

Executive summary

A human rights legal framework for communications surveillance in Latin America

Argentina, Brazil, Chile, Colombia, Mexico, Panama, Paraguay, and Peru

Executive summary

A human rights legal framework for communications surveillance in Latin America

Argentina, Brazil, Chile, Colombia, Mexico, Panama, Paraguay, and Peru

March 2021.

Author: Juan Camilo Rivera and Carolina Botero for Al Sur.

Creative Commons BY License.

This document was made from Al Sur thanks to the INDELA Fund.

Al Sur is a consortium of organizations that work in civil society and the academic field in Latin America and seek with their joint work to strengthen human rights in the digital environment of the region. For more information about Al Sur and its members, visit <https://www.alsur.lat/>

I. Introduction

Communication surveillance is a useful tool for States in their fight against terrorism and organized crime. Its regulation has always posed challenges related, among others, to the secrecy involved in its performance and the evolution of mechanisms by which it is carried out.

It is necessary to recognize that digital technologies have increased how these surveillance activities can interfere with fundamental rights such as freedom of expression and privacy of personal data and affect the exercise of other important rights in a democracy such as those of association and free development of personality.

In this context, the various social actors must keep debates open on the impact of surveillance activities in Latin America, especially in the area of human rights. These discussions should serve to identify and strengthen lines of research and analysis of public policies, especially regarding mass surveillance activities facilitated by technological advances and which are carried out by States themselves, or on occasions - and increasingly - - through its powers to have unlimited access to personal data in the hands of the private sector. In an environment strongly framed by technologies, it is necessary to discuss the impact of technological advances on rights, which, as well as offering new ways of facing threats to the security and stability of societies, also increase them.

Adopting and adjusting the legal frameworks of States to international standards of respect for people's rights is a recurring claim in recent years, aimed at adjusting powers and guaranteeing effective control and monitoring mechanisms, as well as having judicial and extrajudicial enforcement actions.

The need to impose limits on surveillance powers was addressed by the special rapporteurs on freedom of expression of the various international organizations as early as 2013 in their Joint Declaration on surveillance programs and their impact on freedom of expression.¹ Likewise, in fora such as the Organization for Economic Cooperation and Development (OECD),² which is adjusting its Privacy Guidelines and is analyzing the issue of unlimited access by governments to personal data held by companies, they will surely discuss monitoring and control mechanisms for these powers, including the standardization of transparency reports both by private parties and by governments.

Finally, investigations by organizations such as the European Union Agency for Fundamental Rights (FRA) have established that in surveillance matters, the right of people to request reparations is limited and challenging but not non-existent, to the point that they recall how in 2010 the report of the Special Rapporteur on the promotion

¹ It can be viewed at <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927>

² In December 2020, the OECD published a statement on this issue in which it establishes the creation of a group to work on recommendations for its member states. <http://www.oecd.org/sti/ieconomy/trusted-government-access-personal-data-private-sector.htm>

and protection of human rights and fundamental freedoms in the fight against terrorism stated that “persons affected by the illegal actions of an intelligence service may have recourse to an institution that provides them with an effective remedy, including full reparations of the damage suffered ” and explained how it is progressing in practice in Europe:

What is the current situation of the legal framework for communications surveillance in Latin America? That is the question that supports this first analysis focused on criminal investigation and intelligence activities. Having a comparative baseline of countries in the region will allow us to address regional debates and investigations to maintain a legal framework that respects people’s rights, guarantor in their practices, and with effective control and monitoring mechanisms that allow them to claim restitution of rights and serve as democratic control to the broad powers of the States in this matter.

With this purpose, we present this executive summary of the research that we as a consortium of Al Sur organizations carried out, based on the analysis of the legal framework of communications surveillance in eight Latin American countries: Argentina, Brazil, Chile, Colombia, Mexico, Panama, Paraguay and Peru. In particular, the document includes a comparative analysis of the legal systems of the eight countries, presenting details of the analysis performed in each country, noting some differences in the regulation that each jurisdiction has chosen. Following that, some recommendations are presented to improve the legal framework for communications surveillance in these countries.

Likewise, as an annex, comparison tables are added concerning the following topics: the constitutional regime of communications surveillance; the relevance of international human rights treaties in the domestic legal system; and highlights of aspects in the regulation on communications surveillance in intelligence work, as well as the highlights in aspects in the regulation on communications surveillance within the framework of criminal proceedings.

Scope of the document and methodology

Some clarifications are of particular importance considering the purpose described. By focusing on the analysis of the regulations on communications surveillance in the jurisdiction of each country, the intent is not to suggest that this is the only relevant aspect to guarantee the right to the confidentiality of private communications. Clearly, this study must be complemented by others that analyze the degree of compliance with domestic legislation by the corresponding authorities. In any event, it is considered that

The study "Surveillance by intelligence services - Volume II: field perspectives and legal update" can be viewed at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf

The reason for choosing these countries is because, until 2020, those are the base countries to which the members of Al Sur belong.

the description of the national regulatory frameworks helps identify responsibilities in the adequate protection of the confidentiality of private communications.

Second, the document's purpose is to provide a uniform description of the different legal frameworks analyzed, for which some topics were selected regarding which the comparison was made. However, this exercise has limitations for different reasons, among which it is found that not all legal systems describe with the same degree of precision the different topics addressed in the study.

Finally, mention should also be made that regulatory frameworks change over time. So attention should be given to the fact that the purpose of the document is to describe the regulatory situation of the eight countries mentioned as of December 2020, inviting to remember that by the time of querying this document, the national regulation may have changed or there may be proposals aimed in that direction.

II. Communications surveillance in Latin America: a legal framework under construction

The Political Constitution of each of the countries object of this study protects the right to the confidentiality of communications and always adds certain guarantees to protect it. Common to all of them is the requirement that this right may be limited only in the cases expressly provided for in law. Some constitutions include more specific guarantees, such as the exclusion of evidentiary value to documents obtained without complying with the judicial and legal confidentiality of communications, enshrined in the Constitution of Peru, or the duty to identify precisely in the request for interception of communications to the affected person, the duration and the means used, provided for in the Constitution of Mexico.

The constitutional framework of communications surveillance in the eight countries studied must take into account the hierarchy that in the system of sources of law is granted to international treaties, as such international instruments, as well as the pronouncements of international organizations in charge of applying them, contain additional guarantees to the confidentiality of communications. In this sense, it is relevant to note that, with certain particularities, in Argentina, Brazil, Chile, Colombia, and Mexico, the possibility is expressly provided that at least some international human rights treaties have constitutional hierarchy.

Regarding the inviolability of communications due to intelligence activities, all the countries studied, except for Panama, have enacted laws that seek to organize and systematize the legal framework for intelligence work.

The countries' legal systems tend to establish limits that should guide the performance of intelligence work. Sometimes these limits are formulated generally, only indicating that they must respect the Constitution and/or fundamental rights (as in Chile and Mexico). In contrast, in other cases, they are expressly provided in more detail,

referring, for example, to non-discrimination in the exercise of intelligence tasks (as is the case in Argentina, Colombia, and Paraguay) and not to interfere in internal institutional, economic and political life (as is the case in Argentina and Paraguay).

For their part, the type of powers allowed for agencies that carry out intelligence work has essential variations. The most notable is that some countries empower intelligence agencies to intercept telephone communications, while others do not include this as one of the attributions of intelligence work. Argentina, Chile, Mexico, Paraguay, and Peru are in the first category. The need for prior judicial authorization for the interception of communications for intelligence purposes, it should be noted, is established in all these cases.

Finally, to control the exercise of intelligence work, each legislation establishes different controls. Some of these controls operate concerning specific powers attributed to those organizations, as is the case regarding the interception of telephone communications in those countries where it is an attribution of intelligence organizations (i.e., Argentina, Chile, Mexico, Paraguay, and Peru.), as indicated above. In this case, the judicial control proceeds in advance. Other controls operate in regard to the overall operation of the intelligence functions. Among them, the most common is establishing a body in the respective legislative organ that oversees intelligence work. Such is the case in Argentina, Brazil, Chile, Colombia, Mexico, and Paraguay. Sometimes the law does not precisely define the scope of such control, as is the case in Brazil, where it is indicated that its scope will be defined in a subsequent act of the legislative power. In some countries, it is noteworthy that this control not only has the competence to learn of the reports that the intelligence agencies present to them, but it can also request information to fulfill the functions entrusted, as is the case in Argentina and Peru.

Regarding the limitation to the inviolability of communications for criminal investigation purposes, the countries' regulations in the report show more similarities between them. In general terms, it can be stated that the authorities are empowered to intercept private communications when this is relevant to the investigation of crimes. In the case of Mexico, there is a need to mention that such power is recognized in the investigation of crimes as well as for their prevention, which is why the National Guard is allowed to request the interception of communications.

The degree of detail of the regulation of this measure in the eight countries object of this study varies, including the cases of Mexico and Paraguay, where there is no specific regulation of the interception of communications in criminal investigation activities. Among the remainder, some legislations restrict the applicability of the interception of communications for certain crimes, establishing a severity threshold reflected in the minimum penalty with which a crime is sanctioned so that this measure can be ordered in its investigation; such is the case for Brazil, Chile, and Peru. The duration of the measure also varies: the shortest is 15 and 20 days, in Brazil and Panama, respectively, in both cases extendable, while the longest is that of Colombia, where it is allowed to be granted for up to 3 months, extendable.

Additionally, specific legislations include other means of investigation that also limit the inviolability of communications through other channels. For example, in Brazil, the environmental capture of electromagnetic, optical, or acoustic signals is empowered, or in Mexico, the authorities are empowered to proceed with geolocation and request the delivery of preserved data.

The control applicable to perform the interception of communications is judicial and before its realization. The exception to this rule is Colombia, which provides that the performance of interception of communications shall be ordered directly by the Attorney General's Office and submitted to subsequent judicial control within 24 hours after the completion of the corresponding orders.

However, there are other powers other than the interception of communications that can be exercised within the framework of criminal investigation activities that also limit the confidentiality of communications and that do not require prior judicial control. Such is the case in Mexico concerning geolocation and the delivery of preserved data, in which case there is judicial control, but subsequent. Likewise, Brazilian legislation establishes the duty of mobile and fixed telephony concessionaires to make available to the head of the Civil Police and the General Prosecutor's Office (in Portuguese, "*Ministério Público*") *records to identify the numbers of incoming and outgoing terminals for international, long-distance or local calls*. The exercise of this function does not require judicial control.

A unique and remarkable aspect is that Chilean legislation establishes that the communication interception measure must be notified to the person against whom it was directed once it has been carried out and as long as this does not endanger the life or integrity of third parties.

III. The roadmap for Latin American countries should be in compliance with human rights in communications surveillance work

The legal frameworks of different countries in the region have achieved a certain level of standardization to limit the powers to monitor communications to guarantee human rights. Thus, for example, there is generalized constitutional protection for privacy. Such protection is developed in detail by legislation, generally more broadly and specifically in criminal surveillance than intelligence.

In general terms, we find legal frameworks designed for the pre-internet era on the subject of powers. Latin American norms in general still do not address the challenges already recognized in mass surveillance activities, leaving the scope of these powers to judicial interpretation on issues such as data retention, direct access to communications infrastructures, powers regarding open intelligence sources, or intelligence authorities' capabilities to "hack" devices. Nor have the rules on international cooperation been updated.

Some exceptions should be mentioned - which in any case are vague. There are minimum provisions on geolocation and delivery of preserved data in Mexico, while in the laws of Brazil and Colombia, there are broad concepts such as “environmental capture of electromagnetic signals” or “spectrum monitoring.” Additionally, issues such as international cooperation, which are debated at the international level, are still pending in the region.

In terms of control and monitoring of the broad powers of surveillance of communications in intelligence matters, the most common is political, and in general, the laws are very general when defining it. Only some have expressly established that those who can carry out these controls are empowered to, for example, request additional information. Again, in Mexico, some controls have been established in geolocation and data conservation areas, but they are subsequent. As an exceptional measure, we have classified the fact that Chile has provided for the obligation to notify people who are the subject of an interception of communications within a specific context.

The scope of this research does not allow assessing the effectiveness of any of these monitoring and control mechanisms. However, the outlook seems inadequate if we consider that in Europe for the case of intelligence, which is usually more cryptic, in addition to the generalized establishment of parliamentary (political) control, there are judicial resources and the number of countries in which the powers of monitoring and control of these activities are assigned to independent bodies where the role of transparency and public scrutiny increases. For example, although the data protection authorities do not have powers in this field in some countries, in others, they do. In several, they have the same powers in this matter as in any other.

Finally, on the subject of judicial or extrajudicial actions that allow people to enforce their rights, there is no express legal system in the region. That is, existing actions may be used, such as attempting controls using the data protection regime, using habeas data petitions to establish whether the authorities requested your data, or constitutional actions to apply the existing legal framework. However, there are no express pathways that support processes of this type.

To achieve a legal framework suitable for these times, the actors in the region must work to:

1. Seek a legal framework that guarantees surveillance powers to monitor legal communications to be exercised only when necessary and proportional. In this sense, an effort should be made in this process to debate the necessary guarantees in the face of the challenges posed by new technological developments.
2. To drill down into how currently existing monitoring and control mechanisms on communications surveillance activities work in practice and bring the legal

frameworks of the region up to international standards where these mechanisms are not limited to the political sphere.

3. Analyze the feasibility and requirements to work in judicial and even administrative pathways that ensure effectiveness when claiming these rights.
4. Update the legal framework for communications surveillance to account for the challenges and particularities that new technologies bring to the exercise of fundamental rights and go beyond traditional forms of access to confidential information, such as the interception of communications.

IV. Annex: summary tables

1. Constitutional regime for the surveillance of communications

	Regulation of the inviolability of communications
Argentina	Provides for the inviolability of correspondence and private papers. It points out that it can be limited by law indicating the cases and justifications to proceed with the search and seizure.
Brazil	It recognizes the right to the inviolability of the secrecy of communications, adding that it can only be limited when there is a judicial order and in the cases and manners set forth in law in the case of a criminal investigation or to try criminal proceedings.
Chile	It recognizes the right to the inviolability of private communications and provides that there must be a law that specifies the cases and manners to limit these
Colombia	It indicates that correspondence and other forms of private communication are inviolable, specifying that these can be intercepted or logged by judicial order and in the cases and with the formalities established in law.
Mexico	It establishes the right to the inviolability of communications and regulates a comprehensive catalog of guarantees related to this right. Among the most notable are the following: the duty to punish ignorance of the freedom or secrecy of communications; the judicial confidentiality for the interception of any private communication, indicating that it must be authorized by a federal judicial authority, at the request of the federal authority indicated by law or of the head of the Public Ministry of a federative entity, based on legal grounds; the duty of the corresponding federal authority to provide reasoning for the request and to precisely identify the affected person, the duration and the means; and some types of matters on which the intervention of communications may not apply (namely: electoral, fiscal, commercial, civil, labor or administrative matters, nor the communications of the detainee with their defense attorney).
Panama	It establishes that correspondence and other private documents are inviolable, so they cannot be examined or retained, except by order of a competent authority and for specific purposes, in compliance with the manners provided in law. It adds that absolute confidentiality must be kept concerning matters unrelated to the object of the examination or

	retention.
Paraguay	It recognizes the inviolability of telephone, telegraphic, cable, or any other kind of communications. It adds that, as a consequence, such communications cannot be examined, reproduced, intercepted, or seized, except in the case of a court order, in the case of specific matters provided for in the law, and in the case of essential information for clarification of the matters of competence of the corresponding authorities.
Peru	It recognizes the inviolability of communications, telecommunications, and their instruments. It provides that they can only be opened, seized, intercepted, or intervened by reasoned order of a judge, following the guarantees provided in law. The previous exception to the inviolability of communications should be limited to those matters that were grounds for their examination. Evidentiary value is also excluded for documents that have not been obtained in compliance with the provisions of this article.

2. Relevance of international human rights treaties in the domestic legal system

	Legal relevance in the internal legal system of international human rights treaties
Argentina	It recognizes constitutional hierarchy to a comprehensive catalog of human rights treaties expressly provided for in the Constitution.
Brazil	It recognizes constitutional hierarchy of human rights treaties approved by the National Congress by a special majority of its members.
Chile	It recognizes constitutional hierarchy of the human rights treaties ratified by Chile and that are in force.
Colombia	Recognizes constitutional hierarchy to human rights treaties “ <i>ratified by Congress, which recognize human rights and prohibit their limitation in states of exception,</i> ” while indicating that all international human rights treaties ratified by Colombia must be considered in the interpretation of the rights provided in the Constitution.
Mexico	It recognizes constitutional hierarchy of human rights treaties to which the Mexican State is a party.
Panama	There is no specific clause that refers to the normative value of international human rights treaties.
Paraguay	It recognizes the international treaties, conventions, and agreements approved and ratified an infra-constitutional value but higher than that of the laws.
Peru	It assigns the rank of law to international treaties in general.

3. Highlights in the regulation on communications surveillance in intelligence work

	Express limits on intelligence activities	Powers that intelligence agencies may carry out to obtain information	Is there judicial control to authorize intelligence activities?
--	---	---	---

Argentina	No intelligence agency may carry out police or criminal investigation functions, take into account discriminatory grounds in the performance of its functions, seek to influence the political, institutional, military, social, or economic life of the country, or reveal or disclose information acquired in the country in the exercise of their functions (unless there is a court order).	- Interception or capture of private communications of any kind.	Yes, in the case of interception or capture of private communications of any kind. In this case, the control is prior.
Brazil	Intelligence activities must be carried out with <i>“unrestricted respect for individual rights and guarantees, with loyalty to the institutions that govern the interests and security of the State.”</i>	The only power that the legislation specifies related to the collection or production of relevant information for the performance of intelligence functions is to access, by electronic means, databases of the bodies to which they belong.	No judicial control is provided for in the performance of this activity.
Chile	It is established that intelligence activities must be carried out under the Political Constitution and the laws	When it comes to obtaining information not available from open sources, these powers are provided: - Intervention of telephone, computer, radio, and correspondence communications in any of their forms. - Intervention of computer systems and networks - Electronic listening and recording, including audiovisual - Intervention of any other technological systems intended for the transmission, storage, or processing of communications or information.	Prior judicial control concerning all the procedures above related to obtaining information not available in open sources.
Colombia	Intelligence work can only	Two powers that	The two activities

	<p>be carried out to protect certain ends, indicated in the Colombian intelligence law; they cannot be used for discriminatory purposes; and when deciding on its implementation, it must be analyzed that the principles of need, suitability, and proportionality are met.</p>	<p>intelligence agencies can exercise to carry out their functions are expressly regulated:</p> <ul style="list-style-type: none"> - Monitoring of the electromagnetic spectrum, which is different from the interception of personal communications. The latter cannot be done for intelligence purposes. - Demand from telecommunications service operators information that would aid in identifying and locating the users of these services. 	<p>mentioned do not require prior judicial control for their performance.</p>
Mexico	<p>It is generally stated that, when using any method of information gathering, the intelligence authorities must respect individual guarantees and human rights.</p>	<p>The intelligence agencies may make use of any information-gathering method. In addition, Mexican legislation refers to a specific power that allows the collection of intelligence information and limits the confidentiality of the information. It is about the intervention of private communications, applicable to <i>“private communications and broadcasts, made by any means of transmission, known or to be known, or between those present, including the recording of private images.”</i></p>	<p>The intervention of communications for intelligence reasons requires judicial authorization.</p>
Panama	<p>General prohibitions are established for the Executive Secretariat of the National Security Council, which is the body that, among other functions, performs intelligence tasks. Such prohibitions are the following: violate the rights enshrined in the Constitution and the laws; participate in any partisan</p>	<p>Request data, statistics, and information that are related to national security from natural or legal persons, as well as to provide the necessary support and collaboration</p>	<p>The control that the judges may perform regarding intelligence functions that may affect the confidentiality of communications is not specified.</p>

	political activity; disseminate any information that it may have come to know due to its activities; any other activity that threatens the physical and moral integrity, honor and property of the associates; and carrying out activities that involve political espionage.		
Paraguay	Intelligence work cannot be carried out for discriminatory purposes, nor to influence the country's institutional, political, military, police, social or economic situation, nor to carry out repressive, police, or criminal investigation work, nor reveal or disseminate information obtained within the framework of its activities.	The following specific procedures for obtaining information are established: - Intervention of telephone, computer, radio, and correspondence communications in any of their forms. - Intervention of computer systems and networks - Electronic audiovisual listening and recording. - Intervention of any other technological systems intended for the transmission, storage, or processing of communications or information.	The authorization of the so-called specific procedures for obtaining information must be carried out by a supervisory judge [TN: juez de control de garantías].
Peru	A series of operating principles are established for intelligence services: legality, legitimacy, democratic control, relevance, restricted circulation, specialty, and planning.	Intelligence agencies can carry out, among others, "special operations," understood as intelligence and counterintelligence operational actions, which imply the infringement of certain citizens' rights due to threats to national security, requiring prior judicial authorization to carry them out.	The so-called "special operations" require judicial authorization in order to be carried out.

4. Aspects highlighted in the regulation on communications surveillance within the framework of criminal proceedings.

	Criminal investigation measures that interfere with the inviolability of	How does judicial control operate concerning these
--	--	--

	communications	measures?
Argentina	Interception and seizure of postal, telegraphic, electronic correspondence or any other form of communication or any other effect sent by the accused or intended for them, even under an assumed name	Prior judicial control.
Brazil	<ul style="list-style-type: none"> - Interception of communications that take place via information technologies and telematic means. - Environmental capture of electromagnetic, optical, or acoustic signals. - Duty of mobile and fixed telephony concessionaires to maintain for five years at the disposal of the head of the Civil Police and the General Prosecutor's Office "<i>records to identify the numbers of incoming and outgoing terminals for international, long-distance or local calls.</i>" - The head of the Civil Police and the General Prosecutor's Office will be able to access certain information about the account held by, among other entities, telephone companies and internet providers. 	<p>The interception of telephone communications requires prior judicial authorization. Likewise, once the interception procedure has been carried out, the judge must decide whether the results are relevant to the investigation, thus also having subsequent judicial control.</p> <p>Also, prior and subsequent judicial control applies regarding the environmental capture of electromagnetic, optical, or acoustic signals.</p>
Chile	<ul style="list-style-type: none"> - Retention and seizure of postal, telegraphic, or other kinds of correspondence and that addressed to the accused or sent by them, or of those which are presumed to emanate from them or from which they may be the addressee. - Interception and recording of telephone communications or other forms of telecommunication. 	Given that any action that deprives the accused of their rights or restricts or disturbs them requires prior judicial authorization from the supervisory judge, these two measures require this type of control.
Colombia	<ul style="list-style-type: none"> - Interception, by tape recording or similar, of telephone, radiotelephone, and similar communications that use the electromagnetic spectrum, whose information is of interest for the action. - Seizure of the equipment and storage media that the target of investigation could have used to transmit helpful information for the investigation carried out through the Internet or other technological means that produce equivalent effects. - Withholding of private, postal, 	The judicial control of the measures mentioned above is subsequent, within 24 hours following the completion of the corresponding orders.

	telegraphic, or specialized courier correspondence or similar.	
Mexico	<ul style="list-style-type: none"> - Intervention of private communications covers any communication system or program that allows the exchange of data, information, audio, video, messages, as well as electronic files that record, preserve the content of the conversations or record data that identify the communication, which can take place in real-time”. - Geolocation and request for the delivery of stored data. 	<p>Regarding the intervention of private communications, the judge will decide whether to authorize it. Likewise, they may at any time verify that this is carried out in the authorized terms and, in the event of non-compliance, decree its partial or total revocation. On the other hand, once the proceeding is concluded, the Attorney General’s Office will inform the judge.</p> <p>Regarding the delivery of information for geolocation and the delivery of preserved data, there is prior judicial control by the supervisory judge thereof competent. However, in certain circumstances, the measure may be ordered directly by the Attorney General of the Republic or whoever is delegated for this purpose, in which case the judicial control will be subsequent.</p>
Panama	<ul style="list-style-type: none"> - Seizure of correspondence. - Recording of conversations and interception of cyber communications, satellite monitoring, electronic surveillance, and telephone communications. 	The supervisory judge must grant permission to carry out these investigation measures.
Paraguay	<ul style="list-style-type: none"> - Interception and seizing of correspondence. - Intervention of the accused’s communications, whatever the technical means used. 	There is prior judicial control of the restrictive measures of the inviolability of communications.
Peru	<ul style="list-style-type: none"> - Intervention or recording or logging of telephone communications or other forms of communication. - Record of the intervention of telephone communications or other forms of communication. 	Prior judicial authorization is necessary so that the investigation measures related to the interception of communications can be carried out.