

International Principles on the Application of Human Rights to Communications Surveillance and the Inter-American System for the Protection of Human Rights

Juan Carlos Lara Valentina Hernández Katitza Rodríguez

August 2016





Table of Contents

Introduction
I. Legality
II. Legitimate Aim
III. Adequacy
IV. Necessity
V. Proportionality12
VI. Competent Judicial Authority16
VII. Due Process
VIII. User Notification
IX. Transparency
X. Public Oversight
XI. Integrity of Communications and Systems
XII. Safeguards for International Cooperation
XIII. Safeguards against Illegitimate Access and Right to Effective Remedy32
Recommendations

Introduction

The rapid development of digital communications technologies has given people around the world an unprecedented ability to share thoughts and ideas, organize activities—political or other—and communicate with loved ones across the globe more frequently than ever before. Yet these benefits all come with great challenges. As government surveillance capabilities continue to increase, so do threats and challenges to human rights.

Every time we use a phone, computer, or technological device, we leave behind vast amounts of personal information that can reveal our political and religious affiliations, medical conditions, sexual interests, and behavioral patterns. The same technological developments that we celebrate have given States new and efficient tools for collecting and analyzing rich data trails. States now have the ability to monitor, collect, store, and analyze our communications and interactions with our relatives, colleagues, and friends—often without precise legal limits or adequate guarantees to avoid abuses of power. The recent revelations that confirmed the broad State surveillance of digital communications, including mass surveillance, show the extent to which human rights are threatened in these situations.

There is thus an urgent need for States to pass up-to-date national surveillance laws and review their digital surveillance practices in order to guarantee compliance with international standards on human rights and the protection of privacy and fundamental freedoms in general.

These concerns inspired the writing of the International Principles on the Application of Human Rights to Communications Surveillance (hereinafter, "the 13 Principles" or "the Principles"), which set a framework for the application of international human rights law to communications surveillance in the digital age. The 13 Principles are firmly grounded in international human rights law and the decisions of international human rights courts that have interpreted such laws. This includes the case law of the Inter-American Court of Human Rights interpreting the American Convention on Human Rights. In some cases, the Principles attempt to fill the void that exists in international law.

The 13 Principles represent perhaps the most important step taken by civil society in articulating how States should comply with international standards on human rights when conducting communications surveillance in the digital age.

The ultimate aim of this analysis is to provide the Inter-American Human Rights System with a useful guide to the applicable international laws, and explanation of the relevant standards and the legal basis for those standards. This report provides an explanation of the

standards and their legal standing.

l. Legality

Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit human rights should be subject to periodic review by means of a participatory legislative or regulatory process.

The Principle of Legality requires that any restriction on fundamental rights be specifically authorized by law. Given the important role the rights of free expression, assembly, and association play in a democracy, a surveillance law must authorize government access to communications and personal information only under the most exceptional circumstances as defined by legislation. When national security is claimed as the reason for surveillance, the law must clearly specify the criteria to be used to determine when such surveillance is legitimate.

This Legality principle is recognized, in general terms, in Article 30 of the American Convention on Human Rights, which establishes the following:

Article 30. Scope of Restrictions. The restrictions that, pursuant to this Convention, may be placed on the enjoyment or exercise of the rights or freedoms recognized herein may not be applied except in accordance with laws enacted for reasons of general interest and in accordance with the purpose for which such restrictions have been established.

In interpreting Article 30, the Inter-American Court of Human Rights (I/A Court H.R.) defined the term "laws" as follows:

[T]he word "laws" in Article 30 of the Convention means a general legal norm tied to the general welfare, passed by democratically elected legislative bodies established by the Constitution, and formulated according to the procedures set forth by the constitutions of the States Parties for that purpose.¹

Article 30 thus sets forth an indispensable requirement that all interferences with human rights be authorized by law. The restrictions on rights must follow these terms:²

• The restriction must be explicitly authorized by the Convention and comply with

the particular conditions in which it was allowed;

- The aims of this restriction must be legitimate. That is to say, they must be ordered "for reasons of general interest" and may not deviate from "the purpose for which it has been established"; and
- Such restriction must be provided for by the laws and applied in compliance with them.

Thus the general terms and circumstances under which a restriction on a certain human right is authorized must be clearly established by law. And the law that establishes the restriction must be a law in the formal and material sense and in accordance with the restrictions that the Convention itself allows.

The central importance and rigor that the Inter-American system gives to the Principle of Legality in the context of state surveillance is seen in *Escher et al. v. Brazil*, which analyzes Article 11 of the American Convention on Human Rights, and refers to the international responsibility of the State of Brazil for violating the right to privacy by the interception, monitoring, and disclosure of telephone conversations of members of a public interest organization (*organizaciones sociales*) by the Military Police of the state of Paraná. In that case, the Court emphasized several components of legality including the legal rules of appropriateness, competence, and procedure. The Court held that because these requirements were not met, it did not even have to consider other vital principles such as the purpose and necessity of the interception. The American Convention and its interpretation by the Court demand a law in both the material and the formal sense. Similarly, the joint declaration of the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the *Inter-American Commission of Human Rights (IACHR)* Special Rapporteur for Freedom of Expression indicates that:

States must guarantee that the interception, collection and use of personal information, including all limitations on the right of the affected person to access this information, be clearly authorized by law in order to protect them from arbitrary or abusive interference with their private interests. The law must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged.

Two additional issues arise from the Principle of Legality. The first is related to the access people have to the legislation that regulates the right to privacy, and the second is related to its updating.

According to the 13 Principles, not only do we need legislation on the right to privacy, but

such surveillance legislation must be available to individuals to review and comment upon by means of a participatory legislative or regulatory process that accurately reflects the protection of their interests regarding the respect and guarantee of their human rights.

Moreover, as stated by the UN Special Rapporteur on the Promotion and Protection of Freedom of Opinion and of Expression, the legislative proposals for the revision and adoption of restrictions on individual online security "must be subject to public discussion and adopted in line with the ordinary, public, reported, and transparent legislative procedure. States must promote such discussion and procedures, as well as the effective involvement of a wide variety of actors belonging to the civil society and minority groups, and they must avoid the adoption of such legislation by virtue of accelerated legislative procedures."⁴

It is also necessary to update legislation authorizing restrictions on the right to privacy so it is applicable to our current digital age and in accordance with technological developments. This is especially important because of the obsolescence of legal surveillance framework, and because the State may have few if any clearly-stated boundaries for invading peoples' fundamental freedom.

Finally, the Principle of Legality is also crucial in relation to the surveillance capabilities granted to criminal prosecutors and investigators. Given that a person under investigation is usually unaware of the measures used to track their activities, it is especially important that the laws that enable these measures be well-written, publicly accessible, and understandable. In fact, the Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression, by the Special Rapporteurs for Freedom of Expression belonging to the UN and the *Inter-American Commission of Human Rights (IACHR)*, suggested that States disseminate, at least, "information on the regulatory framework of surveillance programs; on the bodies in charge of implementing and overseeing such programs; on the procedures of authorization, selection of aims and data management..."

II. Legitimate Aim

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

The 13 Principles refer to legitimate aim in two ways: first, as the objective in a positive way, proposing that laws permit communication surveillance to a stated legitimate aim; and second, as the objective in a negative way, rejecting discrimination as a factor for which surveillance could be conducted.

In the first sense, it is necessary that communications surveillance be conducted only "to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society." *Article 30* of the American Convention similarly establishes that the restrictions on the rights recognized therein "may not be applied except in accordance with laws enacted for reasons of general interest and in accordance with the purpose for which such restrictions have been established." Moreover, *Article 32.2* of that document establishes that:

The rights of each person are limited by the rights of others, by the security of all, and by the just demands of the general welfare, in a democratic society.

On the scope of this article, the Court has stated that:

29. The requirement that the laws be enacted for reasons of general interest means they must have been adopted for the "general welfare" (article 32.2 [of the American Convention]), a concept that must be interpreted as an integral element of public order in democratic states, the main purpose of which is "the protection of the essential rights of man and the creation of circumstances that will permit him to achieve spiritual and material progress and attain happiness" (American Declaration of the Rights and Duties of Man).⁶

The Inter-American Court of Human Rights (I/A Court H.R.) has elaborated on these articles to emphasize that a generalized assertion of the public good is not a sufficient

specific legitimate aim:

"[P]ublic order" or "general welfare" may under no circumstances be invoked as a means of denying a right guaranteed by the Convention or to impair or deprive it of its true content. (See Art. 29(a) of the Convention). Those concepts, when they are invoked as a ground for limiting human rights, must be subjected to an interpretation that is strictly limited to the "just demands" of "a democratic society," which takes account of the need to balance the competing interests involved and the need to preserve the object and purpose of the Convention.⁷

In accordance with this case law, the 13 Principles require specificity and exclude concepts that are too vague—such as the concept of "national security"—from the justifications used to restrict the right to privacy.

Legitimate aims for the interference with fundamental rights are typically linked to a corresponding specific right in the Convention, for example, the freedom to manifest religion and beliefs (Article 12.3 of the Convention); freedom of thought and expression (Article 13.2 of the Convention); freedom of association (Article 16.2 of the Convention); private property (Article 21.1 of the Convention); the exercise of freedom of movement and residence (Article 22.3 of the Convention), and political rights (Article 23.2 of the Convention).

In contrast, the legitimate aims asserted to justify surveillance are typically for the protection of national security, public order, and public health, among others. The American Convention does not mention these types for the restrictions on the right to privacy, but in any case, it is clear that the general rules provided in the above-mentioned Articles 30 and 32 of the Convention also apply to the right to privacy.

Furthermore, the 13 Principles establish that communications surveillance "must not be applied in a manner that discriminates on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." This means that privacy protections do not discriminate on the basis of the personal status of the persons who may be affected by the surveillance measure. This is a logical conclusion from the equivalent non-discrimination protection of human rights recognized in international treaties, provided for in Articles 1.1 (on the protection or guarantee of a conventional law) and 24 (on the equal protection of the internal law or its application) of the American Convention. Moreover, this prohibition of discrimination is recognized in the Inter-American Convention against all forms of discrimination and intolerance. It includes principles on non-discrimination, meaning no distinction, exclusion, restriction, or preference, in any realm of public or private life. Lastly, in cases where there is a suspension of guarantees due to threats to the independence or security of the States, Article 27 of the

American Convention makes clear that such restrictions do not involve discrimination on the grounds of race, color, sex, language, religion, or social origin. In other words, even in cases where there is a state of emergency, States cannot restrict rights in a discriminatory manner.

III. Adequacy

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

State communications surveillance practices must be "appropriate to fulfill the specific legitimate aim identified." The Court's interpretation of Article II.2 of the American Convention, as explained above, accounts for the same idea: restrictions must be adequate, that is,9 they should be appropriate in order to fulfill their function of protecting other rights.¹⁰

In the Inter-American system, the Inter-American Court of Human Rights (I/A Court H.R.) has specifically taken a stance regarding Adequacy in relation to the right to freedom of expression, understanding it as the capacity "to help achieve" the goal of safeguarding a legal right." Thus, the Principle of Adequacy requires that a measure interfering with the right to private life must be able to help achieve the pursued legitimate aim, such as helping in a criminal or national security investigation.

IV. Necessity

Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.

According to the Principle of Necessity, even when there is a legitimate aim according to the terms of the second principle, the State must explain and prove that the communications surveillance is necessary to achieve that aim.

Article 11.2 of the American Convention on Human Rights, affirms the Principle of Necessity:

The right to privacy is not an absolute one, and, so, it may be restricted by the States provided that their interference is not abusive or arbitrary; accordingly, such restriction must be statutorily enacted, serve a legitimate purpose, and meet the requirements of suitability, necessity, and proportionality which render it necessary in a democratic society.¹²

The I/A Court H.R., interpreting Article 11.2, explicitly recognized the Principle of Necessity in *Chaparro Álvarez and Lapo Íñiguez v. Ecuador* (2007), the I/A Court H.R. held:

(...) it is not sufficient that every reason for deprivation or restriction of the right to liberty is established by law; this law and its application must respect the requirements listed below, to ensure that this measure is not arbitrary: i) that the purpose of the measures that deprive or restrict liberty is compatible with the Convention. It is worth indicating that the Court has recognized that ensuring that the accused does not prevent the proceedings from being conducted or evade the judicial system is a legitimate purpose; ii) that the measures adopted are appropriate to achieve the purpose sought; iii) that they are necessary, in the sense that they are absolutely essential to achieve the purpose sought and that, among all possible measures, there is no less burdensome one in relation to the right involved, that would be as suitable to achieve the proposed objective. Hence, the Court has indicated that the right to personal liberty supposes that any limitation of this right

must be exceptional, and (iv) that the measures are strictly proportionate, so that the sacrifice inherent in the restriction of the right to liberty is not exaggerated or excessive compared to the advantages obtained from this restriction and the achievement of the purpose sought.¹³

According to the Court, a measure is "necessary" when there is no other applicable measure that is less onerous for individuals' privacy that could be used to achieve the pursued aim.

V. Proportionality

Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

- 1. There is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and;
- 2. There is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought, and;
- 3. Other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option, and;
- 4. Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged; and
- 5. Any excess information collected will not be retained, but instead will be promptly destroyed or returned; and
- 6. Information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given; and
- 7. That the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

The Principle of Proportionality requires weighing the legal right that serves as the legitimate aim against the restriction of the affected right. According to this Principle, there must be a proportionate relationship between the appropriateness and the scope of

communications surveillance and the interest of the fundamental freedoms of those affected, even in the cases that go beyond the collection of information (for instance, in the information exchange of state organisms.) The 13 Principles list a series of criteria that are useful for weighing communications surveillance and the protection of individuals' rights, such as: the probability of the commission of a serious crime, the probability of obtaining evidence through surveillance, the lack or uselessness of less invasive measures, the limitations of the object of surveillance, the disposal of unnecessary information, its access and use by the competent specific authority, and the protection of the essence of fundamental rights.

The I/A Court H.R. has stated that the restriction on a right recognized in the Convention must be proportional: indeed, the analysis has been called the "proportionality test." In *Kimel v. Argentina* (2008), the I/A Court H.R. explained the test as follows:

83. In this last step of the examination, it is discussed whether the restriction is strictly proportionate, in a manner such that the sacrifice inherent therein is not exaggerated or disproportionate in relation to the advantages obtained from the adoption of such limitation.¹⁴

The Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism explains the Principle of Proportionality in connection with the rights to privacy and honor (provided for in Article 17 of the International Covenant on Civil and Political Rights), stating that such principle stipulates that the restriction must be "the least disturbing tool for the achievement of the desired outcome and must be proportionate in relation to the interest it tries to protect."¹⁵

Proportionality is consistently used by courts as a measure for controlling state powers. Elaborating on its content and quoting the European case law, the I/A Court H.R. has discussed proportionality in close relation to the requisites of Necessity and Adequacy. In an advisory opinion, the Court explained:

If there are various options to achieve this [legitimate] objective, that which least restricts the right protected must be selected. Given this standard, it is not enough to demonstrate, for example, that a law performs a useful or desirable purpose; to be compatible with the Convention, the restrictions must be justified by reference to governmental objectives which, because of their importance, clearly outweigh the social need for the full enjoyment of the right Article 13 guarantees. That is, the restriction must be proportionate and closely tailored to the accomplishment of the legitimate governmental objective necessitating it.¹⁶

VI. Competent Judicial Authority

Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must:

- *I.* be separate and independent from the authorities conducting Communications Surveillance;
- 2. be conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and
- 3. have adequate resources in exercising the functions assigned to them.

The 13 Principles require that a qualified, impartial, independent and competent judicial authority must adjudicate the appropriateness of communications surveillance actions.

The authorities supporting the Inter-American system require the same. Article 8.1 of the American Convention establishes:

Every person has the right to a hearing (...) by a competent, independent, and impartial tribunal, previously established by law, in the substantiation of any accusation of a criminal nature made against him or for the determination of his rights and obligations of a civil, labor, fiscal, or any other nature.

The Inter-American Court of Human Rights has interpreted this right in a general sense. Thus, Article 8 "does not establish the right to a remedy," pursuant to Article 25 of the Convention, but the right of access to justice, and the way in which justice is made, by independent and impartial judicial authorities, for both judgment and the delineation of every right and obligation.

As stated by the Court:

States have the responsibility to embody in their legislation and ensure due application of effective remedies and guarantees of due process of law before the competent authorities, which protect all persons subject to their jurisdiction from acts that violate their fundamental rights or which lead to the determination of the latter's rights and obligations.¹⁷

The Inter-American Court has further elaborated on the requirement that the judiciary be independent, explaining that the State has an obligation to preserve judicial independence in two ways: "in its institutional aspect, that is, regarding the Judiciary as a system, as well as in connection with its individual aspect, that is to say, concerning the person of the specific judge."¹⁸

On impartiality, the Inter-American Court has considered the case law of the European Court of Human Rights and requires as follows:

The judge acting in a specific dispute approach the facts of the case subjectively free of all prejudice and also offer sufficient objective guarantees to exclude any doubt the parties or the community might entertain as to his or her lack of impartiality.

In addition:

The judge must appear as acting without being subject to any influence, inducement, pressure, threat or interference, direct or indirect, and only and exclusively in accordance with—and on the basis of—the Law.¹⁹

Two aspects of the 13 Principles strengthen these guarantees. The first requires a judicial authority in the even absence of active litigation—for example, the requirement that a judge approve all surveillance requests, including search warrants. The I/A Court H.R. has supported this interpretation as well. In *Escher v. Brazil*, the Court considered the interception of telephone communications conducted by the military police and expressed that "the grounds and justification must show that all the legal requirements and other elements that justify granting or refusing the measure have been taken into consideration."²⁰

As the commentators Blanco and Salmón (2012)²¹ explain, the I/A Court H.R. here clarified this rule in a way it had failed to in the past. In previous cases, the Court had claimed that:

The justification of a judgment must prove that the parties have been heard and their allegations taken into account. Even though this is not possible in a procedure with no hearing of the parties, this does not exonerate the authority from the obligation to justify. On the contrary, it is compelled to conduct a strict assessment of the compliance or noncompliance with the legal provisions in order to grant the authorization to carry out the measure.²²

Competent Judicial Authority is required to authorize intrusive surveillance measures that affect fundamental rights. Such oversight is required not only for criminal procedures, but for all procedures as stipulated in Article 8.1 of the American Convention of Human Rights, and at any of the stages in the procedure, whether during pre-trial arrangements, the trial process, or the execution of the judgment. Such oversight must be present even in the

investigation leading up to a trial. Indeed, judges must intervene and justify all decisions that infringe upon an individual's rights.

Competent Judicial Authority is especially necessary for mass surveillance, given the corresponding negative effects it has on fundamental rights.

The 13 Principles also require a level of expertise in order to make decisions in matters of communications surveillance. Judges must be "conversant with both the relevant technologies and human rights principles so that they properly understand the nature of each surveillance request, and are able to assess its likely impact on individual privacy."²³

VII. Due Process

Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

The legitimacy of communications surveillance also depends on the compliance with specific rules of due process, including safeguards related to procedure and a competent court. Hence, it mirrors the provisions of Article 8 of the American Convention on Human Rights. The Principle of Due Process coincides with the previous principle, related to the participation of an independent and impartial judicial authority. Thus, the judicial authorization allowing a communications surveillance measure is not enough for it to be legitimate; it also needs to be immersed in the framework of a process that establishes certain minimum safeguards for individuals.

Due Process must be followed except in the rare case of emergency when there is an "imminent risk of danger to human life" such that the urgency of the situation does not allow for a fair and pubic hearing to be carried out. In all other cases, the principle prevents States from bypassing a fair and public hearing.

In this way, the Due Process Principle is different from the general cessation of rights permitted during states of emergency, provided for in Article 27 of the American Convention. It also varies from the possibility of closed proceedings that Article 8.1 of the American Convention provides for with respect to certain criminal processes. The 13 Principles support emergency measures, but limit them to very specific legitimate aims, like when there is an "imminent risk of danger to human life," but not when, say, they are needed for "national security," which is ambiguous.

Moreover, the 13 Principles establish their own safeguards in emergency situations, for instance: retroactive judicial authorization must be sought within a reasonably practicable

time period. The 13 Principles make clear that flight risks or destruction of evidence are not enough to justify retroactive authorization in emergency situations.

This requirement mirrors the provisions of Article 8 of the American Convention on Human Rights that states the right of every person to a hearing, with due guarantees and within a reasonable time, by a competent, independent, and impartial tribunal, previously established by law.

VIII. User Notification

Those whose communications are being surveilled should be notified of a decision authorizing Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstance:

- I. Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorized, or there is an imminent risk of danger to human life; and
- 2. Authorization to delay notification is granted by a Competent Judicial Authority; and
- 3. The User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.

The obligation to give notice rests with the State, but communications service providers should also be able to notify individuals, voluntarily or upon request.

The Principle of User Notification plays a central role in the fight against abusive state surveillance and strategic litigation.

Now, States have tools that allow for remote access to files and equipment belonging to individuals who are under investigation, which makes it impossible for them to be aware of the surveillance activities that the State is conducting on them. Such surveillance is troublesome, not only because it's a serious violation of the right to privacy and it has harmful consequences that threaten the right to freedom of expression, but also because it directly affects the right to due process, since affected parties are unable to resort to a judicial authority to plead the legality of the measure.

In *Castillo Petruzzi v. Peru* (1999), the I/A Court H.R. drew attention to the measures that could be used to achieve security objectives and combat crime, establishing that the end does not always justify the means:

As this Court has pointed out, there can be no doubt that the State has the right and the duty to guarantee its own security. Nor is there any question that violations of the law occur in every society. But no matter how terrible

certain actions may be and regardless of how guilty those in custody on suspicion of having committed certain crimes may be, the State does not have a license to exercise unbridled power or to use any means to achieve its ends, without regard for law or morals. The primacy of human rights is widely recognized. It is a primacy that the State can neither ignore nor abridge.²⁴

In the digital age, documents and communications are kept in digital form—often stored in the cloud or otherwise in the custody of others. Internet and telephone service providers are now key players when it comes to communications surveillance, since they control the transmittal and storage of communications for the majority of the population. They often know the identity of a person creating a website, or that of someone posting messages on a social media platform. Whenever a State wishes to know the identity of an Internet user, it submits a request to the intermediary company. The only way an affected person can challenge a State's request for access to data is if they have been notified by the intermediary or the government.

In this regard, the User Notification Principle requires that the subject being surveilled be provided with the necessary notice and information about the authorization of the surveillance measure so that they can challenge it or seek other effective remedies. And such notification must be provided with enough time and information to challenge the surveillance.

Two aspects are emphasized in this principle. The first involves the right to know about the restriction on the right to privacy. The 13 Principles specify the circumstance in which such notification might be delayed—but never bypassed: when the notification poses a serious risk to the success of the aim for which surveillance was required. In all cases, notification must be delivered as soon as the risk disappears.

A competent judicial authority must approve any delay to notification. This safeguard guarantees that any delay is justified and not extended for longer than strictly necessary to protect an investigation or to protect those who face imminent risk to their lives. The affected must also have access to the material supporting the request for a surveillance authorization.

The obligation to notify is embodied in Article 7.4 of the American Convention, with the purpose of making information available and allowing for the possibility of a challenge to restrictions on personal freedom. Regarding criminal convictions, the Inter-American Court has stated that the lack of notification "constitutes, *per se*, a violation of Article 8 of the Convention" and it places the affected "in a situation of legal uncertainty and ma[kes] the exercise of the right to appeal a judgment impracticable." The same criteria should be applied to other judicial decisions that affect fundamental rights, especially when their effect

is unknown to the affected.

In addition to Article 7.4, the right to judicial protection set forth in Article 25 of the American Convention stipulates that everyone has the right to simple and prompt recourse—or any other effective recourse—from a competent court to protect against acts that violate fundamental rights recognized by the constitution or laws or by the Convention, even if such violations are committed by persons acting within the boundaries of their official duties. The I/A Court H.R. has understood effective remedies as in the case of *Mejia Idrovo v. Ecuador*, 2011:²⁶

As for the effectiveness of the remedy, the Court has established that for such an effective remedy to exist, it is not enough that it be provided by the Constitution or by law or that it be formally recognized, but rather it must be truly effective in establishing whether there has been a violation of human rights and in providing redress. A remedy that proves illusory because of the general conditions prevailing in the country, or even in the particular circumstances of a given case, cannot be considered effective. ²⁷

The Court also reiterated in *Ivcher Bronstein v. Perú*, 2001 what constitutes an effective remedy:²⁸

The inexistent of an effective recourse against the violation of the rights recognized by the Convention constitutes a transgression of the Convention by the State Party in which such a situation occurs. In that respect, it should be emphasized that, for such a recourse to exist, it is not enough that it is established in the Constitution or in the law or that it should be formally admissible, but it must be truly appropriate to establish whether there has been a violation of human rights and to provide everything necessary to remedy it. Those recourses that are illusory, owing to the general conditions in the country or to the particular circumstances of a specific case, shall not be considered effective.²⁹

Moreover, States must not only ensure that any person claiming such remedy have his rights determined by a competent authority, but also that they are granted the possibility of judicial remedy—ensuring that competent authorities enforce such remedies when granted. As previously stated, because state surveillance is often shrouded in secrecy, the judge's involvement is of great importance.

The User Notification Principle also obliges the State to notify the user and to not block the intermediary's ability to do so itself, either voluntarily or upon request.

The 2011 report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and other Business Enterprises, established

guiding principles on business and human rights. The report emphasizes that such principles aim to create a dynamic, interrelated system between the preventive and remedial measures by which the State protects these rights, make companies responsible for respecting human rights, and finally, give access to avenues of redress, since it is impossible to avoid all abuses. The Special Representative specifies that the general principles he sets forth are based on—among other aspects—"the role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights." The report was recognized by the OAS in its 2014 resolution on the promotion and protection of human rights in business. The resolution recognizes the importance of continuing to promote the application of the UN Guiding Principles on Business and Human Rights and highlights the importance of making progress on this issue, encouraging States to take this into account when necessary.

Technology and telecommunications companies play a crucial role when it comes to noticing when their users' private communications are at risk of being intercepted. These companies—as well as the State and the people—have an obligation to respect fundamental rights, especially when, due to the typical characteristics of their services, they are the only ones able to detect an infringement and stop undue intrusions. Relatedly, Principle 13.b of the Guiding Principles on Business and Human Rights establishes that:

The responsibility to respect human rights requires that business enterprises:

b) Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.³³

The Special Representative, on the meaning and scope of this provision, specified that:

Business enterprises may be involved with adverse human rights impacts either through their own activities or as a result of their business relationships with other parties. Guiding Principle 19 elaborates further on the implications for how business enterprises should address these situations. For the purpose of these Guiding Principles a business enterprise's "activities" are understood to include both actions and omissions; and its "business relationships" are understood to include relationships with business partners, entities in its value chain, and any other non-State or State entity directly linked to its business operations, products or services. 34

Specifically, Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes adopted by the European Commission Group of Data Protection points out its agreement with the bill presented by the European

Council and Parliament on the law on data protection, which requires companies to notify individuals when a public authority has been granted access to their data over the past twelve months, which, according to the Working Party, will enhance the trust of the population.³⁵

IX. Transparency

States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each.

States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting Communications Surveillance. States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance.

The Principle of Transparency demands that the rules and application of state communications surveillance activities be publicly available and updated periodically with detailed reports. Moreover, the Transparency Principle requires that States not interfere with the information delivered to users by communications service providers. This way, the general public shall be able to assess the content and application of the laws regulating surveillance and the ones guaranteeing the rights affected by it.

This principle is based on the right of access to information, recognized in Article 13.1 of the American Convention.

Even though the right to search for, receive, and disseminate information is included in the right to freedom of expression, the right to public information has been developed separately and independently by the case law of the Inter-American Court of Human Rights, which made the Court the first international court to specifically refer to information as an autonomous human right, guaranteed by convention. In this regard, the I/A Court H.R. has explained:

[B]y expressly stipulating the right to "seek" and "receive" "information," Article 13 of the Convention protects the right of all individuals to request access to State-held information, with the exceptions permitted by the restrictions established in the Convention. Consequently, this article protects the right of the individual to receive such information and the

positive obligation of the State to provide it, so that the individual may have access to such information or receive an answer that includes a justification when, for any reason permitted by the Convention, the State is allowed to restrict access to the information in a specific case. The information should be provided without the need to prove direct interest or personal involvement in order to obtain it, except in cases in which a legitimate restriction is applied. The delivery of information to an individual can, in turn, permit it to circulate in society, so that the latter can become acquainted with it, have access to it, and assess it. ³⁶

It is necessary to highlight the "positive obligation of the State" to provide information. The State is not merely required to respond to information requests, it must provide information *ex officio*. In this regard, the Court stated that "in a democratic society, it is essential that State authorities are governed by the principle of maximum disclosure, which establishes the presumption that all information is accessible, subject to a limited system of exceptions." Thus, the Inter-American Court echoes the 2004 joint declaration by the rapporteurs on freedom of expression of the UN, the OAS, and the OSCE, in which they stipulated that "[p]ublic authorities should be required to publish pro-actively, even in the absence of a request, a range of information of public interest. Systems should be put in place to increase, over time, the amount of information subject to such routine disclosure." 38

Transparency in the form of the right to information plays an important role in a democracy. This role was acknowledged in 2012 by the Inter-American Commission on Human Rights in its report "The Inter-American Legal Framework regarding the Right to Access to Information." It stated that the right to access to public information provides the public with what they need in order to actively participate in a democratic society. Furthermore, this right is especially crucial since such information helps protect fundamental rights and prevent abuses by States. The framework adds that public information is a tool that gives civil society the power to fight corruption and secrecy.³⁹

The Inter-American System's view on the right to access to public information fully applies to communications surveillance. In fact, as we have already stated, States must publish all the information of public interest, including communications surveillance, since such transparency allows people to know how these highly invasive mechanisms work and how they affect fundamental rights. Such information is key, not only to learn about the ways in which people can defend themselves from such intrusions, but also to become aware of the circumstances under which their rights are violated and, thus, be able to seek remedies to put an end to those situations.

In this regard, the UN and OAS special rapporteurs, in their joint declaration, asserted that legal norms should guarantee that people are able to access information about surveillance programs, their scope, and the existing oversight mechanisms that are currently in place.

The rapporteurs establish the State's obligation to disseminate the procedures surrounding the authorization of surveillance measures, the selection of objectives, data management and information about the use of surveillance techniques, including their scope. The rapporteurs also indicate that the State must allow service providers to inform their users about the surveillance procedures that are implemented, and provide, at least, aggregated information about the number and scope of requests that they receive. Finally, they compel States to widely disseminate information about illegal surveillance programs.⁴⁰ Information regarding surveillance shall not be classified confidential or reserved *a priori*, before it occurs. Every classification of information must comply with the proof of harm test as stipulated in *Claude-Reyes et al. v. Chile*,⁴¹ which explained:

58 (c) "According to the broad terms of Article 13, the right of access to information should be governed by the 'principle of maximum disclosure." "The burden of proof corresponds to the State, which must demonstrate that restrictions to access to information are compatible with the inter-America provisions on freedom of expression." "This means that the restriction must not only be related to one of the [legitimate] objectives [that justify it], but it must also be shown that disclosure could cause substantial prejudice to this objective and that the prejudice to the objective is greater than the public interest in having the information." (Evidence of proportionality.)

Moreover, when classifying information as confidential, it must be demonstrated that there is a probable harm that would affect the general interest; consequently, it would be necessary to explain the reasons why this information has not been disclosed. In addition, the possible harm that would affect the general interest must be greater than the public's right to know for "reasons of public interest." Only in this way, could we distinguish between confidentiality based on political criteria versus confidentiality based on matters of public interest. This will ensure the right to access to information is respected.

X. Public Oversight

States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance. Oversight mechanisms should have the authority: to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been comprehensively and accurately publishing information about the use and scope of Communications Surveillance techniques and powers in accordance with its Transparency obligations; to publish periodic reports and other information relevant to Communications Surveillance; and to make public determinations as to the lawfulness of those actions, including the extent to which they comply with these Principles. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

In a democracy, it is important that public officials who have been given the power to conduct communications surveillance are subject to effective oversight to ensure that their capabilities are used legitimately and non-arbitrarily, and to hold them accountable to the general public.⁴²

In a 2006 study on the right to access to information, the Office of the Special Rapporteur on Freedom of Expression from the Inter-American Commission on Human Rights referenced the legitimate limits that can be used as arguments in order to delineate the right to access to public information. The Commission recognized the right to information in accordance with Article 13.1 of the American Convention on freedom of thought and opinion, and maintained that the rights or reputations of others—including national security, public order, and public health or morals—are limits to such a right in accordance with Article 13.2.⁴³

"The Johannesburg Principles on National Security, Freedom of Expression and Access to Information" are cited as a basis for this right. Principles 11 and 12 establish both the general rules on access to information and the interpretation of national security as an exception to access to information. They state that "everyone has the right to obtain information from public authorities, including information relating to national security," and that "the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest," but it may not deny

access to information, unless it designates in the legislation the specific categories of information that are necessary to protect a legitimate national security interest.⁴⁴

With regard to this limitation based on national security, the Office of the Special Rapporteur on Freedom of Expression claimed that:

Any restrictions on the grounds of national security will be only be valid when orientated to protect the territorial integrity of the country and in the exceptional circumstances of extreme violence that threatens the imminent collapse of the democratic order. Any restrictions based on grounds of national security are not legitimate if their purpose is to protect the government's interests rather than those of society as a whole.⁴⁵

As seen, both the Inter-American Court of Human Rights through its Office of the Special Rapporteur on Freedom of Expression, and the Johannesburg Principles establish the so-called principle of maximum disclosure, which, according to Ferreyra (2013), "establishes the assumption that all information is accessible, subject to a limited system of exceptions." ⁴⁶

The Inter-American Court has also referenced the exceptions to the general principle of maximum disclosure, reflected in the opinion of the Inter-American Commission on Human Rights in the sense that "when a punishable fact is being investigated, the decision to classify the information as secret and to refuse to submit it can never depend exclusively on a State body whose members are deemed responsible for committing the illegal act."

The 2004 Joint Declaration referring to the international mechanisms for promoting freedom of expression by the UN Special Rapporteur on Freedom of Opinion and Expression, the Representative of the Organization for Security and Co-operation in Europe, and the OAS Special Rapporteur on Freedom of Expression states that it is not enough to simply recognize the right to access to public information; national authorities must take active measures to overcome the culture of secrecy by implementing, for example, punishments, campaigns related to public information and awareness, and the necessary resources and assistance to successfully implement this type of legislation.⁴⁸

The Principle of Public Oversight mirrors what is established by the bodies of the system, especially by the Inter-American Commission on the importance of properly functioning oversight mechanisms.⁴⁹

XI.

Integrity of Communications and Systems

In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes. 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.⁵⁰

The Principle of Integrity imposes three negative obligations on the State. First, it prohibits States from forcing software or hardware service providers to design or create communication technologies that have surveillance capabilities. Second, it prohibits States from requiring service providers to collect user data. Third, it prohibits States from imposing restrictions on anonymity.

Aside from the enshrinement of the right to privacy, international treaties make no reference to the aforementioned obligations. Notwithstanding, the Principles and the opinion of the UN Special Rapporteur on Freedom of Expression are fully aligned, maintaining that:

"States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption.⁵¹

Both the Office of the Special Rapporteur for Freedom of Expression from the Inter-American Commission on Human Rights and the UN Special Rapporteur for Freedom of Opinion and Expression emphasize the importance of anonymity. The Inter-American System highlights that anonymity is one of the two minimum concrete policies linked to the exercise of the right to freedom of expression online (the other protection is that of personal data)⁵² and Special Rapporteur Kaye states that "[a]nonymity (and encryption), today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity,

activists, scholars, artists and others to exercise the rights to freedom of opinion and expression."53

XII.

Safeguards for International Cooperation

In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service providers and States. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one State could apply to Communications Surveillance, the available standard with the higher level of protection for individuals is applied.

Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for Protected Information to circumvent domestic legal restrictions on Communications Surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

The 13 Principles require that whichever standard guarantees the highest level of protection for individuals is applied when there is cooperation among multiple countries. They also demand the respect for the principle of dual criminality (that a persons' actions constitute an offense in both the requesting and requested States) for being able to use surveillance capabilities in investigations involving more than one State. Furthermore, they indicate that mutual legal assistance cannot be used to circumvent domestic restrictions (for instance, when an intelligence agency receives information from a foreign entity and not from its own surveillance). The Principles of Public Transparency and Due Process also apply to mutual assistance.

In the Inter-American system, the treaty on mutual legal assistance in criminal matters among the members of the OAS is in full force, in compliance with Article 2.(e) of the American Convention. The Principles establish new standards for cooperation, requesting a higher level of protection than the existing one.

XIII.

Safeguards against Illegitimate Access and Right to Effective Remedy

States should enact legislation criminalising illegal Communications Surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.

This last principle demands criminal and civil punishment against illegal communications surveillance, both for the State and for private actors; it also requires redress mechanisms. This principle is found in Article 8 of the Universal Declaration of Human Rights, Article 2.3 of the International Covenant on Civil and Political Rights, Article XVIII of the American Declaration of Human Rights, and Article 25 of the American Convention on Human Rights. This last provision provides as follow:

Everyone has the right to simple and prompt recourse, or any other effective recourse, to a competent court or tribunal for protection against acts that violate his fundamental rights recognized by the constitution or laws or by this Convention, even though such violation may have been committed by persons acting in the course of their official duties.

This provision reiterates the State's duty to provide appropriate effective remedies. The Principles go beyond that, explicitly establishing the appropriateness of criminal and civil sanctions.

In the Inter-American system, the State's obligation to provide sanctions and remedial measures is not subject to the existence of remedies exercised by the possible affected individuals. To the Inter-American Court, "States must prevent, investigate and punish any violation of the rights recognized by the Convention and, moreover, if possible, attempt to restore the right violated and provide compensation as warranted for damages resulting from the violation."⁵⁴

The 13 Principles demand the protection of whistleblowers so that the revelation of illegal acts is not subject to punishment. This protection lies in the right to browse, receive, and disseminate information, recognized in Article 19 of the UDHR, in Article 19.2 of the ICCPR, and in Article 13.1 of the American Convention. This protection is based on an act of warning, relative to issues of public interest, which involves the right to freedom of expression. Several special rapporteurs in international organizations have called for the protection of whistleblowers. Specifically, in terms of treaties, Article 33 of the UN Convention against Corruption gives States the following option:

Each State Party shall consider incorporating into its domestic legal system appropriate measures to provide protection against any unjustified treatment for any person who reports in good faith and on reasonable grounds to the competent authorities any facts concerning offenses established in accordance with this Convention.

The 13 Principles also require that the information obtained in breach of the principles be unacceptable as direct or indirect evidence against those affected, since such evidence would have been obtained without regard for the right to privacy. In this respect, the 13 Principles cover aspects of due process elaborated as rules in national legislations underlying due process as described above. They also demand the return or destruction of the material obtained through communications surveillance once it has been used, taking also into account the existing rules for the cancellation and elimination of personal data. The Principles raise such rules to the standard of a fundamental right that may be affected by the collection, preservation, or processing of that information.

Recommendations

We request that the Inter-American Commission of Human Rights study the application of human rights to communications surveillance. To that end, the Principles are a useful guide.

In particular, we recommend that the IACHR report explore the following topics of interest:

- The right to privacy as a universal right, whose enjoyment does not depend on the nationality or location of the individual, nor may it be recognized and protected in a discriminatory manner.
- The explicit acknowledgment that any communications surveillance act—including the collection, monitoring, interception, control, retention, acquisition, or seizure of communications—represents an interference with fundamental freedoms, which must be justified in compliance with international human rights law. Therefore, all permitted limitations must comply—at least—with the Principles of Legality, Legitimate Aim, Adequacy, Necessity and Proportionality, Due Process.
- The acknowledgment of States' obligation to respect and guarantee human rights, ensuring that the legal procedures guiding the interferences with fundamental freedoms are properly provided for by law, consistently implemented and available to the general public, in alignment with the restrictions allowed by the Convention.
- The acknowledgment that mass surveillance (or "mass collection of information")
 involving a priori retention or collection of data from a significant (or particularly
 vulnerable) subset of the population is an inherently disproportionate interference
 with human rights.
- The need to make the use and scope of communications surveillance laws more transparent, and to include their regulations, activities and the authorities authorized to conduct surveillance.
- The necessity of notice to those affected by any surveillance, as well as the opportunity for due process and redress for improper surveillance.
- The need to establish independent oversight mechanisms in order to guarantee transparency and accountability in communications surveillance.
- The need for the State to provide whistleblowers with enough protection when they reveal violations of human rights, and also provide those affected by communications surveillance with remedial means.

- The reaffirmation that the decisions related to communications surveillance must be made by an impartial, independent, and competent judicial authority.
- The importance of people's right to express themselves anonymously, and that States must therefore refrain from compelling service providers to identify their users, either directly or through efforts to impact the integrity of the communications systems or services offered by providers.
- The need for States to ensure that communications companies that provide services under their jurisdiction are able to meet their obligations in relation to human rights, by ensuring that mechanisms for cross-border requests for information by States comply with the standards required by international law.

- 1 Advisory opinion AO-6/86 of 1986, conclusion.
- 2 Inter-Am Ct. H.R.The Word "Laws" in Article 30 of the American Convention on Human Rights. Advisory Opinion AO-6/86 of 1986, paragraph 18.
- 3 I/A Court H.R., Case of Escher et al. v. Brazil.
- David Kaye, Report of the Special Rapporteur of the Human Rights Council on Encryption and Anonymity to Exercise the Rights to Freedom of Opinion and Expression in the Digital Age, A/HRC/29/32, 2015, available at: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx
- 5 UN Special Rapporteur for the Protection and Promotion of the Right to Freedom of Opinion and of Expression, IACHR Special Rapporteur for Freedom of Expression, from the OAS, Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression, paragraph 12, available at: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&IID=2
- 6 AO-6/86 of 1986, paragraph 29.
- 7 Inter-Am Ct. H.R.. Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism (Arts. 13 and 29 American Convention on Human Rights) Advisory Opinion AO-5/85, paragraph 67.
- 8 Inter-American Convention against All Forms of Discrimination and Intolerance (A-69), available at: http://www.oas.org/en/sla/dil/inter_american_treaties_A-69 discrimination_intolerance.asp
- 9 Inter-Am Ct. H.R., Tristán Donoso v. Panama, paragraph 56; IACHR, Escher et al. v. Brazil, paragraph 116.
- For instance, with respect to the right to free movement, the UN Committee on Human Rights, General Comment nº 27, 1999, CCPR/C/21/Rev.1/Add.9, paragraph 14. The desirability of extending such interpretation to the restrictions to article 17 of the ICCPR arises; cf. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/13/37, paragraph 18.
- II Inter-Am Ct. H.R., Fontevecchia and D'Amico v. Argentina, paragraph 53.
- 12 Inter-Am Ct. H.R., *Tristán Donoso v. Panama*, paragraph 56; IACHR, *Escher et al. v. Brazil*, paragraph 116.
- 13 Inter-Am Ct. H.R., Chaparro Álvarez and Lapo Íñiguez v. Ecuador, paragraph 93.
- 14 Inter-Am Ct. H.R., *Kimel v. Argentina*, paragraph 83 quoted in the Office of the Ombudsman of the Republic of Panama. "Case law of the Inter-American Court of Human Rights in the Matter of Protection of Honor and Freedom of Expression." Available online at: http://defensoria.gob.pa/libros/25.pdf [Accessed on December 16, 2015], p. 16.
- Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/13/37, paragraph 17 and 18.
- 16 AO-5/85, paragraph 46.
- 17 Inter-Am Ct. H.R., *Baena Ricardo et al. v. Panama*. Competence, paragraph 79; *Mohamed v. Argentina*, paragraph 83.
- 18 Inter-Am Ct. H.R.. Apitz Barbera et al. ("First Court of Administrative Disputes") v. Venezuela, paragraph 55.

- Inter-Am Ct. H.R.. *Apitz Barbera et al.* ("First Court of Administrative Disputes") v. Venezuela, paragraph 56.
- 20 Inter-Am Ct. H.R., Escher v. Brazil, paragraph 139
- 21 Blanco, C and Salmón, E. 2012. "El Derecho al Debido Proceso en la Jurisprudencia de la Corte Interamericana de Derechos Humanos" [The Right to Due Process in the Case Law of the Inter-American Court of Human Rights]. Available online at:

 http://idehpucp.pucp.edu.pe/images/publicaciones/derecho_al_debido_proceso_en_jurisprudencia_de_corte_interamericana_ddhh.pdf [Accessed on December 17, 2015], p. 241.
- 22 Blanco, C and Salmón, E. 2012. "El Derecho al Debido Proceso en la Jurisprudencia de la Corte Interamericana de Derechos Humanos" [The Right to Due Process in the Case Law of the Inter-American Court of Human Rights]. Available online at:

 http://idehpucp.pucp.edu.pe/images/publicaciones/derecho_al_debido_proceso_en_jurisprudencia_de_corte_interamericana_ddhh.pdf [Accessed on December 17, 2015], p. 241.
- The 13 Principles and Background and Supporting International Legal Analysis, p. 33.
- 24 Inter-Am Ct. H.R.. Castillo Petruzzi v. Peru, paragraph 204.
- 25 Inter-Am Ct. H.R., Vélez Loor V. Panama, paragraph 180.
- 26 Inter-Am Ct. H.R, Mejía Idrovo vs Ecuador, 2011, available at: http://www.corteidh.or.cr/docs/casos/articulos/seriec_228_ing.pdf
- 27 Inter-Am Ct. H.R. Case of Velásquez Rodríguez v. Honduras. Preliminary Objections, para. 93; Case of the Xákmok Kásek Indigenous Community v. Paraguay. Merits, Reparations and Costs. Judgment of August 24, 2010. Series C No. 214, para. 140, and Case of Abrill Alosilla et al. v. Perú, supra note 19, para. 75.
- 28 Inter-Am Ct. H.R., Ivcher-Bronstein v. Peru Judgment of February 6, 2001 (Merits, Reparations and Costs) Paragraph 136, available at: http://www.corteidh.or.cr/docs/casos/articulos/seriec_74_ing.pdf
- 29 Constitutional Court Case, Judgment of January 31, 2001, Inter-Am Ct. H.R. (Ser. C) No. 71 (2001), paragraph 89, and Judicial Guarantees in States of Emergency (Articles 27(2), 25 and 8, American Convention on Human Rights.
- 30 United Nations, General Assembly, Human Rights Council. 2011. Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, Guiding Principles on Business and Human Rights, p. 4.
- 31 Ibid., p.7.
- 32 AG/RES. 2840 (XLIV-O/14) promotion and protection of human rights in business, passed during the second plenary session on June 4, 2014, available at: https://www.oas.org/es/sla/ddi/docs/AG-RES_2840 XLIV-O-14.pdf
- 33 United Nations, General Assembly, Human Rights Council. 2011. Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, Guiding Principles on Business and Human Rights, p. 16.
- 34 United Nations, General Assembly, Human Rights Council. 2011. Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, Guiding Principles on Business and Human Rights, p. 16.

- Article 29 Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, April 10, 2014, WP215, p. 15.
- 36 Inter-Am Ct. H.R., Claude Reyes et al. v. Chile, paragraph 77.
- 37 Inter-Am Ct. H.R., Claude Reyes et al. v. Chile, paragraph 92.
- Joint Declaration by the Rapporteurs on Freedom of Expression in the UN, the OAS and the OSCE of December 6, 2004. Available at: http://www.cidh.org/relatoria/showarticle.asp?artID=319&IID=2
- OAS, Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression. 2012. "The Inter-American Legal Framework regarding the Right to Access to Information" Second Edition. Available online at: https://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO/2004%20LA%20INFORMACION%202012%202da%20edicion.pdf [Accessed on December 23, 2015], p. 10.
- 40 Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression, paragraph 12
- Inter-American Court of Human Rights Case of Claude-Reyes et al. v. Chile, Judgment of September 19, 2006 (Merits, Reparations and Costs)
- 42 See also the *Tshwane Principles on National Security and the Right to Information* for a State debate on the retention of the public's information with national security purposes. Available at: http://www.right2info.org/national-security/Tshwane_Principles.
- OAS, Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression. 2006. "Special Study on the Right to Access to Information." Available online at: http://cidh.oas.org/relatoria/section/Estudio%20Especial%20sobre%20el%20derecho%20de%20Acceso%20a%20la%20Informacion.pdf [Accessed on December 21, 2015], p. 48.
- Article 19. 1996. The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. Available online at: https://www.article19.org/data/files/medialibrary/1803/Johannesburg-Principles.Spa.pdf [Accessed on December 21, 2015], p. 15.
- OAS, Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression. 2006. op. cit., loc. cit.
- 46 Ferreyra, Leandro. 2013. "Acceso a la Información: Hacia la Democratización de la Administración Pública" [Access to Information: Towards the Democratization of the Public Administration]. Lecciones y Ensayos 91 [Lectures and Essays № 91], p. 123.
- 47 Inter-Am Ct. H.R., *Myrna Mack Chang V. Guatemala*. Merits, Reparations and Costs, paragraph 181; IACHR, *Claude Reyes et al. v. Chile*, paragraph 202. Cf. Inter-American Commission on Human Rights, *Third Report on the Human Rights Situation in Colombia*, OEA/Sev.L/V/II.102, Doc. 9 rev. 1, paragraph 59.
- OAS. 2004. International Mechanisms for Promoting Freedom of Expression. Available online at: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=319&IID=2 [Accessed on December 22, 2015].
- 49 See also Article 29 Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, April 10, 2014, WP215. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opi....
- Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, May 16, 2011, A/HRC/17/27, paragraph 84.

- Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A.HRC/23/40), paragraph 96.
- Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression. 2013. Freedom of Expression and Internet, p. 63.
- Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (A/HRC/29/32), p. 3.
- Inter-Am Ct. H.R.. *Velásquez Rodríguez v. Honduras*. Merits, paragraph 166.
- 55 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Abid Hussain, January 8, 2000; Joint Declaration by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression from the Inter-American Commission on Human Rights, June 21, 2013; Report of the Special Rapporteur for the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin, A/HRC/10/3, February 4, 2009, paragraph 61.