedy for the defense of the individuals who think that are being surveilled. In fact, those who think that are being surveilled do not have a remedy for them to verify if they are indeed the object of surveillance, and they are unable to request the correction, updating and, in their case, filtering of information. In 2009, the Inter-American Commission on Human Rights expressed its concern to the Colombian State about the lack of a remedy of the sort,[90] which was not corrected by Act 1621 of 2013. This Act only mentions that there shall be a commission for the filtering of intelligence records, which shall make recommendations to the national government about data filtering and filtering of intelligence records, which shall be of use for the government to "guide" a filtering system on data and records.[91]

The existence of this remedy is consistent with the case law of the Constitutional Court, which has held that "there is confidentiality with regard to the content of a public document, but not with regard to its existence."[92] This provides a solid justification to the idea that there should be a remedy by which individuals know whether there exists information against them, even if they could not have access to said document.

The lack of this remedy is even more serious when one takes into account that the communications history of the connected phones, the technical identification data of the users who are being surveilled, the location of cell towers and any other type of information that contributes to location must be delivered to intelligence agencies without the need for a judicial control whatsoever, despite the fact that this information interferes with the privacy of the users and, hence, it should have some kind of legal protection.

V.
Recommendations for Improvement

In order to adapt the Colombian legislation on communications surveillance to what is provided for by international human rights law, there are several alternatives that could be taken into account by civil society. The following are four recommendations; three of them are related to legislation and regulations on intelligence and counterintelligence activities, and the other is related to the obligations telecommunications companies have to cooperate with the national authorities.

The Colombian legal system provides for different actions that allow a challenge to the validity of the Colombian legislation that is at odds with international human rights law. Thus, Colombian laws—like the intelligence and counterintelligence law—may be contested through the action of unconstitutionality, and the decrees—like the one that regulates data retention—may be challenged through simple nullity. In the framework of a judicial process or administrative operation, it is also possible to present the applicability of the unconstitutionality exception, to request the invalidity of a regulation that is not recognized in the Constitution.

The action of unconstitutionality would be appropriate even for intelligence and counterintelligence law (Act 1621 of 2013), which was completely revised by the Constitutional Court, taking into account that in its sentence[93] this court only dealt shortly with different serious aspects regulated by this act briefly, which would allow for a new sentence by the court, by virtue of the relating *res judicata*. The same happens, for instance, with the scope of the obligation to cooperate that the communications service providers have. In this issue, the possibility for these companies to conduct mandatory data retention has not been dealt with.

When it comes to the specific legislation on intelligence activities, the Advisory Committee for the Filtering of Intelligence Records (Comisión Asesora para la depuración de archivos de inteligencia) may be an interesting instance of advocacy, since its purpose is to make recommendations about policy in the framework of a serious issue related to communications surveillance: the filtering of intelligence records. In its report submitted to the national government, this commission may suggest important adjustments for the legislation on intelligence, such as the need for a mechanism that enables individuals to request information about the existence of intelligence activities conducted against them.

To strengthen the controls on the functioning of intelligence and counterintelligence

activities, it's important to work side by side with the Legal Commission for the Monitoring of Intelligence and Counterintelligence Activities, with the purpose of setting the scope and properly and efficiently controlling the agencies that provide these services. For instance, it would be of great importance that, in its regulations, the commission make it clear that it will have access to information other than the information handed by the intelligence agencies and their internal control mechanisms, so that the control it exercises is more effective. As argued by the Colombian Commission of Lawyers (*Comisión Colombiana de Juristas*) in the revision of Act 1621 of 2013, in order to be effective:

> *"The Legal Commission should have access to the information that is not necessarily handled by the same agencies it controls, as in the case of the information delivered by members of the civil society, or information obtained directly by the Commission, through investigations conducted on its own initiative. For that matter, it is important to mention that in several legislations the parliamentary oversight mechanism may conduct investigations on its own initiative, request access to any type of intelligence information—not only to information delivered by internal control mechanisms—and summon any intelligence and counterintelligence officials, not only chiefs or inspectors."*[94]

The Colombian legislation is particularly ambiguous in regards to the scope of the obligation that involves telecommunications companies handing over data to intelligence agencies. This should be clarified. As previously stated, Article 44 of Act 1621 requires that telecommunications companies deliver subscriber data to intelligence agencies, and in any case, the agencies shall limit their request to a time period of, at most, five years. This implies that, in order for this obligation to work, telecommunications companies should already have the data storage technology covering that period. What happens to the companies that do not have this technology is yet to be known, as well as what would happen to a company that has the technology but wants to stop using it. These issues must be solved by law.

There is also uncertainty about the scope of the regulation that stipulates that "Internet and telecommunications service providers must keep their subscriber information up to date and store it for at least five years." It is necessary to clearly specify that this provision does not compel companies to keep data about users' communications or also known as metadata, since it would be a disproportionate intrusion on Colombian human rights.

VI.
Conclusion

Recent international revelations about the intensity and areas in which various authorities carry out communications surveillance have caught the attention of the civil society, interested in limiting the scope of action of the authority in order to guarantee the protection of human rights that are so often affected by surveillance activities. The achievement of this purpose poses a lot of different challenges: the most basic one is to understand the way in which the nation regulates State communications surveillance measures to understand what is legal and what isn't. One of the most complicated ones would be to identify the way in which said legislation is applied on the day-by-day, given the pace of technological advances that enable surveillance.

This report aims to be a tool for the assessment and debate about the necessary safeguards in Colombia in order to protect individuals' rights from State communications surveillance. Having this purpose in mind, this report has presented the regulations granting different agencies the power to conduct communications surveillance on individuals, seeking to schematically and comprehensively explain the legal framework in which they are immersed. It has also mentioned the national and international case law, as well as the application of specific regulations, aiming to provide an answer to the issues of adapting the regulations and practices of State communications surveillance to the protection of human rights.

Moreover, this report provides further recommendations applicable for the adaptation of the Colombian national legislation to the international standards for the protection of human rights against State communications surveillance.

Even though the legislation has begun to deal with diverse aspects of communications surveillance—criminalizing illicit data and communications access and regulating intelligence activities, among others—the regulations it provides fail to be absolutely clear, complete and sufficient, or in some other cases, the legislative brand has yielded these tasks to the executive power—for instance, the delimitation of the level of classification of intelligence information. The above poses a serious threat to the right to privacy, freedom of association or freedom of expression, which is why these must be taken into account by competent authorities. The inaction of the Colombian State in relation to the aforementioned problems may challenge, at an international level, its commitment to the acknowledgment of and respect for human rights.

1 Frank La Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, United Nations, A/HRC/23/40, April 17, 2013, paragraph. 33, available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

2 In this regard, the United Nations High Commissioner for Human Rights stated that, "*Revelations about digital mass surveillance have raised questions around the extent to which such measures are consistent with international legal standards and whether stronger surveillance safeguards are needed to protect against violations of human rights."* The Right to Privacy in the Digital Age, A/HRC/27/37, Report of the Office of the United Nations High Commissioner for Human Rights, June 30, paragraph 15, available at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G14/068/74/ PDF/G1406874.pdf?OpenElement

3 The Colombian Administrative Department of Security was created by Decree 2872, on October 31, 1953, available at: https://www.redjurista.com/documents/d2872_53.aspx

4 Statutory Law №1621, of April 17, 2013, by which regulations are passed in order to strengthen the legal framework that allows the agencies conducting intelligence and counterintelligence surveillance activities to accomplish their constitutional and legal mission, available at: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

5 Article 2.1 of the American Convention of Human Rights and Article 2.2 of the International Covenant on Civil and Political Rights.

6 Among others, the United Nations High Commissioner for Human Rights took a stance about this practice and described it as follows: "Information was made public in 2009 that DAS (the national civil intelligence agency reporting directly to the President) had conducted widespread and systematic illegal intelligence operations going at least as far back as 2003. These operations targeted, inter alia, human rights defenders, political opposition leaders, journalists and high-level government officials, such as the Vice-President. Furthermore, disturbing information appeared in the public domain that even magistrates of the Supreme Court were subject to surveillance. The Inter-American Commission on Human Rights, a United Nations special rapporteur and OHCHR-Colombia itself were targeted as well. These actions, in many cases, had the objective of invalidating the work of the victims, who were considered as "legitimate targets" for being potential opponents to Government policies." Annual report of the United Nations High Commissioner for Human Rights of the situation of human rights in Colombia, document A/HRC/13/72, March 4, 2010, paragraph 14, available at: http://www.hchr.org.co/documentoseinfor-mes/informes/altocomisionado/Informe2009_esp.pdf

7 Did someone spy on the negotiators in La Habana? (¿Alguien espió a los negociadores de La Habana?,) Semana Magazine, February 3, 2014, available at: http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3

8 El video del 'hacker' y Zuluaga, Semana Magazine, May 17, 2014, available at: http://www.semana.com/nacion/articulo/el-video-del-hacker-con-oscar-ivan-zuluaga/388438-3

9 El Tiempo, Research Unit, These are the emails that prove the tracking of Vicky Dávila, 7 de December, 2015, available at: http://www.eltiempo.com/politica/justicia/pruebas-de-seguimientos-a-vicky-davila/16451812

10 Privacy International, Demand/Supply: Exposing the Surveillance Industry in Colombia, September 2015, available at: https://www.privacyinternational.org/node/638. See also, Privacy International, Shadow State: Surveillance, Law and Order in Colombia, August 2015, available at: https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf

11 El Tiempo, Prosecutor says 'no' to the Police interception system 'Puma', August 30, 2015, available at: http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092

12 *International Principles on the Application of Human Rights to Communications Surveillance* (2014). Available at: https://necessaryandproportionate.org/text [Accessed September 6, 2015]; See also, Frank La Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/23/40, 17 April, 2013, page 3.

13 In the original paper, written in Spanish, the terms "privacy" and "intimacy" are synonyms. They both make reference to the same right. The former is used at the international level—where we speak of "private life"—and the latter is used at the national level—where we speak of the right to intimacy.

14 Jaime Rodríguez v. Iván Mejía Alvarez, sentence T-1319, Constitutional Court, December 7, 2001, available at: http://www.corteconstitucional.gov.co/relatoria/2001/t-1319-01.ht

15 Constitutional revision of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, and of Act 171 of December 16, 1994, through which said protocol was passed, sentence C-225, Constitutional Court, May 18, 1995, available at: http://www.corteconstitucional.gov.co/relatoria/1995/C-225-95.htm

16 To see a more comprehensive analysis of the constitutional block doctrine, go to Carlos Ernesto Molina's complaint of partial unconstitutionality against article 19 of the Substantive Labor Code, sentence C-401, Constitutional Court, April 14, 2005, available at: http://www.corteconstitucional.gov.co/RELATORIA/2005/C-401-05.htm and Rodrigo Uprimny Yepes, Constitutional, Human Rights and New Criminal Procedure Block, Judicial School Lara Bonilla, Superior Council of Judicature, Bogotá, 2006.

17 On several occasions, the Constitutional Court has taken decisions made by the Inter-American Commission on Human Rights to interpret the regulations appropriate for its own decisions.

18 See Ernesto Rey Cantor's complaint of unconstitutionality against articles 2 (partial), 3 (partial), 5, 6 (partial) 7 c) and f), 8 third section, 10, 11 (partial), 13 first section, 14, 15 (partial), 19 and 20 f) of Act 74 of 1966, through which the transmission of broadcasting services is regulated, sentence C-010, Constitutional Court, January 19, 2000, available at: http://www.corteconstitucional.gov.co/relatoria/2000/c-010-00.htm, in which the Court claimed that inasmuch as the Constitution establishes in article 93 that the constitutional rights and obligations must be interpreted in accordance with the international human right treaties ratified by Colombia, it is evident that the case law of international courts, in charge of interpreting these treaties, make up a hermeneutic criterion relevant to establish the meaning of constitutional regulations on human rights.

19 On multiple occasions, the Constitutional Court has granted a relevant nature to the decisions made by the UN Human Rights Committee, and in some cases, it has made them binding. For instance, in a case about freedom of expression, the Court maintained that For the purpose of this case, the constitutional block related to freedom of expression must be made up by international regulations, namely the Pact of San José and the International Pact on Civil and Political Rights, as well as the interpretations of those documents made by the Inter-American Commission on Human Rights, the Inter-American Court of Human Rights and the United Nations Human Rights Committee. Also, opinions shall be granted a different importance, for the judicial nature of the Inter-American Court of Human Rights and its power upon Colombia implies that opinions must be taken into account and shall not be domestically ignored. Rodríguez v. Alvarez, sentence T-1319, Constitutional Court, 2001. Also, see sentences C-872 of 2003, C-370 of 2006, T-391 of 2007, C-728 of 2009, among others.

20 See, among others, sentences C-370 of 2006, T-821 of 2007 and C-579 of 2007. In sentence T-821 of 2007, in relation to the Guiding Principles on Internal Displacement, established in the Report of the Special Rapporteur

of the United Nations Secretary-General on Internal Displacement and the Principles on Housing and Property Restitution for Refugees and Displaced Persons, the Court maintained that they make up the constitutional block lato sensu, as they are developments adopted by international doctrine, of the fundamental right to the full reparation of the harm. Rosmira Serrano Quintero v. Presidential Agency for Social Action and International Cooperation, sentence T-821, Constitutional Court, October 5, 2007, available at:http://www.corteconstitucional.gov.co/relatoria/2007/t-821-07.htm

21 Thus, for example, as regards the Limburg and Maastricht Principles, related to States' obligations on economic, social and cultural rights, prepared by experts, the Court has maintained that they do not have a binding power, though they might be used to interpret the scope of the rights established in the International Covenant on Economic, Social and Cultural Rights (ICESCR) and the Protocol of San Salvador and the obligations on the Colombian State as regards this subject. The latter are international documents that make up the constitutional block. Carlos Rodríguez Díaz's complaint of unconstitutionality against articles 25, 26, 28 y 51 (as alleged) of Act 789 of 2002, By which regulations are stipulated to support employment and to broaden social security, and some articles of the Substantive Labor Code are modified, sentence C-257, Constitutional Court, March 12, 2008, available at: http://www.corteconstitucional.gov.co/RELATORIA/2008/C-257-08.htm. On another instance, while making reference to the Chapultepec, Johannesburg, and Lima Principles on freedom of expression, it claimed that although they do not make up the constitutional block, they are a relevant doctrine for the interpretation of international treaties that do make it up, Zonia Betancourt Rojas and Gabriela Fuquene Betancourt v. National Police, Constitutional Court, sentence T-511, June 18, 2010, available at: http://www.corteconstitucional.gov.co/RELATORIA/2010/T-511-10.htm

22 Resolución de la Asamblea General de las Naciones Unidas, El derecho a la privacidad en la era digital, UN Doc. A /RES/68/167, 18 de Diciembre de 2013, disponible en: https://eff.org/UN-A-RES-68-167

23 Ben Emerson, Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, UN Doc. A /69/397, disponible en: https://eff.org/A-69-397.

24 Catalina Botero, Annual Report of the Office of the Special Rapporteur for Freedom of Expression, Inter-American Commission on Human Rights, OEA/Ser.L/V/II.149, December 31, 2013, available at: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_22_ia_2013_esp_final_web.pdf

25 Frank La Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 2013.

26 The Right to Privacy in the Digital Age, 2014.

27 David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, on anonymity and encryption UN Doc. A/HRC/29/32, disponible en: https://eff.org/A-HRC-29-32.

28 International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/analisislegal

29 Case of Escher et al v. Brazil, Interpretation of the Judgment on Preliminary Objections, Merits, Reparations, and Costs. Inter-American Court of Human Rights, sentence on July 6, 2009. Series C Nº 200, paragraph 114.

30 Tristán Donoso v. Panama, Interpretation of the Judgment on Preliminary Objections, Merits, Reparations, and Costs. Inter-American Court of Human Rights, sentence on January 27, 2009. Series C Nº 193, paragraph 55.

31 Uzun v. Germany, Case Nº 35623/05 European Court of Human Rights, sentence on September 2, 2010,

paragraph 61 and Weber and Sarabia v. Germany. Case № 54934/00, sentence on June 29, 2006, paragraph 93.

32 Human Rights Committee, General Comment № 16, Article 17 - The Right to Privacy, paragraph 4.

33 Idem, paragraph 8.

34 See Juan Carlos Upegui Mejía, Habeas data. Fundamentos, naturaleza, régimen, Edition Universidad Externado de Colombia, Bogotá, 2008.

35 German Colonia and Ana Mercedes Marin v. Administration of Residential Unit "Los Nogales", sentence T-228, Constitutional Court, May 10, 1994, available at: http://www.corteconstitucional.gov.co/relatoria/1994/T-228-94.htm

36 Rosa Estelia Peña Carabalí v. Caleb Antonio Avendaño Mosquera, sentence T-787, Constitutional Court, August 18, 2004, available at: http://www.corteconstitucional.gov.co/relatoria/2004/t-787-04.htm

37 Constitutional Court, sentences T-129 of 2010, T-067 of 2007, T-411 of 1995, among others.

38 The case law on the non-absolute character of fundamental rights is abundant. In one of the sentences in which the Constitutional Court made reference to this, it indicated: "fundamental rights, regardless of their constitutionality and importance, are not absolute and, therefore, must be consistent with each other and the other goods and values protected by the Constitution, for, if otherwise, the absence of this essential relativism may lead to the impossibility of social and institutional life." Constitutional Court, sentence C-239 of 1997.

39 See also, info-graphic explaining in detail the monitoring programs designed by Karisma Foundation, S*urveillance systems in Colombia exposed*, available at: https://karisma.org.co/sistemas-de-vigilancia-en-colombia-al-descubierto/

40 Privacy International, Shadow State: Surveillance, Law and Order in Colombia, August 2015, available at: https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf

41 Privacy International, Shadow State: Surveillance, Law and Order in Colombia, August 2015, available at: https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf

42 Privacy International, Demand/Supply: Exposing the Surveillance Industry in Colombia, September 2015, available at: https://www.privacyinternational.org/node/638

43 Crisis en la Policía: todos perdieron. Revista Semana. 20 de Febrero de 2016 http://www.semana.com/nacion/articulo/vicky-davila-palomino-y-ferro-escandalo-en-la-policia/461249

44 Las investigaciones pendientes en el escándalo de la Policía. El Tiempo. 18 de Febrero de 2016 http://www.eltiempo.com/politica/justicia/claves-para-entender-el-escandalo-de-la-comunidad-del-anillo-de-la-policia/16513163

45 Las pruebas de las 'chuzadas' a periodistas sí existen. LA F.m. 18 de Diciembre de 2015 http://www.lafm.com.co/justicia/noticias/los-correos-an%C3%B3nimos-enviados-196561

46 Colombia's new spying scandal: Time for real change. Privacy International. 8 de Marzo de 2016. https://www.privacyinternational.org/node/800

47 Pedro Pablo Camargo's complaint of unconstitutionality against the second paragraph of article 2, the third paragraph of article 3 and the first section of article 5 of Legislative Act №.03 of 2002, "which reforms the National Constitution", sentence C-1092, Constitutional Court, November 19, 2003, available at:

http://www.corteconstitucional.gov.co/relatoria/2003/C-1092-03.htm

48 Alejandro Decastro González's complaint of partial unconstitutionality against article 14, 244 and 246 of Act 906 of 2004 "which draws up the Criminal Procedure Code", sentence C-336, Constitutional Court, May 9, 2007, available at: http://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

49 Idem.

50 Articles 235 and 237 of the Criminal Procedure Code. This time period of 36 hours is made up by 12 hours for the judicial police to inform the prosecutor that the order to intercept communications has been given, plus the 24 hours the prosecutor has to conduct the legality control before a criminal judge. See Gustavo Gallón et al. complaint of unconstitutionality against articles 14, 15 (partial) and 16 of Act 1142 of 2007, "which partially reform Acts 906 of 2004, 599 of 2000 and 600 of 2000 and adopt measures for the prevention and repression of criminal activity having a special impact on social coexistence and security," sentence C-131, Constitutional Court, February 24, 2009 —in which a study of constitutionality was carried out on article 237 of Act 906 of 2004— available at: http://www.corteconstitucional.gov.co/ RELATORIA/2009/C-131-09.htm

51 Dagoberto José Lavalle's complaint of partial unconstitutionality against article 52 of Act 1453 of 2011 "which reforms the Criminal Procedure Code, the Children's and Adolescents' Code, the rules on the extinction of property law and stipulates other measures in relation to security", sentence C-594, Constitutional Court, August 20, 2014, available at: http://www.corteconstitucional.gov.co/RELATORIA/2014/C-594-14.htm

52 Articles 236 and 237 of the Criminal Procedure Code.

53 According to article 213 of the Constitution, the state of internal disturbance is declared "in the case of a serious disruption of the public order imminently threatening the institutional stability and security of the State, or the peaceful coexistence of the citizenry—and which cannot be met by the use of ordinary powers of the police authorities".

54 This rule was endorsed by the Constitutional Court in the Constitutional Revision of the draft statutory bill No. 91/92 Senate and 166/92 House "which regulates the state of emergency in Colombia," sentence C-179, April 13 1994, available at: http://www.corteconstitucional.gov.co/relatoria/1994/C-179-94.htm

55 Act 1273 of 2009.

56 Taking up the definition contained in the collection of the United Nations Best Practices Section about intelligence and counterintelligence. Constitutionality revision of the statutory bill nº 263/11 Senate and 195/11 House, "which issues regulations to strengthen the legal framework that allows the organisms conducting intelligence and counterintelligence organisms to accomplish their constitutional and legal mission, and which lays down other provisions," sentence C-540, Constitutional Court, July 12, 2012, available at: http://www.corteconstitucional.gov.co/ relatoria/2012/c-540-12.htm

57 Idem.

58 Idem.

59 Tristán Donoso v. Panama, Inter-American Court of Human Rights (2009), paragraph 56 Escher v. Brazil Inter-American Court of Human Rights (2009), paragraph 116.

60 Myrna Mack Chang v. Guatemala, Series C Nº. 101, Inter-American Court of Human Rights, sentence on November 25, 2003, paragraph 284. Similarly, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Case nº 62540/00, European Court of Human Rights, sentence on June 28, 2007,

paragraph 77.

61 Decree 857 of 2014, which regulates the Statute Law 1621 of April 17, 2013, "which norms are issued to strengthen the legal framework to enable the government agencies that carry out intelligence and counterintelligence activities, meet its constitutional and legal mission, and see also, Article 1 Other provisions."

62 Sentence C-540, Constitutional Court, 2012.

63 Idem.

64 Privacy International, Shadow State: Surveillance, Law and Order in Colombia, August 2015, available at: https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf

65 Act 1341 of 2009.

66 Decree 1704 of 2012.

67 The use of the expression "or other competent authorities" has been temporarily suspended by the Council of State, which claimed that allowing authorities other than the Office of the Attorney General to have the power to request information from communications companies may infringe Act 1453 of 2011 and the Political Constitution. Council of the State - First section, filing number 11001-03-24-000-2013-00018-00, speaker Magistrate Guillermo Vargas Ayala, July 31, 2013.

68 Article 44 of Act 1621 of 2013.

69 International Principles on the Application of Human Rights to Communications Surveillance, 2013, available at: https://es.necessaryandproportionate.org/text, EFF, ARTICLE19, Background and Supporting International Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance, May 2014, available at: https://necessaryandproportionate.org/legalanalysis, Universal Implementation Guide for the International Principles on the Application of Human Rights To Communications Surveillance, 2015, available at: https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf

70 Article 37 of Act 1621 of 2013.

71 Sentence C-540, Constitutional Court, 2012.

72 The national government regulated the levels of classification of intelligence and counterintelligence information through decree 857 of 2014.

73 European Commission, Scientific Committee, Tecnical Definitions, Glossary, available at: http://ec.europa.eu/health/opinions/es/lamparas-bajo-consumo/glosario/def/espectro-electromagnetico.htm

74 El Tiempo, "Prosecutor says no to the interceptation system Puma of the Police", August 30, 2015, available at: http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092.

75 Article 5 of Act 1621 of 2013.

76 Article 17 of Act 1621 of 2013.

77 Article 31 of Act 1621 of 2013.

78 Articles 236 and 237 of the Criminal Procedure Code.

79 This directive compelled the States to ensure the retention of traffic and location data, as well as the necessary information for the identification of an individual, for a time period ranging from six months to two years. Directive 2006/24/EC of the European Parliament and the of the Council on March 15, 2006, available at: http://eur-lex.europa.eu/LexUri- Serv/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

80 Judgment in Joined Cases C - 293/12 and C - 594/12 Digital Rights Ireland and Seitlinger and Others, available at: http:// curia.europa.eu/juris/documents.jsf?num=C-293/12

81 Alejandro Decastro González's complaint of partial unconstitutionality against article 14, 244 and 246 of Act 906 of 2004 "which draws up the Criminal Procedure Code", sentence C-336, Constitutional Court, May 9, 2007, available at: http://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

82 Article 237 and 238 of Act 906 of 2004.

83 Act 1341 of 2009.

84 Bilateral Agreement between the government of the Republic of Colombia and the government of the French Republic on Internal Security Cooperation, signed on July 22, 2003. It has been in force since June 1, 2007, available at: http://apw.cancilleria.gov.co/tratados/SitePages/VerTratados.aspx?IDT=a9ce1083-1d7e-474d-b4df-3501f0bf1ed9

85 NATO-Colombian Cooperation Agreement on Security of Information, signed on June 25, 2013 and enacted through Act 1734 of September 8, 2014, available at: http://apw.cancilleria.gov.co/tratados/SitePages/VerTratados.aspx?IDT=d65b4217-9bd1-44eb-bbcb-b121ee78e8a9

86 Agreement on Operational and Strategic Co-operation between Colombia and the European Police Office, signed on February 17, 2014. It has been in force since February 25, 2014, available at: https://www.europol.europa.eu/content/agreement-operational-and-strategic-co-operation-between-colombia-and-european-police-office

87 Resolution A/RES/52/164 adopted by the United Nations Organization on December 15, 1997, to which Colombia adhered through Act 804 of 2003, available at: http://www.oas.org/juridico/mla/sp/per/sp_per_Con_inter_repr_aten_terro_come_bombas.pdf

88 Signed in Bogotá on July 19, 2008 and enacted by Act 1517 of 2012. [There is no link to the official version]

89 Act 1273 of 2009.

90 Annual Report of the Inter-American Commission on Human Rights2009, December, 2009, document OEA/Ser.L/V/II, Chapter IV, paragraph 137, available at: http://www.cidh.oas.org/annualrep/2009sp/cap.4Colo.09.sp.htm

91 Article 30 of Act 1621 of 2013 points out that "The National government shall initiate, within the year following the Commission's report, a filtering system on intelligence and counterintelligence data and records, using the recommendations report of the Commission as a guide."

92 Franky Urrego Ortiz's complaint of unconstitutionality against Act 1097 of 2006, sentence C-491, Constitutional Court, June 27, 2007, available at: http://www.corteconstitucional.gov.co/relatoria/2007/c-491-07.htm

93 Sentence C-540, Constitutional Court, 2012.

94 Comisión Colombiana de Juristas, Notion of constitutionality in the revision of the statutory bill 263 of 2011 Senate – 195 of 2011 House, available at: http://www.slideshare.net/Coljuristas/concepto-de-constitucionalidad-en-la-re-visin-del-proyecto-de-ley-estatutaria-263-de-2011-senado-195-de-2011-cmara