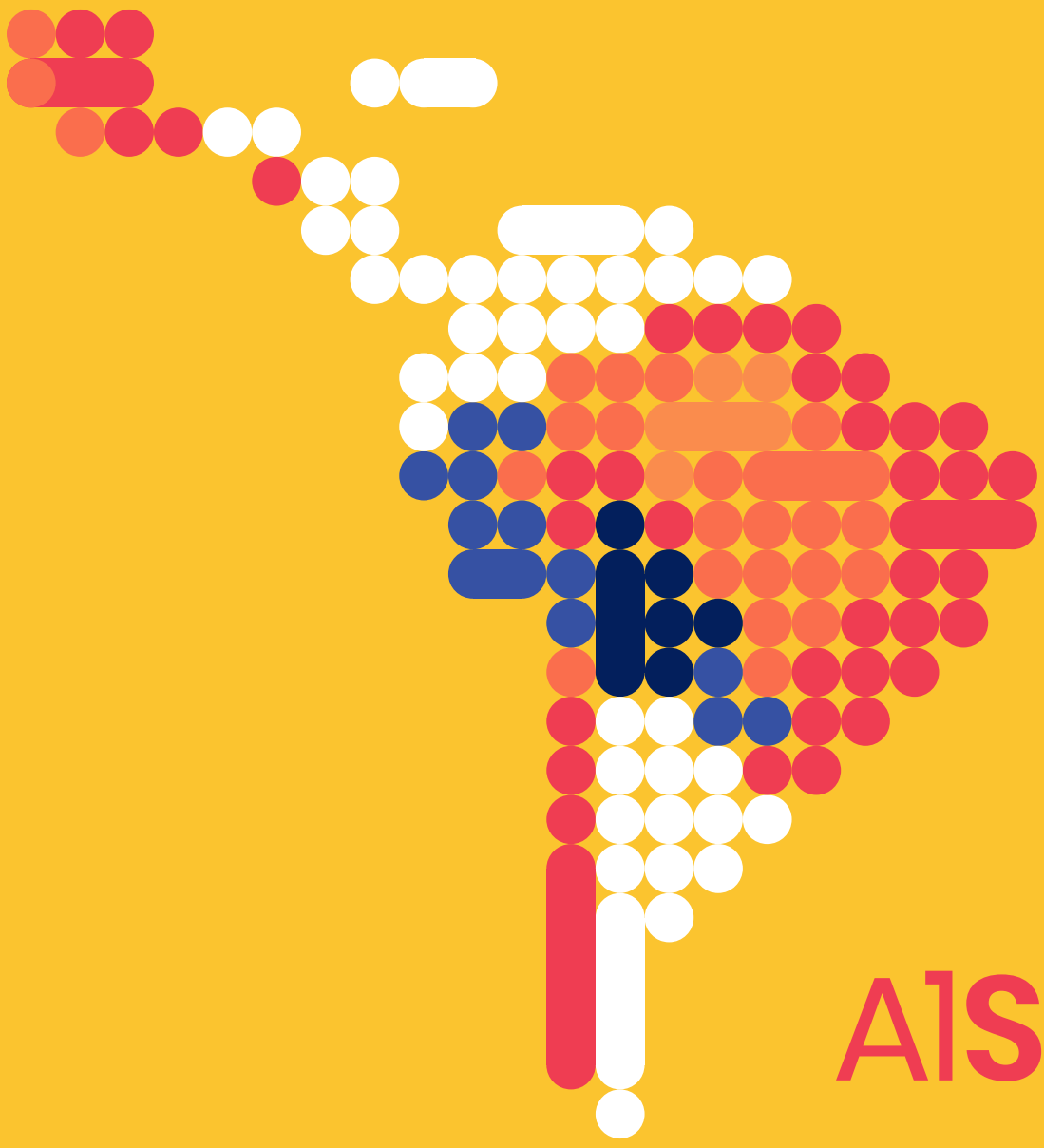
Surveillance trends and practices in Latin America.

Case studies from Brazil, Chile, Colombia, El Salvador, Mexico, Peru, and Paraguay



AlSur

Surveillance trends and practices in Latin America.

Case studies from Brazil, Chile, Colombia, El Salvador, Mexico, Peru, and Paraguay

COORDINATION:
Silvia Calderón, Pan American Institute of Law and Technology (IPANDETEC)
Ana Gaitán, Network for the Defense of Digital Rights (R3D)

AUTHORSHIP AND REVIEW:
Helena Secaf - InternetLab Research Center
Vitor Vilanova - InternetLab Research Center
María Parra - *Karisma Foundation*
Lucia Camacho - Digital Rights
Laura Mantilla - Digital Rights
Maricarmen Sequera - TEDIC
Dilmar Villena - Hiperlaw
Ana Gaitán - Network for the Defense of Digital Rights (R3D)
Silvia Calderón - Pan American Institute of Law and Technology (IPANDETEC)

REVIEW:
Camila Leite – Institute for Consumer Protection (IDEC)
Luã Cruz – Institute for Consumer Protection (IDEC)

DESIGN:
Marcelo Lazarle

PREPARED FOR THE CONSORTIUM: AlSur

FUNDED BY: CHARLES STEWART MOTT FOUNDATION

JUNE 2025

AlSur

"AlSur" is a consortium of 11 organizations working in civil society and academia in Latin America that seek to strengthen human rights in the region's digital environment through their joint efforts.

ORGANIZATIONS THAT MAKE UP AL SUR

- Civil Rights Association (ADC) - Argentina
- Center for Studies on Freedom of Expression and Access to Information (CELE) - Argentina
- Coding Rights - Brazil
- Digital Rights - Regional
- *Karisma Foundation* - Colombia
- Hyperlaw - Perú
- Brazilian Institute for Consumer Protection (IDEC) - Brazil
- Pan American Institute of Law and Technology – Central America
- InternetLab - Brazil
- Network for the Defense of Digital Rights (R3D) - Mexico
- TEDIC - Paraguay

Index

INDEX OF TABLES

Acronyms

ACRONYM	DEFINITION
ABIN	Brazilian Intelligence Agency
ADO	Direct Action of Unconstitutionality by Omission [Brazil]
ADPF	Action for Breach of Fundamental Precept [Brazil]
AFDD	Association of Families of Disappeared Detainees [Chile]
AFEP	Association of Families of Politically Executed Persons [Chile]
ANEF	National Association of Tax Employees [Chile]
Bacib	Cyber Intelligence Battalions [Colombia]
BIPE	Special Police Investigation Brigade [Chile]
CADH	American Convention on Human Rights
Caso CAJAR	Case Members of the "José Alvear Restrepo" Lawyers' Collective Corporation vs. Colombia
CIDH	Inter-American Commission on Human Rights
CNPP	National Code of Criminal Procedure [Mexico]
Corte IDH	Inter-American Court of Human Rights
Córtex	Integrated Public Safety Operations and Monitoring Platform [Brazil]
CUT	United Workers' Central [Chile]
DIGIMIN	Directorate General of Intelligence [Peru]
DINI	National Intelligence Directorate [Peru]
FEADLE	Special Prosecutor's Office for Crimes Against Freedom of Expression [México]
FECH	Student Federation of the University of Chile
FEDEUNAP	Student Federation of the Arturo Prat University [Chile]
FGN	Attorney General's Office [Colombia]
FLIP	Foundation for Press Freedom
ISP	Internet Service Provider
LGN	National Guard Act [Mexico]
MJSP	Ministry of Justice and Public Security [Brazil]
MP	Public Prosecutor's Office
OSIPTEL	Supervisory Agency for Private Investment in Telecommunications [Perú]
PDI	Chilean Investigative Police [Chile]
PGN	Office of the Inspector General [Colombia]
PGR	Prosecutor General of the Republic [Brazil]
PNP	National Police of Peru
RdC	[Journalists from] Conflict Routes [Colombia]
RELE	Special Rapporteur for Freedom of Expression
SEDENA	Secretariat of National Defense [México]
SEIDO	Specialized Deputy Attorney General's Office for Organized Crime Investigation [México]
SEOPI	Secretariat of Integrated Operations of the Ministry of Justice and Public Security [Brasil]
TEDH	European Court of Human Rights
OACNUDH	Regional Office of the United Nations High Commissioner for Human Rights for Central America, the Dominican Republic, and the Caribbean
OEA	Organization of American States
ONU	United Nations Organization

INTRODUCTION

Both the General Assembly and the Human Rights Council of the United Nations (hereinafter, UN) have emphasized that the right to privacy is one of the foundations of democracies and free personal expression and, as such, plays an essential role in the protection and promotion of other rights, including the rights to freedom of opinion, expression, religion, assembly, and association.[1]

Given the interconnectedness of human rights, the adverse effects of privacy violations can also lead to violations of rights such as equality before the law, the right to life, to freedom and personal integrity, to a fair trial and due process, the right to freedom of expression, protest and association, to freedom of movement, the right to enjoy the highest possible standard of health and access to work and social security, among others.[2]

In this regard, both the United Nations High Commissioner for Human Rights and the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression have determined that the surveillance of private communications has repercussions on civil society and democratic discourse.[3] The risk of being a target of surveillance and the desire to avoid being targeted leads people to self-censor. When people perceive themselves to be under surveillance, they alter and limit the way they express themselves and communicate with others. Due to this *"chilling effect,"* surveillance technologies affect not only the people whose data is collected, but also society as a whole, by directly and indirectly interfering with the free exchange and evolution of ideas. [4]

Historically, intelligence activities carried out in Latin America, whether by civil, police, or military authorities, far from serving the general interests of society, have themselves become a threat to respect for human dignity and rights.

Currently, there is documented evidence of the progressive use by governments of communications surveillance technologies to repress, censor, and persecute human rights defenders, journalists, social activists, and political opponents.[5] Such surveillance has put their lives and personal integrity at risk and has hindered efforts to report and ensure accountability for acts of corruption and human rights violations committed by public authorities as well as private individuals or institutions.

---

1 United Nations. General Assembly. (2017). Resolution A/RES/71/199 The right to privacy in the digital age. Available at: https://documents.un.org/doc/undoc/gen/n16/455/37/pdf/n1645537.pdf,
United Nations. General Assembly. (2018). Resolution A/RES/73/179. The right to privacy in the digital age. Available at: https://docs.un.org/es/A/res/73/179 y,
United Nations. General Assembly. (2017). Resolution A/HRC/RES/34/7. The right to privacy in the digital age. Available at: https://docs.un.org/es/A/HRC/RES/34/7

2 Huszti-Orbán, K., Ní Aoláin, F. (2020). Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?". Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf

3 See, for example, United Nations General Assembly (2016). Resolution A/HRC/32/38. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Available at: https://docs.un.org/es/a/hrc/32/38

4 United Nations. General Assembly. (2013). Resolution A/HRC/23/40. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Para. 24. Available at: https://docs.un.org/es/A/HRC/23/40

5 United Nations. General Assembly. (2019). Resolution A/HRC/41/35. Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Para. 1. Available at: https://docs.un.org/es/A/HRC/41/35

Similarly, most current surveillance measures involve the massive and indiscriminate collection and storage of information about the private communications of millions of people, the vast majority of whom are not involved in criminal activity. Access to the content of our communications, as well as the analysis of the metadata associated with them, such as location data, gives the State a high degree of invasive power and control over all individuals, in addition to undermining personal autonomy and civic participation.

In addition, the technologies available to carry out these activities are becoming increasingly sophisticated. The proliferation of mass surveillance technologies, such as fake antennas, outsourcing of mass surveillance, or highly invasive and elusive targeted surveillance technologies such as spyware, is indicative of the lack of clarity and precision regarding the surveillance methods that can currently be considered compatible with human rights standards.

Thus, this report, *Surveillance Trends and Practices in Latin America*, is particularly relevant in the context in which we find ourselves: deteriorating democracies, the proliferation of organized crime, and the rise of authoritarianism. Given the uncontrolled spread of communications surveillance technologies, it is essential to push for greater scrutiny, control, and regulation of these tools.

For this reason, this report documents some of the ways in which various surveillance technologies are used in an opaque, secretive, discretionary, and abusive manner by authorities without legal authority and without adequate safeguards to prevent, mitigate, or remedy such abuses.

It is important to note that, when referring to surveillance trends and practices, this category includes all techniques and technologies owned or used by the state that have the capacity to interfere with, limit, or affect the exercise of the right to privacy, regardless of whether their deployment is covered by local law.

Among surveillance techniques and practices, those that focus on private communications are just one type within a more complex taxonomy of surveillance modalities. Therefore, although the report focuses on private communications, it also explores other modalities and techniques of state surveillance that raise concerns about their impact on human rights.

For example, among the techniques and technologies of surveillance focused on communications[6] are the interception of communications through intermediaries, such as internet service providers; the request for data and metadata from telecommunications service subscribers; the direct and targeted interception of communications by states through, for example, the use of malicious software (spyware); the use of surveillance techniques focused on monitoring social media and the internet, such as cyber patrols; and the use of technologies that intercept signals from communications infrastructure and mobile devices, such as stingrays or IMSI catchers, among others.

However, there are other forms of state surveillance that do not focus on communications, but rather on tracking individuals, such as the deployment and use of facial recognition systems—which we explored in an AlSur report published in 2021[7] and in another one published in 2025[8]—; as well as the deployment and use of vehicle license plate recognition systems, among others.

---

6 Different forms of mass surveillance focused on people's communications are explored in reports A/HRC/23/40 of April 2013 and A/HRC/41/35 of May 2019, both from the United Nations Special Rapporteur on Freedom of Expression.

7 Venturini, J.; Garay, V. (2021). Facial recognition in Latin America. Trends in the implementation of a perverse technology. AlSur. Available at: https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf

8 To be published soon.

This report is the result of research on surveillance practices in Latin America by AlSur organizations in Colombia, Chile, Peru, Mexico, Paraguay, and Brazil. The research was carried out through monitoring and documentation conducted by each of the participating organizations in their respective countries. The research covered the period from 2016—when the use of communications surveillance measures began to grow exponentially in the region—to the end of 2024.

It is important to mention that in many cases the legality of their use is questionable and, in most cases, there is widespread opacity regarding their use. However, the compilation also included data on the legislative landscape, government actions, and security, administrative, and judicial entities.

Chapter 1 of the report compiles the human rights standards applicable to communications surveillance. *Chapter 2* identifies the rules and procedures that regulate communications surveillance in different countries in the region. *Chapter 3* documents emblematic cases in which communications surveillance techniques were used in the region. Finally, *Chapter 4* provides an assessment of trends and practices in Latin America, highlighting regulatory deficiencies, opacity, and irregularities in the acquisition of surveillance technologies, illegal surveillance, and impunity that have existed regarding communications surveillance. The report concludes with a set of findings and recommendations for States on regulation in this matter.

CHAPTER ONE: HUMAN RIGHTS STANDARDS APPLICABLE TO COMMUNICATIONS SURVEILLANCE

The right to privacy and the protection of personal data are fundamental human rights, although they are not always recognized as distinct and autonomous, despite their relationship and interdependence. These rights are recognized in extensive human rights instruments at both international[9] and regional levels.[10]

At the inter-American level, the Inter-American Court of Human Rights (hereinafter, "IACHR") has defined privacy as a right that: "encompasses a series of factors related to the dignity of the individual, including, for example, the ability to develop one's personality and aspirations, determine one's own identity, and define one's own personal relationships."[11]

In a more recent interpretation of the content of the ACHR and the Inter-American corpus iuris[12], the IACHR established that international standards for the protection of personal data require that its processing occur only with the free and informed consent of the data subject or under a regulatory framework that authorizes such processing.[13]

The protection afforded to every person under international human rights law to a private and family life free from arbitrary interference, as well as to the protection of their personal data, extends to their digital communications.[14] Thus, the IACHR has also ruled on the protection of privacy in the context of the communication process, including metadata, emphasizing that its criteria "are fully applicable to intelligence activities involving the surveillance of [such metadata]".[15]

However, the right to a private life is not an absolute right, and the use of intelligence activities can have legitimate purposes and be a useful means of investigating crimes and combating threats to national security. Legitimate limitations on the right to privacy must be aligned with human rights standards. In this regard, the IACHR determined that "measures aimed at controlling intelligence activities must be particularly rigorous, given that, due to the secretive nature of such activities, they may lead to human rights violations and criminal offenses".[16]

---

9 Universal Declaration of Human Rights (art. 12), the International Covenant on Civil and Political Rights (art. 17), the Convention on the Rights of the Child (art. 16), the International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families (art. 14), including General Comment No. 16 of the UN Human Rights Committee of 1988, among other universal human rights instruments.

10 American Convention on Human Rights (hereinafter, "ACHR"), Inter-American Convention on Protecting the Human Rights of Older Persons, art. 11; art. 12, c, ii.; further enriched by the Updated Principles on Privacy and Personal Data Protection of 2021, among others.

11 IACHR. Case of Artavia Murillo et al. (In vitro fertilization) v. Costa Rica. Preliminary objections, merits, reparations, and costs. Judgment of November 28, 2012. Para. 143.

12 Also includes the "Updated Principles of the Inter-American Juridical Committee on Privacy and Personal Data Protection, with Annotations," OEA/Ser.D/XIX.20, January 2022.

13 IACHR. Case of Members of the José Alvear Restrepo Lawyers' Collective v. Colombia, Judgment of October 18, 2023, Preliminary Objections, Merits, Reparations, and Costs, para. 573..

14 Various human rights bodies have adopted a broad perspective on what falls within the scope of privacy protection in the digital context, including: audiovisual surveillance (El Haski v. Belgium [2012] ECHR 2019; (2013) 56 EHRR 31, [102]); metadata (Malone v. United Kingdom [1984] ECHR 10; (1985) 7 EHRR 14, [84]); and geolocation information (Uzun v. Germany [2010] ECHR 2263; (2011) 53 EHRR 24, [12]-[13]).

15 IACHR. Case of Escher et al. v. Brazil, supra, para. 114; and para. 543.

16 Inter-American Court of Human Rights. Case of Myrna Mack Chang v. Guatemala. Merits, Reparations, and Costs. Judgment of November 25, 2003. Series C No. 101, para. 284.

Thus, in order for restrictions on the rights to privacy and personal data protection to comply with national, regional[17],[18],[19], and international standards[20] in this area—and prohibit illegal and arbitrary surveillance measures— the requirements of legality, legitimate purpose, suitability, necessity, and proportionality[21] must be met, which, in turn, implies the establishment of adequate safeguards to prevent, avoid, and remedy the abusive exercise of such measures.

I. Principle of legal reserve: Clear, precise, and detailed definition of the authorities empowered to carry out surveillance measures, the procedure, and the circumstances in which they may be carried out.

According to the IACHR, the reservation of law or the expression "laws," to which the ACHR refers as the means of limiting rights (Art. 30), goes beyond the principle of formal legality, encompassing all legitimate normative acts focused on the common good and emanating from constitutionally and democratically elected bodies.[22]

For its part, the Joint Statement on Surveillance Programs and their Impact on Freedom of Expression states:

> States must ensure that the collection, gathering, and use of personal information (...) are clearly authorized by law in order to protect individuals against arbitrary or abusive interference with their private interests. The law shall establish limits on the nature, scope, and duration of such measures, the reasons for ordering them, the authorities competent to authorize, execute, and supervise them, and the legal mechanisms available for challenging them. 23

---

17 International Principles on the Application of Human Rights to Communications Surveillance. Available at: https://necessaryandproportionate.org/es/necesarios-proporcionados

18 IACHR. Special Rapporteur for Freedom of Expression. Freedom of Expression and the Internet. December 31, 2013. OEA/Ser.L/V/II, para. 165.

19 IACHR. Case of Myrna Mack Chang v. Guatemala, supra; Case of Maritza Urrutia v. Guatemala. Merits, Reparations, and Costs. Judgment of November 27, 2003. Series C No. 103; Case of Huilca Tecse v. Peru. Merits, Reparations, and Costs. Judgment of March 3, 2005. Series C No. 121; Case of Blanco Romero et al. v. Venezuela. Merits, Reparations, and Costs. Judgment of November 28, 2005. Series C No. 138; Case of Goiburú et al. v. Paraguay, supra; Case of La Cantuta v. Peru. Merits, Reparations, and Costs. Judgment of November 29, 2006. Series C No. 162; Case of Escher et al. v. Brazil, supra; Case of Anzualdo Castro v. Peru. Preliminary objection, merits, reparations, and costs. Judgment of September 22, 2009. Series C No. 202; Case of Gelman v. Uruguay. Merits and reparations. Judgment of February 24, 2011. Series C No. 221; Case of González Medina et al. v. Dominican Republic. Preliminary Objections, Merits, Reparations, and Costs. Judgment of February 27, 2012. Series C No. 240; Case of Gudiel Álvarez et al. ("Diario Militar") v. Guatemala, supra; Case of García et al. v. Guatemala, supra; Case of Hermanos Landaeta Mejías et al. v. Venezuela, supra; Case of Rodríguez Vera et al. (Disappeared from the Palace of Justice) v. Colombia, supra; Case of Julien Grisonas Family v. Argentina, supra; Case of Maidanik et al. v. Uruguay. Merits and Reparations. Judgment of November 15, 2021. Series C No. 444; Case of Movilla Galarcio et al. v. Colombia, supra, and Case of Deras García et al. v. Honduras. Merits, Reparations, and Costs. Judgment of August 25, 2022. Series C No. 462.

20 United Nations. General Assembly. (2010). Resolution A/HRC/14/46. Report of Martin Scheinin, Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering terrorism. Available at: https://docs.un.org/es/A/HRC/14/46; United Nations. General Assembly. (2013). Resolution A/HRC/23/40. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Available at: https://docs.un.org/es/A/HRC/23/4; United Nations. General Assembly. (2014). Resolution A/HRC/27/37. The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights. Available at: https://docs.un.org/es/A/HRC/27/37y; United Nations. General Assembly. (2020). Resolution A/RES/75/176. The right to privacy in the digital age. Available at: https://docs.un.org/es/A/RES/75/176

21 IACHR. Case of Tristán Donoso v. Panama, supra, para. 56, and Case of Fernández Prieto and Tumbeiro v. Argentina. Merits and Reparations. Judgment of September 1, 2020. Series C No. 411, para. 105.

22 IACHR. Advisory Opinion OC-6/86 of May 9, 1986. The term "laws" in Article 30 of the American Convention on Human Rights. Available at: https://www.corteidh.or.cr/docs/opiniones/seriea_06_esp.pdf

23 IACHR. (2013). Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression. Available at: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&IID=2

The Special Rapporteur for Freedom of Expression (hereinafter RELE) has established that, in the context of surveillance measures, the law must be sufficiently clear in its terms to provide citizens with adequate guidance regarding the conditions and circumstances under which authorities will be empowered to resort to such measures.24 Similarly, it has pointed out that:

> *Vague or ambiguous legal provisions* that grant very broad discretionary powers are incompatible with the American Convention because *they can support potential acts of arbitrariness that result in the violation of the right to privacy or the right to freedom of thought and expression guaranteed* by the Convention.[25]

Similarly, the IACHR has stated that the first requirement in the exercise of intelligence activities refers precisely to the *principle of legal reserve* for the effective protection of rights and the "adequate control of the exercise of the powers of state bodies." [26]

Regarding the controls and limitations to which intelligence activities must be subject, the IACHR recently ruled that intelligence activities must be regulated as precisely as possible, defining the authorized methods for gathering information, the objectives, the persons and activities subject to surveillance, the degree of suspicion that justifies the gathering of information, the permitted duration of these measures, and the methods of supervision and control.[27]

Furthermore, if the exchange of information between intelligence agencies is permitted, clear conditions, legitimate purposes, competent authorities, and safeguards to protect personal data in particular must be specified.[28]

Likewise, all activities must be formalized through numbered processes, including controls on access to systems, and the processing of personal data must be accompanied by records that i. identify those responsible; ii. the purposes of the processing; iii. the legal basis; iv. the retention periods; and v. the methods used, as well as a history of all actions performed on that data.[29]

Similarly, in terms of personal data collection, the IACHR stipulates that the powers of intelligence services (which are generally exercised without the consent of the data subject) must be based on laws that describe:

> a) the reasons that justify the existence of files containing personal data by intelligence agencies; such reasons, in accordance with the purposes of intelligence activities, shall limit the actions of the authorities in this area; b) the types and categories of personal data that the authorities are authorized to keep in their files, and c) the parameters applicable to the use, storage, verification, rectification, deletion, or disclosure of such data [...].30

---

24 IACHR. Case of Escher et al. v. Brazil. Preliminary Objections, Merits, Reparations, and Costs. Judgment of July 6, 2009. Series C No. 200.

25 IACHR. Special Rapporteur for Freedom of Expression. Freedom of Expression and the Internet. December 31, 2013. OEA/Ser.L/V/II.

26 IACHR. Advisory Opinion OC-6/86, supra, para. 24. Reiterated in Case Members of the José Alvear Restrepo Lawyers' Collective v. Colombia, Judgment of October 18, 2023, Preliminary Objections, Merits, Reparations, and Costs. Para. 529.

27 Case Members of the José Alvear Restrepo Lawyers' Collective vs. Colombia, Judgment of October 18, 2023, Preliminary Objections, Merits, Reparations, and Costs, para. 520.

28 Ibid., para. 539.

29 Ibid., para. 540.

30 Ibid., para. 577.

II. Principles of necessity and proportionality: Safeguards against abuse

The following are presumed: *(i) a constitutionally valid purpose* (one that reflects a prevailing legal interest and is necessary in a democratic society), *(ii) suitability* (adequacy of the restriction of the right to its purpose), *(iii) necessity of the measure* (the means least likely to violate human rights), and *(iv) its proportionality in the strict sense* (between the degree of interference with the fundamental right implied by the legislative measure under examination and the degree to which it achieves its intended purpose).

Finally, *(v) safeguards* must be in place, such as judicial oversight (prior to or immediately following invasive measures), transparency and independent supervision (with accountability), and the right to notification (to affected individuals once surveillance has been completed).

1. Constitutionally valid purpose

Even though communications interception and other invasions of privacy are, in many cases, interference in privacy that pursues legitimate ends such as the investigation of serious crimes and the protection of national security, it is also clear that there are inherent risks of abuse.

Therefore, first, surveillance measures must identify the purposes they pursue in order to then determine whether they are constitutionally valid.[31] Thus, laws should only allow the surveillance of communications by specific state authorities to achieve a legitimate objective that corresponds to an overriding and necessary legal interest in a democratic society. In the words of the Human Rights Council, legal and specific surveillance of digital communications may be a necessary and effective measure for intelligence activities for reasons of national security, prevention of terrorism, or other crimes. It may constitute a legitimate objective, provided that the degree of interference is proportionate to the necessity and benefit of the measure for achieving that objective and as long as Article 17 of the Covenant is respected.[32]

Similarly, the aforementioned Joint Statement on Surveillance Programs and their Impact on Freedom of Expression states that:

> When national security is invoked as a reason for monitoring correspondence and personal data, the law must clearly specify the criteria to be applied in determining the cases in which such limitations are legitimate. Their application should only be authorized when there is a real risk to the interests being protected, and when that risk outweighs the general interest of society in maintaining the right to privacy and freedom of expression and circulation of information.[33]

In this regard, the IACHR specifies that the above objectives are considered "legitimate purposes" insofar as they align with a Rule of Law that always ensures the protection of individual rights.[34] Therefore, vague and imprecise statements cannot justify the actions of intelligence agencies, as this would imply a departure from those purposes, or even contradict or nullify them.[35]

---

31 SCJN. Appeal for review 237/2014. Presiding judge: Arturo Zaldívar Lelo de Larrea. Approved by majority vote. This precedent gives rise to Isolated Thesis 1a. CCLXV/2016 (10a.) FIRST STAGE OF THE PROPORTIONALITY TEST. IDENTIFICATION OF A CONSTITUTIONALLY VALID PURPOSE. Record 2013143

32 United Nations. General Assembly. (2014). Resolution A/HRC/27/37. The right to privacy in the digital age. para. 24.

33 IACHR. (2013). Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression. Available at: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&IID=2

34 IACHR. Case of Members of the José Alvear Restrepo Lawyers' Collective v. Colombia, Judgment of October 18, 2023, Preliminary Objections, Merits, Reparations, and Costs. Para. 533.

35 Ibid., para. 532.

2. Appropriateness of the measure

Secondly, the *suitability* stage determines whether the contested measure is appropriate for achieving the objectives pursued by the legislature or authority.[36] In other words, there must be a relationship between the restriction on the right and the objective pursued by that interference.

The examination of suitability involves corroborating a causal link between the authority's measure and its immediate purpose. The Supreme Court of Justice of Mexico has stated that this causal connection between the means and the end "must be established with empirical premises obtained from general knowledge accepted in society and specialized knowledge of science and technology".[37]

3. Necessity of the measure

Communications surveillance should only be carried out when it is the only means of achieving a legitimate objective, or when, among several means, it is the least likely to violate human rights. The burden of establishing this justification, both in judicial and legislative proceedings, lies with the State.

The second step in assessing necessity is to analyze whether the proposed measure is the least harmful option. In other words, when surveillance measures involve the mass and indiscriminate collection and storage of information on the private communications of, for example, millions of users of telecommunications and online financial services, the vast majority of whom will never be involved in criminal activity, the principle of necessity must lead to an assessment of whether there are measures that are less harmful to the rights of individuals who are not linked to the investigation in question, in order to achieve the intended purpose.

4. Study of the strict proportionality of the measure

This analysis requires comparing the degree of interference or limitation of privacy that the measure in question entails, assessed against the extent to which the intended purpose is achieved. The degree of impact is exacerbated by the fact that surveillance measures tend to involve the massive and indiscriminate collection of information from millions of people, the vast majority of whom will never be involved in the investigation of any criminal offense. The use of communications surveillance tools for crime prevention purposes is therefore disproportionate.[38] Furthermore, the information retained for this purpose is often excessive in comparison with the threat being addressed.

According to the IACHR, a measure that interferes with a right can only be considered *necessary* if there is no other alternative measure that is less harmful to the right in order to achieve the legitimate objective[39], and *proportional* if the impact on the human right is not excessive or disproportionate to the advantages obtained through such limitation.[40]

---

36 SCJN. Amparo in review 237/2014. Presiding judge: Arturo Zaldívar Lelo de Larrea. Approved by majority vote. This precedent gave rise to Isolated Thesis 1a. CCLXVIII/2016 (10a.) "SECOND STAGE OF THE PROPORTIONALITY TEST. EXAMINATION OF THE SUITABILITY OF THE LEGISLATIVE MEASURE." Registration: 2013152.

37 SCJN. Amparo in Review 163/2018 Citing [1] Bernal Pulido, Carlos, The Principle of Proportionality and Fundamental Rights, 2nd ed., Madrid, CEPC, 2005, p. 727.

38 SURVEILLE. (2015). "Surveillance: Ethical Issues, Legal Limitations, and Efficiency". Available at: https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.10-Synthesis-report-from-WP4.pdf p. 22

39 IACHR. (2008). Case of Kimel v. Argentina, Judgment of May 2, 2008, Series C No. 177, para. 74.

40 Ibid., para. 83.

The importance of effective safeguards against the abuse of covert electronic surveillance measures has also been highlighted by the United Nations General Assembly,[41] the UN Special Rapporteur on the Right to Freedom of Expression and Opinion,[42] the Office of the UN High Commissioner for Human Rights,[43] RELE, [44] as well as by civil society organizations and experts who have gathered best practices derived from jurisprudence and comparative doctrine and have developed the International Principles on the Application of Human Rights to Communications Surveillance.[45]

III. Safeguards

Additional safeguards include (i) judicial oversight, (ii) transparency and independent supervision, and (iii) notification to individuals affected by state surveillance measures.

1. Judicial oversight

One of the fundamental safeguards to inhibit the risks of abuse of covert surveillance measures is judicial oversight. The fundamental importance of judicial oversight, whether prior or immediate, has been highlighted by the RELE:

> Decisions to carry out surveillance tasks that invade people's privacy *must be authorized by independent judicial authorities, who must explain why the measure is appropriate* to achieve the objectives pursued in the specific case; whether it is sufficiently restricted so as not to affect the right involved more than necessary; and whether it is proportionate to the interest to be promoted.[46]

Similarly, the IACHR has established that it is essential that judicial authorities to be responsible for authorizing "invasive measures for gathering information," that is, methods of obtaining information such as electronic listening and recording, including audiovisual recording, as well as requests by intelligence agencies for personal data from telecommunications companies, for which judicial authorization must be required.[47]

The IACHR also recognizes that the right to privacy requires specific guarantees regarding the use of new technologies in intelligence activities. Therefore, prior judicial authorization is essential for the use of surveillance methods targeting specific individuals, especially if it involves accessing private databases and information systems containing personal data, tracking users online, or locating electronic devices.[48]

---

41 United Nations. General Assembly. (2013). Resolution A/RES/68/167 on the right to privacy in the digital age. Available at: https://docs.un.org/es/A/RES/68/167

42

43 United Nations. General Assembly. (2014). Resolution A/HRC/27/37. The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights. Para. 37. Available at: https://docs.un.org/es/A/HRC/27/37: "Article 17, paragraph 2, of the International Covenant on Civil and Political Rights establishes that everyone has the right to protection by the law against unlawful or arbitrary interference or attacks on their privacy (...) Internal safeguards, without independent external monitoring, have proven to be particularly ineffective against illegal or arbitrary surveillance methods. While these safeguards can take a variety of forms, the involvement of all levels of government in the oversight of surveillance programs, together with oversight by an independent civilian agency, is essential to ensure effective protection under the law."

44 IACHR. (2013). Special Rapporteur for Freedom of Expression, Freedom of Expression and the Internet, December 31, 2013, OEA/Ser.L/V/II.

45 See: International Principles on the Application of Human Rights to Communications Surveillance. Available at: https://es.necessaryandproportionate.org/text

46 IACHR. Special Rapporteur for Freedom of Expression, Freedom of Expression and the Internet. (2013). OEA/Ser.L/V/II, para. 165.

47 Inter-American Court of Human Rights. (2023). Case of Members of the José Alvear Restrepo Lawyers' Collective vs. Colombia, Judgment of October 18, 2023, Preliminary Objections, Merits, Reparations, and Costs, paras. 542, 547, and 551.

48 Ibid., para. 553.

In the same way, it reinforces the notion of special protection required for information obtained and classified as "sensitive data," which includes data affecting the most intimate aspects of individuals that may reveal aspects such as health, sexual orientation, religious, philosophical, political, or moral beliefs, affiliations, genetic data, biometric data, financial data, or data related to minors and personal geolocation. This data allows for the creation of detailed profiles and, due to its impact and potential to discriminate against its owner, requires enhanced protection.[49]

Likewise, other safeguards have been recognized as essential to mitigate the inherent risks of abuse of surveillance measures, such as transparency measures and independent supervision, or the right of notification to the affected party.

2. Transparency measures and independent oversight

The RELE has stated that "States must establish independent supervision mechanisms for the authorities responsible for carrying out surveillance tasks." [50]

The UN Special Rapporteur on the Right to Freedom of Opinion and Expression has recommended that States establish or maintain "effective independent national supervision mechanisms capable of ensuring transparency, where appropriate, and accountability for State surveillance of communications and the interception and collection of personal data."[51] It has also argued that States should make transparent requests for intervention or access to individuals' communications, their purpose and the investigation to which they relate, as well as the legal framework that legitimizes such surveillance and the procedures applied for this task. [52]

The IACHR has indicated that it is essential for the legal framework to provide for the existence of a civilian body that is independent of the Executive Branch and of the intelligence services themselves. This entity, which may be parliamentary, administrative, or judicial in nature, must have adequate technical expertise and the necessary powers to perform its functions, including full access to the information necessary to fulfill its role.[53]

3. Right to notification

Another fundamental safeguard to protect the right to privacy is the obligation of the authorities to notify a person that their privacy or personal data has been interfered with by means of covert surveillance. Although such notification may not be carried out in advance or immediately, as this could jeopardize the success of an investigation, it must occur when an investigation is no longer at risk, there is no risk of flight or destruction of evidence, and knowledge of the surveillance could pose an imminent risk to the life or personal integrity of any person.

This right to notify individuals affected by surveillance measures has been recognized, for example, by the UN Special Rapporteur on the right to freedom of opinion and expression, who stated that "in any case, once the surveillance has been completed and there is the possibility of seeking appropriate redress for the use of communications surveillance measures". [54]

---

49 Ibid., para. 554.

50 IACHR. Special Rapporteur for Freedom of Expression, Freedom of Expression and the Internet. (2013). OEA/Ser.L/V/II, para. 170

51 United Nations. General Assembly. (2014). Resolution A/RES/68/167 on the right to privacy in the digital age. Available at: https://docs.un.org/es/A/RES/68/167

52 United Nations. General Assembly. (2013). Resolution A/HRC/23/40. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Available at: https://docs.un.org/es/A/HRC/23/40

53 IACHR. Case of Members of the José Alvear Restrepo Lawyers' Collective v. Colombia, Judgment of October 18, 2023, Preliminary Objections, Merits, Reparations, and Costs. Para. 564..

54 Ídem.

The right to notification has also been recognized by the European Court of Human Rights (hereinafter ECHR), which determined in the case of Ekimdziev v. Bulgaria that once surveillance has ceased and the time strictly necessary for the legitimate purpose of the surveillance to be achieved has elapsed, notification to the affected person must be carried out without delay.[55]

In summary

The right to privacy and the protection of personal data are fundamental rights recognized by international human rights treaties and instruments. These rights extend to the realm of digital communications, including metadata or communications traffic data.

Consequently, for intelligence activities to be legitimate in a democratic State and compatible with human rights, restrictions on our rights (privacy, protection of personal data, among others) must:

- Be provided for in a law that is particularly precise, clear, and detailed by the legitimately empowered authorities, describing the procedure and circumstances in which communications surveillance measures may be carried out (principle of legality). Vague or ambiguous laws are incompatible with human rights, as they can be used in an arbitrary and abusive manner.
- Provide for a legitimate purpose;
- Maintain a causal relationship with the legitimate purpose (principle of suitability); that is, the restriction of our privacy and protection of personal data must be connected to the safeguarding of public or national security;
- There must be no more effective or less rights-infringing measures available (principle of necessity);
- Nor should the degree of impact on our rights be greater than that of implementing the measure (principle of proportionality).

In this regard, mass and indiscriminate surveillance of communications is particularly problematic, as it affects people who are not involved in the commission of any crime.

In addition, adequate safeguards must be established to prevent, avoid, and remedy abuses, such as:

- Prior judicial oversight, to ensure that surveillance measures are authorized by independent judges who serve as a counterweight in analyzing whether the measures complied with the principles of legality, necessity, and proportionality.
- Transparency and independent supervision, to ensure proper accountability for possible abuses in the acquisition and use of surveillance measures; and,
- The right to notification to affected persons, to ensure the right of access to justice, due process, and effective remedy for persons to challenge surveillance measures imposed against them.

55 ECHR. (2007). Case of the Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application No. 62540/00.

CHAPTER TWO: RULES AND PROCEDURES GOVERNING THE MONITORING OF COMMUNICATIONS

The countries covered by this investigation—Brazil,[56] Mexico,57 Colombia,[58] Chile,[59] Paraguay,[60] Peru,[61] and El Salvador[62]—have constitutional provisions enshrining the inviolability of communications and the protection of privacy and personal data.

Now, we will address the rules and procedures that regulate communications surveillance in the countries covered by the investigation, focusing on:

- The authorities in each country empowered to intercept private communications (with or without a court order),
- The circumstances and procedures under which communications may be intercepted, and,
- Fundamental safeguards for the prevention of abuse, arbitrariness, and discretion in surveillance measures.

1. Who, in what cases, and under what procedures can communications surveillance measures be carried out??

Authorities seeking prior or subsequent judicial authorization to intercept private communications must duly substantiate and justify their requests, specifying precisely and clearly the circumstances and procedures applied in each measure. As we shall see, the justification for the measure must satisfy criteria of necessity, proportionality, and, in some cases, evidentiary standards of probable cause.

---

56 The Federal Constitution of Brazil guarantees these rights in Article 5, section XII, which protects the inviolability of communications and correspondence, and in section LXXIX, which recognizes data protection as a fundamental right.

57 Article 16 of the Political Constitution of the United Mexican States recognizes the right to privacy by establishing that "no one may be disturbed in their person, family, home, papers, or possessions, except by virtue of a written order from the competent authority, which establishes and motivates the legal cause of the proceeding [...]". In addition, the second paragraph of Article 16 of the Constitution recognizes the right to the protection of personal data by recognizing that "every person has the right to the protection of their personal data, to access, rectify, and cancel it, as well as to express their opposition, under the terms established by law [...]". For their part, the twelfth and thirteenth paragraphs of Article 16 of the Constitution recognize the right to the inviolability of private communications.

58 Article 15 of the Political Constitution of the Republic of Colombia establishes that no interference in the private lives of individuals shall be made without a law determining the conditions for doing so and without judicial oversight. Similarly, Article 250 limits the authorities and timeframes in which the legal process for intercepting communications must occur.

59 Article 19 of the Chilean Constitution, amended in 2024, provides in its fourth paragraph for the protection of privacy and personal data.

60 Article 36 of the Constitution of the Republic of Paraguay guarantees the inviolability of private documents and communications. In this regard, documentary records (regardless of their format), correspondence, writings, and communications of any nature may not be examined, reproduced, intercepted, or seized, except by court order in cases specifically provided for by law, and when this is essential for the clarification of matters within the competence of the relevant authorities.

61 Article 10 of the Political Constitution of Peru guarantees the inviolability of private communications and documents. Communications, telecommunications, or their instruments may only be opened, seized, intercepted, or tapped by order of a judge, with the guarantees provided for by law.

62 Article 24 of the Constitution of the Republic of El Salvador recognizes that correspondence of all kinds is inviolable. It also prohibits interference with and interception of telephone communications.

Table 1. Authorities empowered by country to intercept communications (with or without a court order) and circumstances and procedures under which communications may be intercepted

COUNTRY	EMPOWERED AUTHORITIES	CIRCUMSTANCES AND PROCEDURES UNDER WHICH COMMUNICATIONS MAY BE INTERCEPTED
Brazil	• The Brazilian Intelligence Agency (hereinafter ABIN) is the main state entity authorized to plan, execute, supervise, and control surveillance activities for intelligence purposes. ABIN does not have the prerogative to carry out interceptions without judicial authorization; however, it can access information obtained by other bodies of the Brazilian Intelligence System (Sisbin)[63] through cooperation mechanisms established in current legislation. • Regarding registration data, only law enforcement authorities and the Public Prosecutor's Office (hereinafter, MP) may request it without a court order.[64]	• The Telephone Interception Act allows for the violation of secrecy and the interception of communications when there is reasonable evidence of authorship or participation in a crime punishable by imprisonment.[65] • Furthermore, the Code of Criminal Procedure requires a statement of reasons and specific evidence to justify "the breach of secrecy";[66] and, • The Telephone Interception Act prohibits surveillance for an indefinite period. Judicial authorization must be justified and limited to a maximum period of 15 days. This period may be renewed if justified.[67]
Chile	• The Public Prosecutor's Office, with the prior authorization of a court of law that assesses the suitability, necessity, and proportionality of the measure.[68] • Intelligence agencies' directives with prior judicial authorization.[69]	The interception of communications,[70] understood as those that "simulate telecommunications transmission systems,"[71] and remote access to computer equipment[72] must meet the following requirements of origin • There must be "reasonable suspicion," based on specific facts that a person has committed or participated in the preparation/commission of a crime.[73] • Factual and legal circumstances referring to specific crimes and specific individuals must be stated; and, • It must be determined as "strictly indispensable" when there is no other investigative measure to achieve the end pursued by the authorities.[74]

63 ABIN is part of Sisbin, which comprises various federal public administration bodies responsible for producing information relevant to intelligence activities. Sisbin's operations are regulated by Law No. 9,883/99 and Decree No. 11,693/23.

64 As provided for in specific regulations: the Criminal Organizations Act (Act No. 12,850/2013), the Money Laundering Crimes Act (Law No. 9,613/1998) and the Code of Criminal Procedure (Art. 13-A), which limits this possibility to investigations of crimes such as kidnapping, human trafficking, extortion, and the irregular sending of children or adolescents abroad.

65 Telephone Interception Law, Law No. 9,296/1996, Article 2, 1.

66 Code of Criminal Procedure, Article 13-B.

67 Telephone Interception Act, Section 8-A.

68 Criminal Procedure Code, Article 222.

69 Law 19974 on the state intelligence system and creates the national intelligence agency, articles 24 and 25.

70 Duration of the order: For the interception of communications, a period not exceeding 60 days, extendable for equal periods.

71 Duration of the order: 30 days, extendable for periods of up to the same duration. In the case of measures that "simulate telecommunications transmission systems", technical measures are included to preserve the integrity of the content and security, to prevent unauthorized access, as well as a deadline for its destruction.

72 Duration of the order: A maximum period of 30 days, extendable for periods of equal duration up to a maximum of 60 days.

73 Criminal Procedure Code, Article 222.

74 Law 19974 on the state intelligence system and creates the national intelligence agency, articles 24 and 25.

COUNTRY	EMPOWERED AUTHORITIES	CIRCUMSTANCES AND PROCEDURES UNDER WHICH COMMUNICATIONS MAY BE INTERCEPTED
Colombia	• The Public Prosecutor's Office;[75] • Judicial Police Authorities;[76] • Military Forces and National Police;[77] and, • National Intelligence Directorate.	• To investigate crimes and prosecute alleged offenders before competent courts and tribunals; • To carry out intelligence and counterintelligence activities, in which the Armed Forces and the National Police are the only authorized entities; and, • The Prosecutor's Office may order the judicial police to retain, seize, or recover information and have it analyzed by computer forensic experts so that it may be used as evidence.[78]
El Salvador	The Attorney General of the Republic and the Director of the Intervention Center are the authorities empowered to request the interception of telecommunications, either directly or through a delegate appointed by them, who must belong to the Center and meet the same requirements as those required by this law to serve as Director.[79]	• For the investigation, there must be a procedure for investigating a criminal act; and, • Among the elements of the trial, investigations must indicate the existence of reasonable evidence that a criminal act established by law has been committed, is being committed, or is about to be committed.[80]
México	• The National Guard, empowered by the National Guard Act (hereinafter, LGN); • The Public Prosecutor's Office, empowered by the National Code of Criminal Procedure (hereinafter, CNPP); and, • The Public Prosecutor's Offices of the 32 federal entities, empowered by the CNPP. • However, a reform to the National Guard Law— introduced in June 2025— proposes empowering the Secretariat of National Defense (SEDENA) to process and use information for intelligence activities for national security reasons.	• The LGN establishes a standard of necessity for communication surveillance measures, confirming the existence of sufficient evidence to prove that crimes are being organized.[81] • Article 16 of the Constitution requires that authorities seeking authorization from federal judicial authorities to intercept private communications must provide legal grounds and justify their requests. • When the head of the Public Prosecutor's Office "considers it necessary" to intervene in an investigation file for the commission of a crime.[82] • The National Security Act establishes the standard of necessity, requiring compliance with the requirement of imminence of threats to national security, described in the law.[83]
Paraguay	The Public Prosecutor's Office and the National Police, through a court order and due process, may intercept communications.[84]	Communications interception will be exceptional.[85]

75 Political Constitution - Article 250. Law 906 of 2004 (Amended by Article 52 Law 1453-2011) Decree 1704-2012 Article 235.

76 Article 235 of Law 906 of 2004 states that the competent authorities are responsible for the technical operation of interception, but does not explicitly determine which authorities are competent. However, Constitutional Court ruling C-594/14 indicates that Article 46 of Law 938-2004 "states that such competence lies with the judicial police authorities."

77 Law 1621-2013 - Article 3.

78 Law 906 of 2004 (Amended by Article 53 of Law 1453-2011) Article 236.

79 Special Law on Telecommunications Interception, as amended. Decree No. 552, Article 7.

80 Ibid., Article 6.

81 National Guard Law, Articles 100 and 103.

82 National Code of Criminal Procedure, Article 291.

83 National Security Act, Articles 5, 33, and 35.

84 Criminal Procedure Code, Articles 198, 199, 200, and 228. Duration of the order: 6 months, extendable once for the same duration.

85 Criminal Procedure Code - Article 200.

COUNTRY	EMPOWERED AUTHORITIES	CIRCUMSTANCES AND PROCEDURES UNDER WHICH COMMUNICATIONS MAY BE INTERCEPTED
Perú	• The Peruvian National Police (hereinafter, PNP) may intervene, without a court order, when it is solely a matter of accessing geolocation metadata.[86] • The Public Prosecutor's Office (hereinafter, MP)must have a court order and legal guarantees,[87] acting under judicial supervision. • Supervisory Agency for Private Investment in Telecommunications (hereinafter, OSIPTEL).[88]	• The PNP may request geolocation data in cases of crimes committed in flagrante delicto;[89] • The Prosecutor's Office may intercept private communications and documents in cases of serious crimes (corruption, terrorism, kidnapping, money laundering, among others);[90] and, • OSIPTEL may request mobile operators to provide real-time access to technical and geolocation data from the device in order to verify the quality of the mobile Internet service.[91]

Source: Own elaboration based on information provided by AlSur organizations

II. Fundamental safeguards

The following section presents information regarding the safeguards identified by country. These guarantees are essential for preventing abuse, arbitrariness, and discretion on the part of the authorities.

In **Brazil**, judicial authorization is required to obtain metadata and geolocation data on individuals.[92] The law provides for habeas data proceedings, which allow citizens to access information about themselves in official records or request its correction.[93] It is also possible to bring civil or criminal proceedings against abuses or illegalities committed in the execution of surveillance measures. Exceptionally, if the court before which the surveillance order is brought does not rule within 12 hours, the Prosecutor's Office or a police officer may request geolocation data and metadata directly from telecommunications and telematics companies.[94]

In **Chile**, communications between Lawyers and Defendants are exempt from interception measures, and internet service providers are required to destroy their subscribers' data once the maximum storage period for such information has elapsed.[95] The affected person must also be notified of the interception measure once it has been executed. [96]

In **Colombia**, no interference in people's private lives will take place without a law determining the conditions for doing so and without judicial oversight.[97] The authorities and timeframes for the legal process for intercepting communications are limited.[98] Intelligence activities shall be limited by "respect for human rights and strict compliance with the Constitution, the Law, International Humanitarian Law, and International Human Rights Law". [99]

---

86 Legislative Decree No. 1182 – Article 4.3

87 Political Constitution of Peru Article 2.10, Law No. 27697 Articles 1 and 2, Criminal Procedure Code (Legislative Decree No. 957) Article 230.

88 OSIPTEL Resolution No. 137-2021-CD - Article 4.

89 Legislative Decree No. 1182 – Article 4.3

90 Law No. 27697 – Articles 1 and 2

91 OSIPTEL Resolution No. 137-2021-CD - Article 4.

92 In accordance with Article 10, § 1 of the Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014) and Article 13-B of the Code of Criminal Procedure.

93 Federal Constitution of the Federative Republic of Brazil, Article 5, Section LXXII.

94 Article 13-B, §4 of the CCP.

95 Criminal Procedure Code, Article 222.

96 Ibid., Article 224.

97 Political Constitution of the Republic of Colombia, Article 15.

98 Ibid., Article 250.

99 Law 1621 of 2013, Article 4.

Likewise, and exceptionally, communications between the accused and their lawyer may be intercepted with a well-founded judicial authorization indicating specific facts linking the lawyer to the crime under investigation.[100]

In **El Salvador**, telecommunications may be intercepted on a temporary and exceptional basis with judicial authorization.[101] In exceptional cases, the judicial decision may be appealed by the prosecutor, who must justify the grounds for the appeal. The judge must refer the case without further proceedings to the competent Chamber. The Chamber shall decide on the appeal based solely on the case file, within the shortest possible time, which shall not exceed 24 hours from receipt.[102]

In **Mexico**,[103] Article 16 of the Constitution establishes, first, the need for federal judicial authorization to carry out the interception of private communications,[104] a requirement that is also reproduced by the CNPP for the access to real-time geolocation data and access to retained data.[105] Second, the interception of communications is prohibited in electoral, fiscal, commercial, civil, labor, or administrative matters, as well as in the case of communications between a detainee and their legal counsel.

There are several exceptions whereby the Prosecutor's Office may order access to geolocation data or data stored by telecommunications companies without prior judicial authorization when the physical integrity or life of a person is in danger, or the object of the crime is at risk, as well as in cases related to unlawful deprivation of liberty, kidnapping, extortion, or organized crime.[106] However, there is an obligation to inform the supervisory judge within 48 hours of the request being made, so that the judicial authority can ratify the measure in whole or in part or revoke it.[107] And in the case of geographic location data retained by credit institutions, the Administrative Provisions governing the retention and delive ry of such data do not require any judicial oversight.[108]

In **Paraguay**, the interception of communications requires a well-founded decision by a judge;[109] and the inviolability of the secrecy of correspondence carried out by telecommunications services and documentary heritage is provided for, except when there is a court order.[110] Exceptionally, both the judge and the Prosecutor's Office are granted the power to request reports from public or private individuals or entities.[111] Such reports may be requested verbally or in writing, including details of the procedure, the name of the accused, the place of delivery of the report, the deadline for its submission, and the consequences of non-compliance. This facilitates access to data held by telecommunications companies without judicial oversight.

---

100 Criminal Procedure Code, Article 222.

101 Political Constitution of the Republic of El Salvador, Article 24, and Special Law for the Intervention of Telecommunications, with its amendments. Decree No. 552, Article 8.

102 Special Law on Telecommunications Interception, as amended. Decree No. 552, Article 11.

103 It should be noted that as of June 2025, the date of completion of this report, various laws are in the process of being approved in Mexico that seek both to reform the exception mechanism—to expand the circumstances in which judicial authorization can be circumvented—and to establish that intelligence authorities (including the Army) may request, without any safeguards, unrestricted and direct access to any public or private record, as well as to a Single Identity Platform that will contain the biometric identification of all individuals as a requirement for accessing any type of service.

104 Political Constitution of the United Mexican States, Article 16.

105 National Guard Law, Article 9, Section XXVI, and the National Code of Criminal Procedure.

106 National Code of Criminal Procedure, Article 303.

107 Idem, Article 303.

108 Ministry of Finance and Public Credit, General provisions referred to in Article 115 of the Credit Institutions Law.

109 Criminal Procedure Code, Article 200.

110 Telecommunications Law No. 642/95, Article 89.

111 Criminal Procedure Code, Article 228.

In **Peru**, communications can only be intercepted with a reasoned court order. The court authorization must be substantiated, specify the type of communication, be limited in time, and unrelated information must be kept confidential.[112] Furthermore, the interception of private communications is only permitted in cases of serious crimes (corruption, terrorism, money laundering, etc.).[113] Once the interception has ended, the affected party must be notified and may challenge the decision in court.[114] Furthermore, habeas corpus may be invoked in cases of unlawful interception affecting personal freedom,[115] and habeas data may be invoked in cases of unlawful processing of personal data or violation of privacy.[116]

Exceptionally, and in the case of geolocation data, the police may access this information without a prior court order for certain types of crimes. This access must then be validated at the judicial level. In this regard, telecommunications operators must store geolocation data for a minimum period of one (1) year, with the possibility of extending this obligation for up to two (2) additional years.[117]

In summary

ON THE AUTHORITIES EMPOWERED TO INTERCEPT COMMUNICATIONS, CIRCUMSTANCES AND PROCEDURES FOR DOING SO

Although most regional legal frameworks provide for general requirements regarding justification and grounds, the clarity and precision of the circumstances and procedures for carrying out surveillance measures varies within the regional legal framework.

For example, in **Brazil**, the interception of private communications requires *"reasonable grounds"* for the commission of a crime, based on concrete evidence and within a specific time frame; in **Chile**, it requires *"well-founded suspicions,"* based on factual and legal circumstances relating to specific crimes and specific individuals;

In **Colombia**, it is generally considered that private communications may be intercepted *"to investigate crimes and prosecute alleged offenders,"* as well as *"to carry out intelligence and counterintelligence activities."*

Both legislations contain very broad, subjective, and ambiguous criteria that violate the principle of legality, leaving us defenseless by failing to limit and restrict the actions of the authorities in order to prevent arbitrary, capricious, or abusive interference in the legal sphere of individuals. In **El Salvador**, there must be reasonable evidence that a criminal act has been committed, is being committed, or is about to be committed.

Countries such as **Peru**, on the other hand, base the justification for such measures on the category of crimes being investigated, i.e., crimes committed in flagrante delicto and serious crimes, such as corruption, terrorism, kidnapping, or money laundering.

However, although the rules described above suggest a general requirement for justification and motivation, including the verification of objective elements that justify their necessity and proportionality, their application is doubtful both in the development of specific rules of origin in other secondary laws, and in practice.

---

112 Political Constitution of Peru, Article 2.10.
113 Up to 60 days, extendable. Articles 1, 2.7, and 2.8 Law No. 27697.
114 Criminal Procedure Code, Articles 231.3 and 228.
115 Political Constitution of Peru, Article 200.1.
116 Idem, Article 200.3
117 Legislative Decree No. 1182, Articles 3 and Second Final Complementary Provision.

On the other hand, although most laws establish which authorities are empowered to intercept communications, we have detected regional legal uncertainty due to the use of vague or generic terms regarding the circumstances in which these authorities may use surveillance measures.

For example, in **Mexico**, Prosecutors may order the interception of communications when they *"deem it necessary"* as part of a criminal investigation.

ON SAFEGUARDS FOR THE PREVENTION, IDENTIFICATION, AND REDRESS OF UNLAWFUL SURVEILLANCE MEASURES

Most countries covered by this research establish the need for abprior judicial oversight for the interception of private communications. However, some countries in the region provide for concerning exceptions that allow such oversight to be bypassed.

For example, in **Brazil**, if the court does not rule within 12 hours, the Prosecutor's Office or a police officer may request the data directly from telecommunications and telematics companies. Similarly, in **Mexico**, the exceptional mechanism established in Article 303 of the National Code of Criminal Procedure allows prosecutors to request access to stored data or real-time geolocation from telecommunications companies without first obtaining judicial authorization, where the exception has become the general rule and a significant number of requests made under the exceptional mechanism are not ratified by the judicial authority.

Likewise, in **Paraguay**, both judges and the Prosecutor's Office are granted the power to request reports from individuals or public or private entities without judicial authorization; and in **Colombia**, the use of communications data in criminal investigations[118] and for intelligence purposes[119] does not impose an obligation of judicial control.

In this regard, it should be emphasized that circumventing judicial oversight of surveillance measures encourages abuse by removing necessary checks and balances, prevents the detection of such abuse, and allows for impunity, which encourages its chronic repetition. Therefore, it is necessary for legal frameworks to clearly detail the need for prior or immediate federal judicial oversight of all surveillance measures recognized by their legal frameworks, without exceptional mechanisms that allow the evasion of this requirement.

On the other hand, it is observed that some legal frameworks, such as those of **Brazil** and **Peru**, provide for additional safeguards for the exercise of the right to personal data protection—such as habeas data—as well as the mention of habeas corpus as an effective remedy against cases of abuse.

It is also noteworthy that the legal frameworks of **Chile** and **Peru** recognize the right of notification to affected persons, granting an effective remedy of access to justice for individuals facing potential abuses of surveillance measures. However, it remains to be analyzed—especially considering the lack of transparency that prevails in the use of such surveillance measures—in how many cases this safeguard has been effectively implemented practice.

118 Decree No. 1704 of 2012.

119 Law 1621 of 2013, Article 44.

Chile is one of the most protective countries in terms of its legal framework, expressly establishing an exception for the interception of communications between lawyers and defendants (as in **Mexico**) and ordering internet service providers to destroy their subscribers' data once the maximum storage period for such information has expired.

It should be noted that **none of the countries in the region contemplates statistical transparency measures or independent supervision** regarding the use and scope of the powers and techniques of communications surveillance employed. In this regard, one of the main problems in analyzing this type of measure is that we do not have sufficient information to understand the scope, nature, and application of laws that allow for communications surveillance.

On the contrary, authorization often falls to a hierarchical superior within the same requesting institution. This situation can be observed, for example, in access to information by the ABIN and police forces in Brazil; the National Guard Law in Mexico; the PNP and OSIPTEL in Peru; and the Armed Forces, National Police, and National Intelligence Directorate in Colombia, which raises concerns due to the lack of separation between those who investigate and those who authorize the measure.

Therefore, legal frameworks must provide for a civilian institution that is independent of the intelligence services and the Executive Branch, with technical expertise, to oversee the empowered authorities, both in terms of their transparency obligations and in terms of accountability.

CHAPTER THREE: CASES OF COMMUNICATIONS SURVEILLANCE IN THE REGION BY TYPE OF SURVEILLANCE USED

The following chapter provides a brief summary of cases in which the use of some form of communications surveillance was detected, namely: **(I)** cases of interception of private communications in general terms, including: (a) collaboration with telecommunications companies; and (b) extraction of information; **(II)** the use of spyware; **(III)** geolocation based on the exploitation of vulnerabilities in telecommunications infrastructure (SS7); **(IV)** cyber patrols; and **(V)** surveillance of individuals through license plate reading systems.

For each case, a brief description is provided on the surveillance technique, the type of technology used, the authorities that used it, and the profile of the victims, in order to identify trends and patterns in the use of surveillance measures in Latin America.

Interception of private communications

Below are examples of the interception of private communications in general terms (in **Colombia** and **Chile**), as well as specific examples of: (a) the collaboration of telecommunications companies in accessing retained data records (in **Paraguay**, **Chile**, and **Mexico**); and (b) the extraction of information.

It should be noted that the scope of what should be understood as private communications has been expanding with the evolution and dynamic nature of technology, and that various courts have interpreted that communications traffic data or metadata are also protected by the right to the inviolability of communications. Consequently, the sole purpose of the division made is to better visualize the different ways of intercepting private communications.

In this regard, with respect to this surveillance technique, a broad definition of the concept of private communications interception is contemplated, which encompasses all types of information and both the content of the communications themselves and the metadata, also referred to as communications traffic data. In turn, it is understood that the concept covers both access and the recording, collection, and storage of information, both in real time and after the communication process has taken place.120

It is also specified that the interception of communications, even when based on powers conferred by law, can give rise to abuses in its application, as well as to the use of technologies that violate the right to privacy.

Below are two emblematic cases, in general terms, of the interception of private communications in **Colombia** and **Chile**.

120 The legal definition in Article 34, paragraph 2, of Mexico's National Security Law was taken into account.

COLOMBIA

A report by *Semana magazine*[121] revealed that, from December 2019 to February 2020, the National Army carried out espionage activities using a "computer monitoring program" designed to carry out 'profiling' and "special tasks"[122] by collecting personal information on more than 130 people.[123] Among those affected were journalists, former ministers, presidential officials, generals, politicians, trade unionists, and US journalists.

This illegal surveillance was carried out by the National Army through its cyber intelligence battalions (hereinafter, "Bacib").[124] An important indicator of the irregularities were the alerts issued by US intelligence agencies, which reported having identified the illegal use of technical equipment that they themselves had donated to the Colombian Army.

In 2019, the Ministry of Defense, under the National Army, acquired the Hombre Invisible software,[125] which was supplied by the Spanish company *Mollitiam Industries*.[126] The purpose of the contract was the "acquisition of the penetration suite platform for the development of activities carried out in the field of active cyber defense by the National Army." To date, information about the contract is not publicly accessible on the government procurement website.

Following the publication of *Semana magazine*, the Foundation for Press Freedom (hereinafter, "FLIP") documented and identified a total of 52 cases of journalists illegally monitored by the National Army as of June 2020.[127] FLIP also submitted a request to the Prosecutor's Office (hereinafter, "FGN") for more information on the case. According to the statement, the FGN stated that there were not "130 targets of illegal monitoring, surveillance, interception, profiling, and special operations by the National Army, but rather a number of people not exceeding 20".[128]

---

121 Semana. (2020). Espionage by the National Army: The secret files.
Available at: https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/

122 According to the terminology used by the military.

123 For example, phone numbers, home and work addresses, email addresses, friends, family members, children, colleagues, contacts, traffic violations, and even polling places—for various individuals.

124 These "belong to the military intelligence brigades and the Information Security Counterintelligence Battalion (Bacsi). Both report to the Military Intelligence Support Command (Caimi) and the Military Counterintelligence Support Command (Cacim)".

During December 2019, Carlos Holmes Trujillo was Minister of Defense and Nicacio Martínez was commander of the Army. The former was Minister of Defense during the early years of Iván Duque's administration, while the latter was former commander of the Army who announced his retirement at the same time that the Supreme Court of Justice raided that entity. By May 2020, when Semana published its article on the so-called "secret files," the commander of the Army was Eduardo Zapateiro. According to *Semana magazine*, these changes in command were related to the discovery of irregularities in digital surveillance carried out by the Army in late 2019.

125 Rico, M. (February 20, 2023). Mollitiam: this is the Army contractor and its cyber espionage tools.
Available at: https://www.elespectador.com/judicial/mollitiam-asi-es-la-contratista-del-ejercito-y-sus-herramientas-de-ciberespionaje/

126 *Mollitiam Industries*. https://www.mollitiamindustries.com/ (Contract awarded through process No. 277-CENAINTELIGENCIA 2019).

127 Foundation for Press Freedom (FLIP). (2020). Fourteen new cases of journalists who were victims of profiling by the National Army.
Available at: https://flip.org.co/en/pronunciamientos/catorce-nuevos-casos-de-periodistas-que-fueron-victimas-de-acciones-de-perfilamiento-por-parte-del-ejercito-nacional

128 Foundation for Press Freedom. (2020). Four months after the secret files.
Available at: https://flip.org.co/en/pronunciamientos/cuatro-meses-despues-de-las-carpetas-secretas

Following the publication of the complaint in the magazine, some victims reported experiencing violence or reprisals related to the case. One example was the journalists from *Rutas del Conflicto* (hereinafter "RdC"), a journalism project that documents events related to the armed conflict in the country. According to Óscar Parra, a member of the RdC team, despite having no evidence linking the events, they believe that the start of their "profiling" as an organization began following an information request submitted to the National Army as part of an investigation conducted by RdC in 2019.[129]

According to O. Parra, after submitting the request and having to insist through legal channels, two military officers showed up at the organization's office to respond in person, avoiding responding by physical or digital mail. The officers remained outside the building that same day.

In light of what happened, Parra described this as intimidation, which they reported to the judge handling the case, who ultimately ordered the Army to provide the relevant information. Similarly, General Nicacio Martínez filed a constitutional protection action[130] against the same journalist, arguing that RdC was discrediting the Army. The court ruled in favor of RdC and closed the case.

Although this is one of the few reports related to any type of reprisal in addition to the surveillance measures denounced by *Semana magazine*, it is important to highlight that journalists in Colombia are constantly targeted by these illegal surveillance actions and their right to freedom of expression and privacy are violated more frequently than those of other sectors. Since 2019, FLIP has documented a high number of attacks against journalists, with a sustained trend of between 400 and 500 attacks per year in Colombia.[131]

Following the exposure of the unlawful surveillance activities, two investigations were launched—one by the Office of the Inspector General (hereinafter, PGN) and another by the Public Prosecutor's Office (hereinafter, FGN). According to the newspaper El Espectador,[132] by 2021, the investigation led by the PGN was the most advanced, having "ordered formal charges against military personnel based on evidence regarding the equipment used, the individuals involved, the orders issued, and the recovered information".[133]

However, in February 2021, the same media outlet reported that the investigations by both entities did not agree on the number of victims of these illegal actions. It also indicated that, as of that date, *"there was no information on the progress of the disciplinary proceedings and the formulation of charges brought by the Inspector General's Office against thirteen military personnel, nor on the public hearing that was supposed to take place."* [134]

---

129 Abu Shihab, L. (May 5, 2020). We spoke with one of the victims of espionage by the Colombian Army. VICE. https://www.vice.com/es/article/nuevo-escandalo-en-colombia-por-seguimientos-ilegales-del-ejercito-a-periodistas-politicos-y-defensores-de-derechos-humanos/

130 The action of constitutional protection is a mechanism established in Article 86 of the Political Constitution of the Republic of Colombia. The action consists of the power that every person has to claim before a judge, at any time and place, through a preferential and summary procedure, the immediate judicial protection of their fundamental constitutional rights.

131 El Colombiano. (2024). Violence against journalists is disguised as the right of those in power to debate. Available at: https://www.elcolombiano.com/colombia/la-violencia-contra-los-periodistas-se-disfraza-como-el-derecho-a-debatir-de-los-gobernantes-flip-OH23715128

132 El Espectador. (2021). "Secret files": After the complaint, silence. Available at: https://www.elespectador.com/judicial/carpetas-secretas-despues-de-la-denuncia-el-silencio-article/

133 This was ordered on May 20, 2020, against thirteen military officers, including Generals Eduardo Quirós and Gonzalo Ernesto García, who will face disciplinary proceedings in the Office of the Inspector General. The latter was an official in the now-defunct Administrative Department of Security, which was dissolved after the wiretapping scandal during the Álvaro Uribe administration.

134 El Espectador. (2021). "Secret files": After the complaint, silence. Available at: https://www.elespectador.com/judicial/carpetas-secretas-despues-de-la-denuncia-el-silencio-article/

Apart from the measures taken by national entities, in October 2020, the IACHR convened a public hearing on the case.[135] "The Colombian State delegation, led by Alejandro Ordóñez, ambassador to the OAS, denied the systematic nature of these activities. He also stated that, as of the date of the hearing, "there were nine investigations open regarding these events, further denying the lack of participation of the victims." This hearing is not found in the IACHR's audiovisual records, and it is unclear which nine investigations Ordoñez was referring to. The following was emphasized at the hearing:

> The issue of illegal intelligence in Colombia [at that time] had occupied the IACHR for sixteen years, during which impunity and a lack of information about the content of these illegal activities persisted, as did a lack of clarification about the motivations and structure behind the interceptions and the repetition of the events.[136]

CHILE

In October 2019, it was revealed that thousands of intelligence files deployed by the Carabineros de Chile police force had been leaked, showing illegal surveillance of the communications of social leaders, human rights defenders, and trade unions in the country.[137]

The leaks, known as PacoLeaks,[138] were published on October 25, 26, and 28, 2019.[139] The third leak revealed data from more than 300 internal memos and 10,000 attachments from the Carabineros, with detailed information on the activities of social movements and trade unions,[140] as well as reports on the monitoring and surveillance of leaders and their organizations.[141] In this regard, it was evident that environmental movements and feminist groups are the main target of the Carabineros' intelligence work.

Although in this case it was not possible to identify the operator of the surveillance technology, developer, or intermediaries that enabled the extraction of the information, this leak of intelligence files revealed various surveillance and espionage mechanisms used by the police institution in question against social organizations. According to one of the sources consulted,[142] these mechanisms include: searching for activity and communication exchanges on social media, infiltrating events, on-site monitoring of protesters and leaders, first-person police photographic records, espionage via drones, and recognition files with personal data.

---

135 Colombian Commission of Jurists. (2020). IACHR reiterated that illegal surveillance in Colombia is systematic and called for guarantees for victims.
Available at: https://www.coljuristas.org/sala_de_prensa/cidh-reitero-que-la-vigilancia-ilegal-en-colombia-es-sistematica-y-pidio-garantias-para-las-victimas

136 Ibíd.

137 CIPER (2019). Hacking of Carabineros amid crisis exposes 10,515 files, including intelligence data.
Available at: https://www.ciperchile.cl/2019/10/29/hackeo-a-carabineros-en-medio-de-la-crisis-expone-10-515-archivos-entre-ellos-hay-datos-de-inteligencia/

138 Paco, a term widely used in Chile to refer to police officers.

139 La Izquierda Diario (2019). PACOLEAKS. Leaked police documents reveal surveillance of political and social organizations.
Available at: https://www.laizquierdadiario.com/Filtracion-de-documentos-de-Carabineros-revela-seguimientos-a-organizaciones-politicas-y-sociales

140 Legal strikes, collective bargaining, graffiti/painting protests, press conferences, or public events.

141 Interference (2019). PacoLeaks: These are the names and organizations that have been monitored by the Carabineros in recent months.
Available at: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

142 Doble Espacio (2019). From the Communist Youth to the Catholic University: organizations and institutions investigated by the Carabineros.
Available at: https://doble-espacio.uchile.cl/2019/11/04/desde-las-juventudes-comunistas-a-la-universidad-catolica-las-organizaciones-e-instituciones-investigadas-por-carabineros/

According to some media outlets,[143] among the social organizations, leaders, and human rights movements that appeared in the surveillance and intelligence documents were: unions and trade associations such as the Teachers' Association, the National Association of Fiscal Employees (hereinafter "ANEF"), Confusam, and the United Workers' Union (hereinafter "CUT"); student organizations such as the Federation of Students of the University of Chile (hereinafter "FECH") and the Federation of Students of the Arturo Prat University (hereinafter "FEDEUNAP"); and human rights groups such as the Association of Families of Disappeared Detainees (hereinafter "AFDD"), the Association of Families of Politically Executed Persons (hereinafter "AFEP") and the National Coordinator of Human and Social Rights Organizations. Also included are social and thematic movements such as No+AFP, Modatima, No a Ciclo, and the Movement for Water and Territories, as well as feminist groups such as the Chilean Network Against Violence Against Women, the Northern Women's Network, and the Voz en Fuga Collective.

In addition, files containing photographs, personal data, and, in some cases, detailed movements of social leaders classified as "targets of interest" [144] were disclosed, including Rodrigo Mundaca, leader of Modatima; Bárbara Figueroa, president of the CUT; Mario Aguilar, of the Teachers' Association; Luis Mesina, spokesperson for the No+AFP Coordinating Committee; and Emilia Schneider, interim president of the FECH.

Carabineros of Chile confirmed the authenticity of the leaked documents, justifying its actions under the Intelligence Law and the protection of public safety and physical integrity of those organizing social activities.[145]

In the case of the Modatima leader, the leaked information details the exact time of his arrival in Chile on October 1, 2019, after receiving the International Human Rights Award in Nuremberg, Germany. The leader said he received anonymous death threats on social media upon his arrival in the country.[146] For the environmental leader, the information from the Carabineros about his arrival in Chile:

> (...) confirms what we have been denouncing for a long time: there is coordinated action by state intelligence forces [...] to monitor our every move and keep us under constant surveillance, which violates fundamental human rights, the right to freedom, freedom of opinion, and the right to dissent.[147]

In addition to the above, Emilia Schneider, interim president of the FECH, stated that "it is worrying that we are being labeled as targets of interest, especially when we see leaders who have been assassinated, such as Macarena Valdés and Camilo Catrillanca".[148] After the leaks, several social organizations informed the media about the Carabineros' monitoring of activities that did not involve large crowds.

---

143 Interference (2019). PacoLeaks: These are the names and organizations that have been monitored by the Carabineros in recent months. Available at: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

144 Interference (2019). PacoLeaks: Carabineros created files on social leaders to keep them under surveillance. Available at: https://interferencia.cl/articulos/pacoleaks-carabineros-creo-fichas-de-lideres-sociales-para-mantenerlos-vigilados

145 Interference (2019). PacoLeaks: These are the names and organizations that have been monitored by the Carabineros in recent months. Available at: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

146 Interferencia (2020). Mundaca speaks out on the Supreme Court's rejection of his appeal in the 'Pacoleaks' case: "It's a vote of confidence in a police force that violates human rights. Available at: https://interferencia.cl/articulos/habla-mundaca-sobre-el-rechazo-de-la-suprema-su-amparo-por-pacoleaks-es-un-voto-de

147 Interferencia (2019). PacoLeaks: These are the names and organizations that have been monitored by the Carabineros in recent months. Available at: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

148 Interferencia (2019). PacoLeaks: Carabineros created files on social leaders to keep them under surveillance. Available at: https://interferencia.cl/articulos/pacoleaks-carabineros-creo-fichas-de-lideres-sociales-para-mantenerlos-vigilados

In 2019, following the leaks of intelligence files, multiple legal actions were initiated against the Carabineros and the Ministry of the Interior.[149] For example, the Teachers' Association filed a constitutional protection petition against the director general of the Carabineros, Mario Rozas, and the Minister of the Interior, Gonzalo Blumel.[150]

The request was rejected by the Santiago Court of Appeals on the following grounds:

> (...) in order for the evidence brought before the court to be considered, it must have been obtained legitimately and in accordance with the law; otherwise, it cannot be taken into consideration or validated in legal proceedings [...] this appeal is based on an unlawful act, namely the hacking and extraction of information from the Carabineros of Chile, in respect of which the affected institution has, as it has stated, filed the corresponding criminal complaint.[151]

The leader of Modatima also filed a petition for constitutional protection against the Director General of the Carabineros and the Minister of the Interior, requesting clarification on when the surveillance practices began and *"the purpose of analyzing what we do, what we think, and who we meet with."*[152] The Santiago Court of Appeals also rejected the petition for protection on the same grounds as in the case of the Teachers› Association. [153]

In the same sense, the Vice-Rector for Outreach and Communications at the University of Chile, the president of the Association of Families of Disappeared Detainees, the president of the FECH, and other activists filed a complaint against the Minister of the Interior and the Director General of the Carabineros for spying on them.[154] This complaint was also rejected on the grounds of previous cases regarding the origin of the evidence brought to the court's attention.[155]

149 Interferencia (2019). Social leaders under surveillance take legal action against Rozas and Blumel. Available at: https://interferencia.cl/articulos/dirigentes-sociales-vigilados-toman-acciones-legales-contra-rozas-y-blumel

150 For more information, see: https://juris.pjud.cl/busqueda/pagina_detalle_sentencia?k=eHFSeVBncXp0Z085dzhVU2M-veThnQT09

151 CHILEAN TEACHERS' ASSOCIATIONS A.G / CHILEAN POLICE - MINISTRY OF THE INTERIOR VISTA EN POS DEL ING. CORTE 2460-2019: 09-12-2019 (-), Case No. 2473-2019. In the Court of Appeals Search Engine. (https://juris.pjud.cl/busqueda/u?7ps0). Date of consultation: March 2025

152 Interference (2020). Mundaca speaks about the Supreme Court's rejection of his appeal in the 'Pacoleaks' case: "It is a vote of confidence in a police force that violates human rights.. Available at: https://interferencia.cl/articulos/habla-mundaca-sobre-el-rechazo-de-la-suprema-su-amparo-por-pacoleaks-es-un-voto-de

153 MUNDACA CABRERA RODRIGO / CHILEAN POLICE VISTA WITH ENG. CORTE 2319, 2362, 2460, 2473, 2507, 2512 AND 2682 ALL FROM 2019.-: 09-12-2019 (-), Case No. 2295-2019. In the Court of Appeals Search Engine. (https://juris.pjud.cl/busqueda/u?7psz). Date of consultation: March 2025

154 Interference (2019). Social leaders under surveillance take legal action against Rozas and Blumel. Available at: https://interferencia.cl/articulos/dirigentes-sociales-vigilados-toman-acciones-legales-contra-rozas-y-blumel

155 OLIVARES SAAVEDRA ROSARIO-ASTUDILLO ASTUDILLO LEANDRO-BARRA ARANCIBIA GUILLERMO-SCHNEIDER VIDELA EMILIA/MINISTRY OF THE INTERIOR AND PUBLIC SECURITY-CARABINEROS OF CHILE. HEARING IN THE CASE OF ENG. CORTE 2507-2019.-: 09-12-2019 (-), Case No. 2512-2019. In the Court of Appeals Search Engine. (https://juris.pjud.cl/busqueda/u?7hgt). Date of consultation: March 2025

II. Collaboration of telecommunications companies in access to retained data records

As noted by the then United Nations High Commissioner for Human Rights in his 2014 report on "The right to privacy in the digital age," both the content of communications and their metadata are protected by the right to privacy, as metadata can also reveal data about individuals' behavior and allow conclusions to be drawn about their private lives.[156]

In this regard, the retention and storage of communications metadata by telecommunications companies is often part of legislative and public policy measures on cooperation with the justice system, mainly to enable authorities to request access, subject to prior judicial authorization, for the purposes of preventing and investigating crimes.

However, most legal frameworks regulating such access do not clearly and precisely establish which authorities may access such personal data, under what circumstances, under what procedures, and with what safeguards. This is particularly concerning given that this practice involves the mass and indiscriminate retention of the personal data of millions of mobile phone users, most of whom are not, and will not be, involved in the commission of a crime.

In this regard, serious irregularities and abuses have been detected in the region with regard to access to such data. Examples of its use are provided below with documented cases in **Paraguay**, **Chile**, and **Mexico**.

PARAGUAY

In Paraguay, the Public Prosecutor's Office can request access to communications metadata held by Internet service providers without judicial authorization and without a formal charge or prior accusation, simply because it is investigating a case and considers it necessary.[157]

Currently, there are more than 20 cases before the Supreme Court of Paraguay challenging this procedure. However, since 2004, the Court has maintained its position, considering that metadata is not part of communications and, therefore, can be requested by the Prosecutor's Office without a court order.[158]

156 United Nations. General Assembly. (2014). Resolution A/HRC/27/37. The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights. Para. 19. Available at: https://docs.un.org/es/A/HRC/27/37

157 Based on Article 228 of the Criminal Procedure Code.

158 For more information, see the summary "Who defends your data" (all editions), where ISP TIGO provides the number of requests for reports made annually by the public prosecutor's office. See also: https://www.tedic.org/wp-content/uploads/2025/02/QDTD_Paraguay_2024-WEB.pdf

CHILE

In the context of the social and political unrest of 2019, the Western Metropolitan Prosecutor's Office of Chile[159] requested that internet service providers (ISPs) hand over data on mobile phone subscribers who were present near the burned-down metro stations.[160] The request demanded access to all phone numbers that connected to *Entel*, *Movistar*, and *WOM* antennas and cell towers between October 18 and 28 near five Metro stations located in western Santiago.[161]

The Prosecutor's Office submitted the request on two occasions, on November 4 and 12, 2019. In the first request, it asked the Special Police Investigation Brigade (hereinafter "BIPE") of the Chilean Investigative Police (hereinafter, "PDI") to *Entel*, *Movistar*, and *WOM* to provide information on the traffic of telephone antennas installed between the municipalities of Maipú and Pudahuel, where the attacks on Metro stations were recorded.

According to reports by *La Tercera*[162] media outlet, WOM was the only company that provided the information upon the first request, without a court order required by law[163] to authorize such disclosure. *Movistar* refused and *Entel* provided only partial information.

As a result of the above, a second request was issued, in which the Prosecutor's Office filed a petition before the Ninth Court of Guarantees of Santiago, asking the court to issue a general court order requiring *Entel* and *Movistar* to hand over the information requested by the Prosecutor's Office.[164] On November 12, the court ordered them to submit the data on all mobile phones that connected to the antennas of those telephone companies at the metro stations that were attacked.

In this regard, WOM issued a statement saying that:

> It requested greater precision in the request sent by the agency and, once the clarification was received, it proceeded to comply with the court order issued by the Public Prosecutor's Office. This information only refers to traffic on our antennas, which does not imply specific customer data.[165]

According to an inquiry made by CIPER Chile to the Prosecutor's Office in 2023,166 six people were convicted for the attacks on Metro stations in western Santiago. To date, no correlation has been established between their convictions and the Prosecutor's request for information from mobile phone companies.

---

159 BioBioChile (2020). Prosecutor's office requests data from mobile phone companies to identify those who attacked Metro stations. Available at: https://www.biobiochile.cl/noticias/ciencia-y-tecnologia/moviles-y-computacion/2020/01/08/afirman-que-wom-entrego-informacion-de-usuarios-durante-estallido-social-compania-se-defendio.shtml

160 The surveillance measures presented respond to a geofence case. This consists of a request by the authorities for the location and reverse identification data of people who were near certain Santiago Metro stations that had been burned down.

161 *La Tercera* (2019). Prosecutor's office requests cell phone tower data from the days when attacks on the Metro occurred. Available at: https://www.latercera.com/nacional/noticia/fiscalia-pide-levantar-informacion-antenas-celulares-dias-ocurrieron-ataques-al-metro/963909/

162 *La Tercera* (2020). WOM on providing information to prosecutors regarding Metro attack: "No specific customer data involved. Available at: https://www.latercera.com/nacional/noticia/wom-entrega-informacion-fiscalia-ataque-metro-no-implica-datos-especificos-los-clientes/966760/

163 Enacted in Article 19 of Law 21732.

164 *La Tercera* (2019). Prosecutor's office requests cell phone tower data from the days when attacks on the Metro occurred. Available at: https://www.latercera.com/nacional/noticia/fiscalia-pide-levantar-informacion-antenas-celulares-dias-ocurrieron-ataques-al-metro/963909/

165 *La Tercera* (2020). WOM on providing information to prosecutors regarding Metro attack: "No specific customer data involved. Available at: https://www.latercera.com/nacional/noticia/wom-entrega-informacion-fiscalia-ataque-metro-no-implica-datos-especificos-los-clientes/966760/

166 CIPER (2023). Prosecutor's office closes cases on attacks on the Metro: 14 people convicted and no organized groups found to have burned stations.
Available at: https://www.ciperchile.cl/2023/10/17/fiscalia-cerro-las-causas-por-ataques-al-metro-condeno-a-14-personas-y-no-detecto-grupos-organizados-para-quemar-estaciones/

MÉXICO

In Mexico, Article 190, Section II, of the Federal Telecommunications and Broadcasting Law (hereinafter, "LFTR")[167] establishes the obligation of telecommunications concessionaires to keep, for two years, a record of the communications metadata of all their users without discrimination. This record includes metadata such as: the origin and destination of communications; their date, time, and duration; identification data of the communicators and devices; and even the approximate geographical location of users.

Article 190, section III of the LFTR also establishes the obligation to deliver retained data to the authorities empowered to access such records. In this regard, in response to requests for access to information, R3D: Network in Defense of Digital Rights detected serious discrepancies between the number of accesses reported by the authorized authorities, the federal judiciary, and telecommunications companies, suggesting a widespread practice of illegal access to data retained by telecommunications companies.

In addition, there is evidence that the exceptional mechanism provided for in Article 303 of the CNPP, whereby authorities can directly request access to data without prior judicial review, has been systematically abused to obtain such information without any judicial oversight.

Among the abuses that have been documented there is evidence revealed by *The New York Times* in November 2023 on how the Prosecutor General Office of Justice of Mexico City accessed phone records, text messages, and location data of various political figures, both from the ruling party and the opposition.[168]

The Attorney General's Office requested this information from the telecommunications company *Telcel*, arguing that the data would be used in investigations on kidnappings and forced disappearances and invoking the grounds for exception to prior judicial authorization referred to in Article 303 of the CNPP.

According to *The New York Times*, among those under surveillance from 2021 to date are Dolores Igareda, a senior official of the Supreme Court of Justice of the Nation; Ricardo Amezcua, a member of the Mexico City judiciary; Santiago Taboada, mayor and candidate for head of government of the capital; Higinio Martínez, Morena Senator for the State of Mexico; Horacio Duarte, then head of the National Customs Agency; Senator Lilly Tellez; and former legislator Alessandra Rojo de la Vega. According to the newspaper, none of these individuals were involved in kidnapping cases.

This *modus operandi* by the authorities was also denounced in 2019 by journalist Marcela Turati; Mercedes Doretti, co-founder of the Argentine Forensic Anthropology Team (EAAF); and human rights defender Ana Lorena Delgadillo. They reported that Mexico's Office of the Special Prosecutor for Organized Crime Investigation (hereinafter, "SEIDO") accessed their phone records by including them in the same case file in which members of a criminal organization were being investigated.[169]

---

167 Federal Telecommunications and Broadcasting Law, available at: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf – soon to be reformed, Articles 189 and 190 will now become Articles 160 and 161 of the new law.

168 Maria Abi-Habib, Natalie Kitroeff, and Emiliano Rodríguez Mega (2023). Politicians and officials targeted for surveillance in Mexico.. https://www.nytimes.com/es/2023/11/09/espanol/mexico-vigilancia-fiscalia-Telcel.html

169 R3D. (2021). SEIDO accessed phone records to spy on journalist and women's rights defenders for investigating the San Fernando massacre.
Available at: https://r3d.mx/2021/11/26/seido-accedio-a-registros-telefonicos-para-espiar-a-periodista-y-defensoras-por-investigar-masacre-de-san-fernando/

The SEIDO investigated Turati, Delgadillo, and Doretti for the crimes of forced disappearance and kidnapping. In doing so, the authorities accessed their personal information, the phones they used, and their geographical location. In Turati's case, they also obtained the personal data she provided to the Ministry of Foreign Affairs to process her passport.

It should be noted that access to the stored data was obtained without judicial authorization and that under no circumstances the access to such information can be considered justified, as there is no evidence that the journalist, defender, and expert witness, respectively, participated in the commission of any crime. Rather, their participation in the case consisted exclusively of accompanying the families of the victims who filed the complaint.

Based on these cases, a *modus operandi* has been observed in Mexico whereby prosecutors open an investigation or use an existing one and, based on "anonymous information," request telecommunications companies to provide them with information on numbers that are not related to any crime. In this way, files on kidnapping or other serious crimes are used as a pretext to bypass the obligation to obtain prior federal judicial authorization.

Furthermore, in no case do they submit requests for access to retained data for judicial ratification, contrary to the provisions of Article 303 of the CNPP. They argue that they found the information useless and therefore saw no point in requesting judicial ratification, so they proceeded to destroy it in a manner that cannot be verified.

The documented pattern suggests that there could be many more cases in which authorities have fraudulently obtained communications metadata and real-time geolocation from telecommunications companies without conducting investigations to identify other victims and punish those responsible.

III. Information extraction

Within the category of private communications interception, other communications interception technologies detected in the region include forensic extraction tools.

These tools allow all information stored on a physical device to be extracted, including private communications, communication identification data, as well as information, documents, text files, audio, images, or videos contained on any device, accessory, electronic device, computer equipment, storage device, and anything else that may contain information, including that stored on remote platforms or data centers linked to them.[170]

They also allow SIM card cloning, password extraction, recovery of deleted information, and in some cases even allow access to the content of messaging applications such as WhatsApp and iMessage, among others.

The Israeli company *Cellebrite* is the developer of the most popular forensic extraction tool in the world. For years, the sale of these products to dozens of governments, including autocratic or oppressive regimes in countries such as China, Turkey, Venezuela, Belarus, Russia, and Bangladesh, has been documented. These governments have used such equipment to unjustifiably monitor dissidents, journalists, activists, members of the LGBTIQ+ community, and people belonging to ethnic minorities.[171]

---

170 The legal definition in Article 291, paragraph 4, of the CNPP, amended on June 17, 2016, was taken into account.

171 Access Now. (2021). What spy firm *Cellebrite* can't hide from investors. Available at: https://www.accessnow.org/what-spy-firm-Cellebrite-cant-hide-from-investors/

Following controversy surrounding the misuse of equipment sold by *Cellebrite* and its interest in going public, the company stated that it would form an ethics committee and stop selling its products to authoritarian or oppressive governments. However, former employees of the company have stated that it has done nothing to prevent abuse.[172] The only times the company has taken action against abuse have been when the cases reach the media or when they are forced to act through legal proceedings.[173]

MÉXICO

In Mexico, dozens of federal and state authorities have acquired forensic extraction tools developed by *Cellebrite* and other similar companies. In many cases, the legality of their use is questionable, and in most cases there is widespread opacity regarding their use.[174]

PARAGUAY

In Paraguay, there is evidence that the Public Prosecutor's Office and the National Police have used Septier, according to public procurement data for, at least, 2018 during the administration of President Mario Abdo Benitez through the company *Winner*.[175]

IV. Spyware

One of the most invasive surveillance technologies detected is the use of surveillance systems known as spyware. Although the characteristics may vary, typically the infection of a device through the operation of spyware allows the indiscriminate interception and collection of all types of communications and data, whether encrypted or not, as well as remote and secret access to personal devices and the data stored on them, facilitating real-time surveillance and manipulation of the data contained on those devices.[176] In other words, the technology used by spyware gives its users not only the ability to monitor the person, but also to manipulate the infected device, including altering, deleting, or even implanting incriminating information.

Once a device is infected, spyware operators can typically record video and audio communications; collect messages, texts, and emails (even from supposedly secure platforms); and access calendars, contacts, and geolocation data. They can also access other connected devices, such as wearable technology or vehicles, which may contain more data relating to the person's health and location.[177]

---

172 Haaretz. (2021). I worked at Israeli phone hacking firm *Cellebrite*. They lied to us. Available at: https://www.haaretz.com/israel-news/2021-07-27/ty-article/i-worked-at-israeli-phone-hacking-firm-Cellebrite-they-lied-to-us/0000017f-f652-d460-afff-ff764fae0000

173 Dhaka Tribune. (2021). Israeli phone-hacking firm *Cellebrite* to stop sales to Bangladesh. Available at: https://www.dhakatribune.com/world/middle-east/255655/israeli-phone-hacking-firm-Cellebrite-to-stop

174 Network in Defense of Digital Rights (R3D). (2025). The State of Surveillance. Available at: https://r3d.mx/wp-content/uploads/EDLV_2025.pdf https://r3d.mx/wp-content/uploads/EDLV_2025.pdf

175 Vinner SRL. See: https://Winner.com.py/

176 United Nations. General Assembly. (2018). Resolution A/HRC/39/29. The right to privacy in the digital age. Para. 19. Available at: https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age-report-united-nations-high: Governments seem to be increasingly resorting to malicious interception software that infiltrates people's digital devices. This type of hacking allows for the indiscriminate interception and collection of all types of communications and data, whether encrypted or not, as well as remote and secret access to personal devices and the data stored on them, thus facilitating real-time surveillance and manipulation of the data contained on those devices."

177 United Nations. General Assembly. (2022). Resolution A/HRC/51/17. The right to privacy in the digital age. Available at: https://docs.un.org/es/A/HRC/51/17

Its use is illustrated below with documented cases in **Paraguay**, **Mexico**, and **El Salvador**.

PARAGUAY

In 2012, the Paraguayan government acquired *FinFisher* spyware[178], according to investigations by the Citizen Lab at the University of Toronto and the newspaper ABC Color. These investigations include official documentation such as purchase invoices, as well as delivery and receipt documents signed by the National Anti-Drug Secretariat (SENAD), confirming the state's use of this malware for surveillance activities.

Another relevant case is that of the *Galileo* – Remote Control System (RCS) software, developed by the company *Hacking Team*. The leaks of *Wikileaks*[179] exposed communications between this company and the Paraguayan Public Prosecutor's Office, which showed an intention to purchase the system. Subsequently, in October 2014, *Hacking Team*'s local partner requested additional equipment, suggesting a sustained interest by the Paraguayan authorities in this espionage technology.

Likewise, *Wikileaks*[180] revealed diplomatic conversations about the acquisition of telephone tapping equipment by the Ministry of the Interior in 2010. This practice was carried out in 2012, during the government of Federico Franco, when equipment worth US$2.5 million was purchased. However, this equipment mysteriously disappeared from the offices of the Ministry of the Interior, according to a report by the Executive Branch's General Audit Office in November 2013.[181]

Although there are no specific, fully identified cases of citizen surveillance in Paraguay, it cannot be ruled out that such practices are taking place. This background suggests that the country could be following regional trends in state surveillance, which are often characterized by opacity and a lack of public oversight.

178 Citizen Lab (2015). Pay No Attention to the Server Behind the Proxy.
Available at: https://citizenlab.ca/2015/10/mapping-FinFishers-continuing-proliferation/

179 *Wikileaks*. (2014). Cable on Paraguay.
Available at: https://Wikileaks.org/hackingteam/emails/emailid/249367

180 *Wikileaks*. (2010). Cable on Paraguay.
Available at: https://Wikileaks.org/plusd/cables/10ASUNCION97_a.html

181 Sequera, M., Samaniego, M. Cybercrime: Challenges of harmonizing the Budapest Convention in the Paraguayan criminal justice system. Page 48.
Available at: https://www.derechosdigitales.org/wp-content/uploads/minuta_TEDIC.pdf

MÉXICO

In Mexico, the acquisition and abuse of spyware technologies have been widely documented with regard to *FinFisher* spyware from Gamma International[182] company; *Galileo* from *Hacking Team*;[183] and *Pegasus* from the Israeli company *NSO Group*. The main findings regarding *Pegasus* spyware[184] are summarized below.

NSO Group Technologies is one of the companies whose name has been widely linked to surveillance activities in several countries, including Mexico.[185] The company claims that its technology is used exclusively by government clients approved by the Israeli Ministry of Defense.[186] Despite claiming to respect a human rights policy, the number of documented cases in which its technology is used abusively against civil society around the world continues to grow.

The first known case involving of *Pegasus* in Mexico was recorded in 2012, when journalistic investigations revealed that the Secretariat of National Defense (hereinafter, "SEDENA") became *NSO Group's* first international client when it acquired the *Pegasus* system as part of a series of contracts with *Security Tracking Devices S.A. de C.V.*, totaling 5.6 billion pesos.[187] These contracts were signed after a demonstration of how the *Pegasus* system works in May 2011 to then-President Felipe Calderón and Secretary of National Defense Guillermo Galván Galván.[188]

In June 2017, Citizen Lab, as well as ARTICLE 19, the Network in Defense of Digital Rights (R3D) and SocialTIC published the report *"Spy Government: Systematic Surveillance of Journalists and Human Rights Defenders in Mexico"*,[189] which documents multiple cases of attempts to infect human rights defenders and journalists with *Pegasus* malware during the administration of President Peña Nieto.[190]

---

182 In 2013 and 2015, an investigation by Citizen Lab, a multidisciplinary laboratory at the University of Toronto, revealed evidence of *FinFisher* command and control servers in 32 countries, including Mexico. The then Federal Institute for Access to Information and Data Protection (IFAI) announced the launch of an investigation, but no relevant results were reported.

183 A large number of emails and internal documents from the Italian firm *Hacking Team* were leaked to the public on July 5, 2015. These showed that the spyware company had sold its products to governments in countries facing serious human rights crises, such as Bahrain, Sudan, and Uzbekistan. Of a total of 35 nations, Mexico turned out to be the firm's main customer, with transactions made by different local governments, agencies, and federal agencies through intermediary companies and, in virtually all cases, without legal authority to do so. The following chart shows Mexico's spending in relation to other *Hacking Team* client countries.

184 In any case, information has emerged in the region about other countries where *Pegasus* may have been deployed, possibly including Colombia. However, the best documented case and the one for which there is the most abundant evidence of *Pegasus* use in the region is undoubtedly that of Mexico.
On the case of Colombia.
Available at: https://es.wired.com/articulos/estados-unidos-confirma-que-financio-el-uso-del-software-espia-Pegasus-en-colombia
On El Salvador.
Available at: https://elfaro.net/es/202503/el_salvador/27785/embajador-johnson-no-dudo-que-pudo-haberse-usado-Pegasus-en-el-salvador
On Panama.
Available at: www.univision.com/noticias/especiales/exclusiva-martinelli-tambien-espio-a-estadounidenses-dice-testigo

185 Cox, J. and L. Franceschi Bicchierai, (2016). "Meet *NSO Group*, the new major player in the government spyware business," Motherboard.
Available at: https://motherboard.vice.com/en_us/article/nso-group-new-big-player-in-government-spyware

186 Ibid.

187 Aristegui Noticias. (2012). Federal government via Sedena purchased 5 billion pesos worth of espionage equipment.
Available at: https://aristeguinoticias.com/1607/mexico/gobierno-federal-via-sedena-compro-5-mil-mdp-en-equipo-para-espionaje/

188 Network in Defense of Digital Rights (R3D). (2021). *NSO Group* showed *Pegasus* to Felipe Calderón and his Secretary of Defense.
Available at: https://r3d.mx/2021/08/11/nso-group-mostro-Pegasus-a-felipe-calderon-y-su-secretario-de-defensa

189 Network in Defense of Digital Rights (R3D). (2017). Spy Government: Systematic Surveillance of Journalists and Human Rights Defenders in Mexico.
Available at: https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf

190 Ahmed, A., & Perlroth, N. (2017). Using texts as lures, government spyware targets Mexican journalists and their families. *The New York Times*.
Available at: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

Despite the change in government and repeated statements by then-President Andrés Manuel López Obrador that journalists and human rights defenders would no longer be monitored and that *Pegasus* and any other similar private communications interception system would no longer be used, surveillance continued during his administration. In 2022 and 2023, the *"Spy Army"* investigation revealed new cases of surveillance using *Pegasus* that could be attributed, with a high degree of certainty, to the Mexican Army.[191]

To date, documented victims of SEDENA espionage include the undersecretary for human rights, Alejandro Encinas,[192] the coordinator of the Truth Commission for the "Dirty War"—the period of forced disappearances, torture, and executions committed by Mexican security forces, including the army, between 1960 and 1980—Camilo Vicente Ovalle;[193] a human rights organization, the Miguel Agustín Pro Juárez Human Rights Center (Centro Prodh), human rights defender Raymundo Ramos, and two journalists, Ricardo Raphael and a journalist from the digital media outlet Animal Político.[194] **In fact, the Pegasus infections occurred at a time when the victims were working on cases related to human rights violations committed by the Armed Forces.**

In 2017, 2022, and 2023, human rights defenders and journalists monitored by *Pegasus* spyware filed criminal complaints with the Special Prosecutor's Office for Crimes Against Freedom of Expression (hereinafter "FEADLE") for, among other things, the crimes of illegal interception of private communications and illegal access to computer systems. However, to date, impunity has prevailed.

The fact that one of the victims, the Centro Prodh, has been targeted by *Pegasus* surveillance under two different administrations and has filed two separate criminal complaints shows how impunity and the lack of adequate measures led to the repetition of illegal surveillance.

EL SALVADOR

Between July 2020 and November 2021, the same *Pegasus* software was used to infect 35 devices belonging to journalists and members of civil society, according to the T*orogoz Project* report developed by Citizen Lab and Access Now.[195]

The report noted that out of the 35 people who were infected and monitored with the software, 22 are members of the investigative journalism outlet *El Faro*.[196] The report also concluded that access to the journalists' mobile devices coincided with the publication of *El Faro* reports containing information of public interest.

191 Network in Defense of Digital Rights (R3D). Spy Army.
Available at: https://ejercitoespia.r3d.mx/

192 Kitroeff, Natalie & R. Bergman, "Mexican President Said He Told Ally Not to Worry About Being Spied On", *The New York Times*, May 23, 2023, available at: https://www.nytimes.com/2023/05/23/world/americas/mexico-president-spying-Pegasus.html

193 Lopez, Oscar & M. Sheridan, "He's leading Mexico's probe of the Dirty War. Who's spying on him?", The Washington Post, June 23, 2023, available at: https://www.washingtonpost.com/world/2023/06/03/mexico-Pegasus-dirty-war-lopez-obrador/

194 Network in Defense of Digital Rights (R3D), Article 19, Social Tic, et. al., Spy Army, available at: https://ejercitoespia.r3d.mx/

195 The Citizen Lab & Access Now. (2022). Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with *Pegasus* Spyware. University of Toronto.
Available at: https://utoronto.scholaris.ca/items/025fd761-7d3f-4356-b6f8-f43eeab65128

196 See: https://elfaro.net/es?ref=inicio

This case occurred during the first term of President Nayib Bukele in El Salvador. The government denied any connection to these events and claimed not to be a client of *NSO Group*.[197] However, the T*orogoz Project* report establishes that, although there is no evidence linking the specific infection to a particular *Pegasus* client, a *Pegasus* client operating in El Salvador since November 2019 was identified and named *"Torogoz"*.[198] Furthermore, as previously mentioned, *NSO Group* has stated that this software is sold only to governments.[199]

The IACHR and its RELE, as well as the Regional Office of the United Nations High Commissioner for Human Rights (hereinafter OACNUDH) expressed concern about the information on the use of *Pegasus* against journalists and civil society organizations in El Salvador. They also urged the State to investigate the case effectively and impartially and to ensure the protection of the victims.[200]

At the national level, Cristosal, an organization dedicated to the defense of human rights, filed a lawsuit before the Administrative Chamber of the Supreme Court of Justice against the Court of Accounts in El Salvador for refusing to investigate the possible use of state funds for the purchase of *Pegasus*. However, the lawsuit was dismissed.[201] Cristosal stated that it would file an appeal for the lack of investigation into the use of state funds for the purchase of the software.[202]

Internationally, in December 2022, journalists from *El Faro* filed a complaint against *NSO Group* in a US federal court. The lawsuit was filed with the aim of forcing the company to reveal who the customer was that purchased *Pegasus*, clarify what information was collected from the journalists, what was done with this information, and that it be deleted from its servers.[203] The case was dismissed on the grounds that neither the defendants nor the plaintiffs were located in the United States.[204]

In July 2024, technology companies and press organizations in the United States filed an *amicus curiae* brief before the Ninth Circuit Court of Appeals in support of *El Faro*'s lawsuit against *NSO Group*. The lawsuit is currently under appeal following the initial dismissal of the case.[205]

---

197 Abi-Habib, M. (2022). *Pegasus* spyware was used to hack journalists in El Salvador. *The New York Times*. Available at: https://www.nytimes.com/es/2022/01/12/espanol/el-faro-Pegasus.html

198 The Citizen Lab & Access Now. (2022). Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with *Pegasus* Spyware. University of Toronto. Available at: https://utoronto.scholaris.ca/items/025fd761-7d3f-4356-b6f8-f43eeab65128

199 NDTV. (2021). Firms like NSO can't sell *Pegasus* to non-government actors, Israel's ambassador to India says. Available at: https://www.ndtv.com/india-news/firms-like-nso-cant-sell-Pegasus-to-non-government-actors-israels-ambassador-to-india-2590792

200 IACHR. (2022). The IACHR, its Special Rapporteur for Freedom of Expression, and the OHCHR express concern over findings regarding the use of *Pegasus* software in El Salvador. https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp

201 Swissinfo.ch. (2023). The Salvadoran Supreme Court does not admit lawsuit against entity that did not investigate *Pegasus*. Available at: https://www.swissinfo.ch/spa/el-supremo-salvadore%C3%B1o-no-admite-demanda-contra-ente-que-no-investig%C3%B3-Pegasus/48445076

202 DW. (2023, mayo 1). NGO to file an amparo petition with El Salvador's Supreme Court over *Pegasus* spyware used against journalists. LatAm Journalism Review. https://latamjournalismreview.org/es/news/ong-presentara-demanda-de-amparo-ante-corte-suprema-de-el-salvador-por-espionaje-con-Pegasus-a-periodistas/

203 De Assis, C. (2022). After being spied on, some journalists from *El Faro* are suing the manufacturer of *Pegasus* spyware in the United States. LatAm Journalism Review. Available at: https://latamjournalismreview.org/es/articles/tras-haber-sido-espiados-periodistas-de-el-faro-demandan-en-estados-unidos-al-fabricante-del-spyware-Pegasus/

204 Electronic Privacy Information Center. (2024). Dada et al. v. *NSO Group*. Available at: https://epic.org/documents/dada-et-al-v-nso-group/

205 Gressier, R. (2024). Tech giants and media outlets back *El Faro*'s appeal in the *Pegasus* case. *El Faro*. Available at: https://elfaro.net/es/202407/el_salvador/27511/Gigantes-de-tecnolog%C3%ADa-y-prensa-dan-espaldarazo-a-la-apelaci%C3%B3n-de-El-Faro-en-caso-Pegasus.htm

V. Geolocation based on the exploitation of vulnerabilities in telecommunications infrastructure (SS7)

In addition to antennas, the mobile phone network consists of switches, interfaces, and databases that enable devices to be located and the information needed to provide them with telecommunications services to be obtained.

The way our devices and antennas communicate is dictated by a protocol. The Signaling System No. 7 (SS7) is a set of protocols used by mobile network operators to exchange information, establish and route phone calls, text messages, and other communications within 2G and 3G networks.[206]

The protocol was adopted almost forty years ago, at a time when the mobile telecommunications field was made up of a few companies that knew each other, so it was not designed with authentication measures in mind. The lack of measures against unauthorized access has led to the protocol being abused by various entities for surveillance purposes. Two representative cases of geolocation based on the exploitation of these vulnerabilities can be found in **Brazil** and **Peru**.

BRASIL

In early 2023, the press revealed that the Brazilian Intelligence Agency (Abin) illegally used electronic device geolocation tools during the Bolsonaro administration (2019-2022), the main one being the *FirstMile* spyware.[207]

FirstMile, developed by Israeli company Cognyte (formerly Verint), is spyware that exploits vulnerabilities in telecommunications networks (SS7) to track the location of mobile devices. The technology allowed up to 10,000 mobile phones to be monitored per year, simply by entering the target's phone number, regardless of the network used (3G, 4G, or 5G). Based on a phone number entered, *FirstMile* can provide the location of a device—and therefore the person to whom it belongs—based on its position when connecting to a mobile network.

In Brazil, the company *Suntech* acted as representative and developer for *FirstMile*, according to information from the Santa Catarina Association of Technology Companies (Acate).[208] The contract for the acquisition of this software was signed directly by Abin in December 2018, during the final days of Michel Temer's administration. The acquisition took place through contract 567/2018[209], which is confidential.

206 Electronic Frontier Foundation. (2024). EFF to FCC: SS7 is Vulnerable, and Telecoms Must Acknowledge That. Available at: https://www.eff.org/deeplinks/2024/07/eff-fcc-ss7-vulnerable-and-telecoms-must-acknowledge

207 Dantas, D.; Camporez, P.; Bronzatto, T.. Bolsonaro's Abin used secret program to monitor people's locations via cell phones. OGlobo, 14 mar. 2023. Available at: https://oglobo.globo.com/politica/noticia/2023/03/abin-de-bolsonaro-usou-programa-secreto-para-monitorar-localizacao-de-pessoas-por-meio-do-celular.ghtml.

208 G1. First Mile: o que se sabe sobre o software espião usado pela Abin. G1, 25 ene. 2024. Available at: https://g1.globo.com/tecnologia/noticia/2024/01/25/fist-mile-o-que-se-sabe-sobre-o-software-espiao-usado-pela-abin.ghtml.

209 Ibid.

It is not known with certainty how many times the spyware was used, but there is documented evidence[210] that it was used to spy on Brazilian citizens between December 26, 2018, and May 8, 2021, the period of the contract during which the tool was acquired, as confirmed by the Brazilian Intelligence Agency. Investigators indicate[211] that, although the contract ended in 2021, there are signs that the system was used more frequently in the last years of Bolsonaro's government (2019-2022) to illegally monitor public officials, politicians, police officers, lawyers, journalists, and even judges and members of the Federal Supreme Court (hereinafter STF).

For example, reports indicate that the software was widely used between May 2020 and April 2022, when Alexandre Ramagem was head of ABIN, to illegally monitor public officials—including journalists, Supreme Court judges, and political opponents—and other citizens, suggesting possible use for intimidation or control of dissent[212]. At the time, the agency operated under the supervision of the Institutional Security Office (GSI) of the President's Office, headed by General Augusto Heleno.

Investigations by the Federal Police launched in 2023 suggest that a group within Abin, especially during Ramagem's tenure, used the agency to illegally monitor authorities, public officials, and other citizens without any judicial or legislative oversight, allowing this mass surveillance to occur without the victims being notified or having the possibility of defending themselves.[213] The way in which it was used raises questions about abuse of power and violation of constitutional rights.

Investigations are ongoing, and documents obtained so far indicate that Abin carried out illegal monitoring operations with the tool for at least three years, without transparency regarding its use or accountability mechanisms.[214] The lack of transparency in the acquisition and use of the tool remains one of the main points of investigation by the Federal Police and the STF in 2024.

In January 2023, the Federal Police launched *"Operation Last Mile"* to investigate the instrumentalization of Abin for political purposes, known as the "parallel Abin." According to the decision of Minister Alexandre de Moraes, the investigation indicates the existence of a political nucleus within Abin, especially under the management of Alexandre Ramagem, who used technology illegally to monitor authorities, public officials, and citizens.

In January 2024, the Federal Police launched *Operation Vigilância Aproximada* (Close Surveillance) – an offshoot of Última Milha – to investigate a criminal organization within Abin that allegedly illegally monitored individuals and authorities, hacking into electronic devices and telecommunications infrastructure. One of those under investigation is Congressman Alexandre Ramagem (PL-RJ), former director of Abin. Twenty-one search and seizure warrants were executed, and at least seven Federal Police officers are under investigation. In 2025, advances in the case led to the suspension of federal police officer Carlos Afonso Gonçalves Gomes Coelho, coordinator of the Federal Police's Operational Aviation Command, accused of being part of the "high management core" of the "parallel Abin" along with Ramagem at the time of the events.

---

210 Ibid.

211 G1. PF prende dois servidores e apura se Abin rastreou celulares de forma ilegal na gestão Bolsonaro. G1, 20 oct. 2023. Available at: https://g1.globo.com/politica/noticia/2023/10/20/policia-federal-abin-geolocalizacao.ghtml.

212 G1. First Mile: o que se sabe sobre o software espião usado pela Abin. G1, 25 ene. 2024. Available at: https://g1.globo.com/tecnologia/noticia/2024/01/25/fist-mile-o-que-se-sabe-sobre-o-software-espiao-usado-pela-abin.ghtml.

213 Pontes. F.. Abin espionou autoridades do Judiciário, do Legislativo e jornalistas. Agência Brasil, 11 jul. 2024, available at: https://agenciabrasil.ebc.com.br/geral/noticia/2024-07/abin-espionou-autoridades-do-judiciario-do-legislativo-e-jornalistas.

214 Ibid.

In January 2024, the National Telecommunications Agency (hereinafter, Anatel) opened three confidential administrative proceedings to investigate the possible involvement of mobile phone companies in the illegal monitoring of phones using *FirstMile* software. The investigation is looking into whether the operators identified attempts to access information at the time or only became aware of them later, through the press. Their duty to report to the agency is also being examined. The companies denied having had any contact with Abin or knowledge of the illegal surveillance, stating that they implemented blocks against unauthorized access through international interconnection protocols. There are reports that Abin operated without prior interaction with the operators, but it is unclear when they detected the attacks.[215]

In December 2023, the Inspector General's Office (hereinafter "PGR") filed a Direct Action of Unconstitutionality by Omission (ADO 84), which became Action for Non-Compliance with a Fundamental Precept (ADPF) 1143 before the STF. The action challenges the lack of regulation on the use of spyware by public bodies. The PGR argued that the acquisition and use of spyware without clear rules compromises fundamental rights such as privacy, intimacy, and the secrecy of communications. It requested that Congress establish a deadline for passing legislation on the matter. The case is still pending, but in June 2024, Minister Cristiano Zanin convened a public hearing on ADPF 1143, with the participation of 33 entities.

PERÚ

The *Pisco Project* was a mass surveillance measure implemented by the government of Ollanta Humala between 2011 and 2016 through the National Intelligence Directorate (hereinafter "DINI"). It consisted of the acquisition, without public tender, of a legal communications interception system from the Israeli-US company *Verint Systems*, worth USD 22 million, financed by the Ministry of Economy and Finance.[216]

The system allowed the interception of phone calls, text messages, emails, chats, and web browsing, as well as real-time geolocation of up to 5,000 people and the simultaneous recording of 300 conversations.[217]

It also included the *SkyLock* module, a tool capable of locating mobile devices inside and outside the country.[218] Although initially managed by the DINI, the system was later transferred to the Ministry of the Interior, falling under the responsibility of its General Intelligence Directorate (hereinafter "DIGIMIN"). It was also revealed that the operators Movistar, Claro, Entel, and Bitel signed cooperation agreements to allow the State access to their networks.[219]

---

215 STF: Constitutional review of spyware: [Does not investigate the specific case, but seeks regulation of this technology.]

216 Morachimo, M. (2016). The communications espionage system left behind by Humala. Available at: https://hiperderecho.org/2016/08/proyecto-pisco-skylock-peru-verint/

217 Associated Press (2016). Snapping up cheap spy tools, nations 'monitoring everyone'. Available at: https://apnews.com/736dd5c3aa644cd499d6f6da8b9e5974

218 This tool exploits vulnerabilities in telecommunications infrastructure (such as SS7).

219 Digital Rights (2016). Peru paid USD $22 million to spy on its citizens' communications. Available at: https://www.derechosdigitales.org/10389/peru-pago-usd-22-millones-para-espiar-las-comunicaciones-de-sus-ciudadanos/.

During the administration of former President Humala, there were reports of surveillance and monitoring of high-profile politicians, such as former President Alan García and opposition candidate Keiko Fujimori.[220] Consequently, although there are no publicly identified victims or official figures on the number of people affected, the design and scope of the system suggest that, if used, anyone with access to digital media or mobile phones could have been subject to surveillance, regardless of their profession or activity.

The *Pisco Project* has been the subject of legal, political, and administrative investigations by various Peruvian government entities. For example, in the criminal sphere, in 2023, the Prosecutor's Office, through the Anti-Corruption's Office, initiated a preliminary investigation against former President Humala and senior officials from his administration for the alleged crime of aggravated collusion.

In this regard, the Prosecutor's Office maintains that the purchase of the system from the Israeli-US company *Verint Systems*, valued at USD 22 million and carried out without public tender, was irregularly directed, causing financial harm to the State. In October of that year, the Prosecutor's Office filed charges requesting 10 years and four months of effective imprisonment.[221] To date, no sentence has been issued.

In the parliamentary sphere, in August 2015, the Intelligence Committee of the Congress of the Republic announced that it would analyze the purchase of the system, describing it as a priority issue. Sessions were scheduled to evaluate the case, and the then-Comptroller General Fuad Khoury was summoned to report on the findings of the Comptroller General's Office.

The Comptroller's Office, for its part, also reportedly launched investigations into the purchase of the system, although the results of these proceedings have not been fully disclosed or made public.

Similarly, there are other countries, such as **Paraguay**, where since 2014 the Ministry of the Interior of the government of Horacio Cartes has had Septıer technology[222]. However, for "security" reasons, there are no details on the public procurement portal and only information on the tender to the company GALCORP, S.A. is available.[223]

In **Mexico**, the illegal use of geolocation has also been documented through the Geomatrix tool developed by Rayzone Group, with evidence that the Prosecutor's Office illegally acquired and operated the geolocation system to spy on the campaigns of presidential candidates in 2018.[224]

---

220 América TV (2015). DINI: new documents confirm surveillance of Alan García and Keiko Fujimori. Available at: https://www.americatv.com.pe/cuarto-poder/dini-nuevos-documentos-confirmarian-seguimientos-alan-garcia-y-keiko-fujimori-noticia-22831

221 Infobae (2023). Prosecutor seeks ten years in prison for Ollanta Humala in the Pisco Project case. Available at: https://www.infobae.com/peru/2023/10/12/ollanta-humala-fiscalia-pide-diez-anos-de-carcel-por-caso-proyecto-pisco/

222 Septier. See: https://www.septier.com/products/

223 Tender contract, available here: https://www.contrataciones.gov.py/licitaciones/adjudicacion/contrato/284615-galcorp-sociedad-anonima-1.html

224 Network in Defense of Digital Rights (R3D). (2021). #FiscalíaEspía: the FGR acquired equipment capable of illegally spying on all Internet users in Mexico. https://r3d.mx/2021/04/14/fiscaliaespia-la-fgr-adquirio-equipo-capaz-de-espiar-ilegalmente-a-todos-los-usuarios-de-internet-en-mexico/

VI. Cyber patrol

Another surveillance technique identified in the region is mass and indiscriminate internet monitoring—also known as "cyber patrol"—carried out mainly by security and intelligence forces. This technique consists of the systematic monitoring of content circulating on the internet which, if considered by the authorities as "public data" – given its publication and circulation online – can be used for any purpose, including surveillance and subsequent criminal prosecution. [225]

Cyber patrol can be deployed by both police and military forces and is justified on the grounds of preventing, detecting, or investigating illegal behavior. However, when carried out on a massive and indiscriminate scale, it can lead to the violation of fundamental rights such as privacy, personal data protection, freedom of expression and association, and the presumption of innocence.

In the region, Digital Rights compiled a 2024 report[226] on the deployment of cyber patrols in countries such as Argentina, Brazil, Bolivia, Colombia, Mexico, and Uruguay, as well as the acquisition of technologies for this purpose. It also documented the creation of fake undercover agent profiles that enhance the reach of cyber patrols in the region.

In this section, we focus on the experience of Colombia, recognizing that, as this is a relatively new surveillance practice, information on its deployment is constantly being updated.

COLOMBIA

In 2021, several public demonstrations were held against the administration of President Iván Duque,[227] which eventually became known as the 2021 National Strike. In this context, social media became the tool for reporting abuses and human rights violations against citizens by the security forces.

During this period, the Unified Cyber Command Post (PMU-Ciber) monitored open sources.[228] According to the authorities, this was done to identify fake news on social media that was damaging the image of public institutions and to identify those responsible for "acts of vandalism."

In the context of the protests, the PMU-Ciber spent more than 20,000 hours monitoring citizens' activity on the internet, while simultaneously carrying out a strategy to fake a cyberattack on the Ministry of Defense and promote the #ColombiaIsMyTruth (#ColombiaEsMiVerdad) campaign.[229]

---

225 Camacho, L.; Ospina, D.; Upegui, J.C.(2022). State intelligence on the internet and social media: the Colombian case. Dejusticia.
Available at: https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf ; see also: Zara, N. (2023). Open source intelligence (OSINT) and human rights in Latin America: a comparative study in Argentina, Brazil, Colombia, Mexico, and Uruguay. CELE.
Available at: https://www.palermo.edu/Archivos_content/2023/cele/papers/233008-reporte-regional-OSINT.pdf

226 Digital Rights (2024). Social media profiling and cyberpatrol as new forms of mass surveillance deployed by states: relevant cases in Latin America.
Available at: https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf

227 Ivan Duque was elected as the candidate for the Democratic Center party, a political organization whose guiding principles are "democratic security, investor confidence, social cohesion, government austerity, and popular dialogue." According to the Karisma Foundation, the party is sympathetic to the most conservative factions in Colombian politics.

228 The PMU-Ciber consisted of cooperation between different authorities that coordinated to carry out "cyber patrol" activities. The member entities of the PMU-Ciber were the Police Cyber Center; the Ministry of Information and Communications Technology (MinTIC); the MinTIC Cyber Emergency Response Team; the National Intelligence Directorate (DNI); the National Police's Computer Security Incident Response Team; the Joint Cyber Command of the Armed Forces; and the Attorney General's Office (FGN), headed by Francisco Barbosa.

229 Foundation for Press Freedom (FLIP). (2021). The judges of truth, the sea of lies behind the state's cyber patrolling. https://flip.org.co/pronunciamientos/los-jueces-de-la-verdad-el-mar-de-mentiras-detras-del-ciberpatrullaje-del-estado

Through this campaign, publications deemed false by the monitoring authorities were shared, without explaining the criteria used to classify a news item as such and without any kind of counterbalance or control. As part of their social media monitoring, the authorities began to label posts identified as fake news as "digital terrorism." The label "digital terrorism" stigmatized opinions against the authorities and censored individuals by deleting posts and social media accounts, in complete violation of the rights to access information and freedom of expression.

At the time, Defense Minister Diego Molano stated that the news items were identified as false thanks to tools such as *Colombiacheck* and La Silla Vacía's Lie Detector, both of which are national news fact-checkers.[230] These two fact-checkers stated that their classifications of false content follow specific criteria and methodologies, which include explaining why content is classified as such and providing the sources used.

According to research conducted by *Karisma Foundation*, as part of cyber patrol activities during the 2021 National Strike, the practice of "undercover agents in virtual environments" was also implemented, in accordance with the provisions of Article 16 of Law 1908 of 2018. This involved the monitoring of public social media profiles and WhatsApp groups by the Prosecutor's Office, with the aim of collecting information that could serve as digital evidence in subsequent investigations for the prosecution of acts related to the social protests in 2019 and 2021.[231]

According to the State report to the IACHR, during its working visit to Colombia in June 2021, there were 21,675 hours of "cyber patrols" from the start of the demonstrations on April 28 until June 8, 2021, the latter being the start date of the visit.[232] During this period, Colombian authorities identified at least 154 pieces of fake news and more than 2,300 posts containing threats to life or physical integrity.[233]

Therefore, according to the June report of the IACHR, cyberpatrolling constitutes a risk to individual freedoms, since: (a) it "criminalizes expressions about public officials or matters of public interest," while (b) it has a "strong inhibitory effect on the dissemination of ideas, criticism, and information".[234] The IACHR also identified the link between the Ministry of Defense and the company Alotrópico S.A.S, related to the #ColombiaEsMiVerdad campaign, through a *"service to position the 'brand' of the Ministry of Defense using OSINT tools for marketing activities such as perception analysis, detecting image crises on social media, and identifying important actors or allies in this communication strategy"*.[235]

---

230 Saavedra, A. M. (2021, November 8). Colombiacheck and the Colombia is my truth campaign. Colombiacheck. https://colombiacheck.com/investigaciones/colombiacheck-y-la-campana-colombia-es-mi-verdad

231 Karisma Foundation is about to publish the report referenced in this section.

232 IACHR. (2021). IACHR concludes working visit to Colombia and presents its observations and recommendations. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/167.asp

233 Reports on the actions monitored by the PMU-Ciber were shared from May 22, 2021, to July 2, 2021, through the Ministry of Defense's X account. (@mindefensa). This was preceded by other publications on the activities of the PMU-Ciber in January 2020 and in early May 2021. Similarly, in June 2021, the Police Cyber Center (CCP) published a general report of the public demonstrations between April 28 and June 3, 2021. According to this institution, during this period, "93 pieces of fake news (...) that were detrimental to the institutional image [were identified through cyber patrol activities on social media]". This report was also shared via its X account (@CaiVirtual).
On July 2, 2021, the latest report was published by MinDefensa on its X account, in which it stated that it had identified 157 pieces of fake news; that is, three more than those reported to the IACHR.

234 Inter-American Commission on Human Rights. (2021, June 10). IACHR concludes working visit to Colombia and presents its observations and recommendations. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/167.asp

235 Before the 2021 National Strike, four state entities had contracted technology services with companies that provide digital surveillance tools. Namely, DIJIN; the Joint Cyber Command of the Police; the National Army; the National Police; and FGN. These contracts were signed with three private companies: a. Gamma Ingenieros SAS: GAMMA Ingenieros was a distributor for 4IQ, a Spanish company now called Constella Intelligence, which provides intelligence tools based on open-source searches. The contract was awarded in 2016 directly between the National Army and the company, and the purpose of the contract was to purchase intelligence equipment with license extension and hardware architecture for the open source system. The contract number is 325-DIADQ-CADCO-CENACINTELIGENCIA-2016. https://gammaingenieros.com/ b. Deinteko SAS: Representative in Colombia of the Israeli company Cibersixgill (formerly Sixgill). This company was contracted by three of the entities

In the context of the protests, the Prosecutor's Office (FGN) issued Directive 002 of 2021, which allowed the FGN to investigate acts committed during protests and prosecute them under terrorism charges.[236] This is quite alarming, because Directive 002 of 2021 implied a change in "criminal policy (...) that allowed for macro-charges, understood as charges for serious crimes over acts of lesser harm."

By establishing the possibility of applying the crime of terrorism in investigations related to the National Strike, investigations could be aligned with the narrative of "cyberterrorism" and the implications that this had for subsequent prosecutions. In addition, the State used certain powers established in Law 1908 of 2018 to collect information obtained from WhatsApp groups or public social media pages as digital evidence for future investigations related to the crime of terrorism, which in previous years could not be considered applicable in the context of protests (Directive 0008 of 2016).

According to research by Fundación Karisma, following the 2021 protests, based on information provided by the FGN, at least 538 people were identified as being linked to events that took place during the protests between April and July 2021. Out of these, 259 have been charged in different cities in Colombia (Bogotá, Cali, Medellín, Pasto, and Bucaramanga). According to the information gathered, the FGN collected information during the period under review and has used it as digital evidence to secure convictions for the crimes of conspiracy to commit a crime, terrorism, violence against public servants, aggravated damage to property, and obstruction of public roads affecting public order.

To date, no investigation has been launched into potential abuses in the use of the PMU-Ciber's powers. The only related action was taken by the new Attorney General, Adriana Camargo, who issued a new Directive 0001 of 2024,[237] repealing the guidelines established in Directive 0002 of 2021 and establishing that peaceful social protest enjoys constitutional protection[238] and will not be subject to prosecution or criminal punishment. It also establishes new criteria for interpreting acts with criminal characteristics that occur during protests. Unlike Directive 0002 of 2021, the parameters for interpreting cases of terrorism investigations follow a logic of non-criminalization of protest.

mentioned above: (a) the DIJIN in 2019; (b) the Joint Cyber Command in 2020; and (c) the Prosecutor's Office in 2022.

236 See: https://cr00.epimg.net/descargables/2021/06/06/8e14ef349816167a499eadd80bbfe740.pdf

237 See: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=166137

238 The Directive stipulates that such acts "must be interpreted in accordance with the scope of protection of the fundamental rights of freedom of expression, freedom of assembly, and peaceful demonstration, and only those that exceed the legitimate exercise of these rights shall be investigated and prosecuted in accordance with substantive and procedural criminal law".

VII. Surveillance of individuals through vehicle license plate reading systems

Automatic license plate readers are high-speed camera systems controlled by computers, installed on poles, police vehicles, streetlights, or other structures, to automatically record vehicle license plates, location, date, and time they were captured.[239]

This surveillance measure allows for the systematic recording, storage, and analysis of license plates of vehicles traveling in public spaces on a massive and indiscriminate basis. It is ostensibly intended for security or traffic management purposes. However, its application may infringe on fundamental rights such as the right to privacy, freedom of movement, and data protection.

BRASIL

The Integrated Public Safety Operations and Monitoring Platform (*Córtex*) is an initiative of the Brazilian Ministry of Justice and Public Safety (hereinafter, "MJSP"), officially established by Portaria No. 218 of September 29, 2021. This platform is operated and managed directly by the Secretariat of Integrated Operations (hereinafter, "SEOPI") of the aforementioned ministry.

Cortex is linked to the *Smart Sampa* program, an initiative of the São Paulo City Hall that integrates surveillance cameras in the city to allegedly improve public security. No public details have been found on the participation of specific developers or private intermediaries in the implementation or management of the *Córtex* platform or the *Smart Sampa* program.

Its deployment took place mainly during the administration of Jair Bolsonaro (2019-2022), although its use continues under the administration of Luiz Inácio Lula da Silva (2023-present). During the Bolsonaro administration, the MJSP, through SEOPI, was responsible for the management and operation of *Córtex*.[240]

Reports indicate that, during Jair Bolsonaro's administration, the Ministry of Justice chose not to audit the *Cortex* system, sparking debates about possible misuse of the platform to monitor targets without adequate justification.[241]

In a 2020 article[242], The Intercept defined *Cortex* as:

> artificial intelligence technology that uses license plate reading by thousands of road cameras spread across highways, bridges, tunnels, streets, and avenues throughout the country to track moving targets in real time.

239 EFF. (n.d.). Automated License Plate Readers (ALPR).
Available at: https://sls.eff.org/es/technologies/lectores-automatizados-de-matriculas-alpr

240 Seopi is a department within the MJSP that gained notoriety in July 2020 when it was revealed that the secretariat had produced an intelligence dossier on police officers and teachers linked to anti-fascist movements, which was suspended by the STF following a trial. In São Paulo, the Smart Sampa initiative, promoted by the Municipal Government, seeks to improve urban security through advanced technologies.

241 Freitas, C.; Valente, R.. Ministry of Justice declined to audit the Bolsonaro administration's use of Córtex. Agência Pública, 12 oct. 2024.
Available at: https://apublica.org/2024/10/cortex-mj-nao-quis-auditar-sistema-espiao-pelo-governo-bolsonaro/.

242 Rebello, A.. Give your license plate number to the CPF. The Intercept Brasil, 21 sep. 2021.
Available at: https://www.intercept.com.br/2020/09/21/governo-vigilancia-cortex/.

Cortex is a mass monitoring system that integrates national and municipal databases with license plate recognition technologies and, in some cases, facial recognition. Not only does it monitor vehicles in real time through cameras installed on roads, identifying license plates and tracking their routes, but it is also capable of collecting and cross-referencing personal data from more than 160 databases—including those of the federal public administration, such as the Ministry of Economy's Annual Social Information Report—and storing the data for a period of ten years.

The system allows approximately 55,000 civilian and military agents to monitor "targets" without the need for specific justifications. According to the Public Agency,243 in 2024 the platform received images from 35,900 cameras installed on roads, in urban areas, soccer stadiums, and federal highways. Operating 24 hours a day, the system allows for continuous surveillance of people and vehicles.

Córtex was the subject of a request for access to information in 2024,[244] seeking to find out how many people and vehicles had been monitored. The MJSP denied the request, arguing that disclosing the information could compromise ongoing investigations, but confirmed that *Córtex* "targets" can be monitored indefinitely, until evidence emerges for their prosecution, due to its function as an "auxiliary investigative tool." In 2022, in response to a similar request, the Ministry revealed that, to date, the system had identified approximately 360,000 targets and enabled the recapture of more than 20,000 people.

There are also indications that municipalities, state governments, and other agencies have unrestricted access to *Cortex*, provided they offer something in return, namely access to their own databases. As of March 2023, the MJSP had signed 184 Technical Cooperation Agreements (ACTs) under this model.

On January 10, 2025, the federal government signed a cooperation agreement with São Paulo, Brazil's most populous city, to integrate the *Smart Sampa* cameras—which currently includes more than 20,000—with the *Cortex* Platform.[245] This allows municipal cameras equipped with license plate recognition to access the national database of stolen vehicles, issuing alerts to the appropriate authorities for intervention.

An article in Crusoe magazine on the subject indicated that police officers can even identify, in real time, whether a vehicle was on a particular beach.[246] In more recent news, the same media outlet also revealed that the MJSP has been feeding the *Cortex* with access to student records from municipal education networks.[247]

Since its official launch, civil society has mobilized against the *Córtex* platform. In 2020, after The Intercept published an article about *Córtex*, the Coalition for Internet Rights issued a statement accusing the platform of being incompatible with the principles governing the protection of personal data and of being a tool for the exercise of authoritarianism, something unacceptable in a democratic State governed by the rule of law.[248]

---

243 Valente, R.; Freitas, C.. Ministry of Justice surveillance program allows 55,000 agents to follow "targets" without justification. Agência Pública, 9 oct. 2024.
Available at: https://apublica.org/2024/10/vigilancia-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/#_.

244 Through the Public Agency via the Access to Information Act (LAI).

245 Cidade de São Paulo. Smart Sampa cameras begin reading license plates to identify stolen vehicles. News, January 10, 2025.
Available at: https://capital.sp.gov.br/w/c%C3%A2meras-do-smart-sampa-come%C3%A7am-a-ler-placas-para-identificar-ve%C3%ADculos-roubados-%C2%A0%C2%A0.

246 BIG brother federal. Crusoe. 21 Jan. 2022.
Available at: https://crusoe.com.br/edicoes/195/big-brother-federal/.

247 Valente, R.; Freitas, C.. Ministry of Justice intelligence has access to student records, documents reveal. Agência Pública, February 3, 2025.
Available at: https://apublica.org/2025/02/cortex-ministerio-da-justica-monitora-ate-dados-de-alunos-e-pais/.

248 Coalition for Internet Rights. The federal government's Cortex system threatens citizens' rights. Coalition for Internet Rights, Oct. 1, 2020.
Available at: https://direitosnarede.org.br/2020/10/01/sistema-cortex-do-governo-federal-ameaca-direitos-dos-cidadaos/.

In 2022, the NGOs Data Privacy Brasil, Conectas, Transparency International, and Artigo 19 filed a complaint with the Federal Prosecutor's Office arguing that *Córtex* allowed access to and sharing of personal and sensitive data without effective governance, which would leave room for abuse and illegal monitoring without accountability.[249]

The complaint pointed out that this is a "virtual panopticon" and that the regulatory framework governing *Cortex* is inadequate, indicating that Ordinance 218/2021 fails to clarify the scope of the system and, even less so, the safeguards related to its use. For instance, the Ordinance allows ad hoc decisions on who should be included in the electronic surveillance and does not stipulate basic criteria for due process and ongoing investigation, based on evidence and legitimate reasons for such a violation of fundamental rights, for a person to be constantly monitored by *Cortex*. In the complaint, the NGOs demanded information about the system, as well as the opening of a civil investigation and the necessary steps to clarify the concerns raised. In January 2025, however, the MPF decided to close the investigation, arguing that no evidence of irregularities was found to justify the continuation of the process—the platform operated within a regulatory framework and had internal audit and access control mechanisms.

Newspaper articles warning about the risks and opacity of the system have also been published by Agência Pública and plea Crusoé[250]. In 2024, a new open letter from the Coalition stated that "the *Córtex* system and its current management represent a systematic violation of personal data protection". [251]

249 See: https://www.telesintese.com.br/wp-content/uploads/2022/02/representacao-controle-externo-da-atividade-policial.pdf.

250 Valente, R.; Freitas, C.. Ministry of Justice surveillance program allows 55,000 agents to follow "targets" without justification. Agência Pública, 9 oct. 2024.
Available at: https://apublica.org/2024/10/vigilancia-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/#_.; and Crusoé. Big Brother Federal. Crusoé, 21 Jan. 2022.
Available at: https://crusoe.com.br/edicoes/195/big-brother-federal/.

251 Coalition for Internet Rights. Position statement by the Coalition for Internet Rights and partner organizations on the CÓRTEX system of the Ministry of Justice and Public Security. Coalition for Internet Rights, Nov. 8, 2024.
Available at: https://direitosnarede.org.br/2024/11/08/posicionamento-cdr-entidades-parceiras-sistema-cortex-do-mj/.

In summary

The cases documented in this chapter illustrate the worrying upward trend in the use of technology to obstruct human rights defense and investigative journalism; to attack, censor, repress, and persecute people who reveal information of public interest (particularly those historically excluded); and to preserve a lack of accountability in Latin American contexts with a legacy of repression, impunity, and constant human rights violations.

For example, in **Chile**, the illegal monitoring of social leaders, human rights defenders, and trade unions by the Carabineros was revealed. Similarly, the Western Metropolitan Prosecutor's Office of Chile requested access to sensitive personal data from internet service providers in the context of social and political unrest. In **Colombia**, with regard to cyber patrols and in the wake of various public demonstrations against President Duque's administration, the PMU-Ciber monitored social media, thereby violating the rights of access to information and freedom of expression of millions of people. Similarly, FLIP documented and identified a total of 52 cases of journalists illegally monitored by the National Army in June 2020 using computer tracking software, illegally profiling more than 130 people.

In **Mexico**, there have been reports of illegal access to data held by telecommunications companies to monitor journalists, experts, and social activists, as well as the use of spyware against journalists and human rights defenders who report acts of corruption and human rights violations committed by the State, mainly the Mexican Army. Similarly, in **El Salvador**, the use of *Pegasus* against journalists and members of civil society has also been documented. In **Paraguay**, the acquisition of *FinFisher* spyware was documented, and *Wikileaks* revealed the acquisition of telephone tapping equipment by the Ministry of the Interior.

Furthermore, most of these surveillance measures have been carried out **illegally**, as they have been implemented without complying with the principles of legality, suitability, necessity, and proportionality, and without adequate safeguards, reflecting abuses, lack of transparency, and impunity. In all cases, violations of fundamental human rights such as privacy, personal data protection, freedom of expression, and association were identified, in contexts where those primarily affected are involved in journalism, activism, social movements, and political opposition.

Furthermore, the documented cases also reflect a State and regional trend toward strengthening mass and indiscriminate surveillance, as evidenced by the cases identified involving the interception of private communications in **Colombia**, **Chile**, and **Peru**, as well as access to the retained data records of all mobile phone users in **Paraguay**, **Chile**, and **Mexico**, thereby affecting various freedoms of the majority of the population, including our right to the presumption of innocence, the principle of non-discrimination, and self-determination.

In this regard, worrying patterns were identified not only of collaboration between telecommunications companies and State agencies in private communications surveillance activities, but also of geolocation based on the exploitation of vulnerabilities in telecommunications infrastructure (SS7) and monitoring of public networks.

The case of **Brazil** exemplifies how ABIN illegally used electronic device geolocation tools during the Bolsonaro administration, with *FirstMile* being the main spyware. In **Peru**, the Ollanta Humala administration implemented a mass surveillance system that allowed the interception of communications and the geolocation of thousands of people, even outside the country.

The Brazilian case also illustrates the surveillance of individuals through license plate reading systems that allow for the mass and indiscriminate recording, storage, and systematic analysis of license plates of vehicles circulating in public spaces. These cases highlight the illegal use of surveillance measures by States in collaboration with private actors, thereby violating fundamental human rights.

Finally, cases of information extraction detected in the region using forensic extraction tools, such as the case in Mexico with the acquisition of tools developed by **Cellebrite** and evidence of the use of **Septier** in Paraguay, demonstrate the lack of transparency in the use of these tools by state authorities.

CHAPTER FOUR: DIAGNOSTIC

Technological advances have enabled the use of a broad range of surveillance measures in the region, which are increasingly advanced and invasive, without regulation that keeps pace with these advances to ensure compliance with the international human rights standards set forth in Chapter Two.

In this regard, based on a comparative analysis of regulations on communications surveillance, we have identified a recurring regulatory deficiency in terms of laws that establish in a precise, detailed, and clear manner the authorities, procedures, and circumstances in which surveillance measures may be used.

I. Material jurisdiction requirements

The circumstances or procedures for using communications surveillance measures vary significantly among countries in the region, but they agree that in most cases they are broadly, ambiguously, and/or vaguely defined, leaving citizens defenseless and encouraging discretion and abuse in practice. This is exemplified by legal deficiencies in Brazil, Colombia, Mexico, and Peru.

In the case of **Brazil**, Law No. 9,883/1999 creates the ABIN and aims to establish "the Brazilian Intelligence System, which integrates the planning and execution of the country's intelligence activities, with the purpose of providing support to the President of the Republic in matters of national interest". [252]

Concerns related to state surveillance fall largely within the scope of Brazilian intelligence.[253] The law regulating ABIN defines excessively broad powers, raising concerns about its limits. For example, Article 4 establishes generic powers, such as the collection and analysis of confidential data to advise the President of the Republic; the protection of sensitive information related to State and societal security; and the assessment of internal and external threats to the constitutional order. This broad scope leaves room for extensive interpretation, creating a scenario similar to that of the former National Security Law,[254] which was used to justify abuses during the military dictatorship.

In **Colombia**, the IACHR, in the case *Members of the Collective of Lawyers "José Alvear Restrepo" v. Colombia*, recognized the State's responsibility for abuses of intelligence functions and ordered the reform of Law 1621 of 2013—which regulates intelligence and counterintelligence activities—[255] to include guarantees such as the principles of legality and due process, as well as the need for judicial oversight. A reform bill has now been presented to Congress proposing substantial changes to the law to comply with the Inter-American Court's ruling.

---

252 See: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11693.htm#art21

253 Escola de Ativismo. (2024). Techno-authoritarianism: what does the "parallel Abin" tell us about surveillance mechanisms and democracy? https://escoladeativismo.org.br/tecnoautoritarismo-o-que-a-abin-paralela-nos-diz-sobre-mecanismos-de-vigilancia-e-de-mocracia/) Note: ABIN has a structural and operational legacy (from the National Information Service (SNI), an organ of the dictatorship responsible for the surveillance and repression of militants, activists, political parties, trade unions, the media, and other sectors of society). (https://oglobo.globo.com/politica/noticia/2024/02/04/quais-sao-os-limites-maior-escandalo-da-abin-reabre-discussao-sobre-as-atividades-de-inteligencia.ghtml).

254 Ibíd.

255 Including monitoring of the electromagnetic spectrum and interception of private communications.

In **Mexico**, the clarity and precision of the substantive requirements for carrying out surveillance measures varies within the Mexican legal framework. For example, the CNPP[256] establishes that the admissibility of a request for authorization to intercept private communications, access retained data, or real-time geolocation requires only that the head of the Public Prosecutor's Office "considers necessary" the intervention within an investigation file in which the commission of a crime is being investigated.

The necessity of the measures must be assessed by the competent federal supervisory judge on the basis of objective evidence presented by the authority requesting the authorization. However, the wording differs excessively from that used by the authority itself to justify the relevance of a surveillance measure.

In **Peru**, Legislative Decree No. 1141—which regulates the functioning of the National Intelligence Directorate (DINI) and the National Intelligence System (SINA)— establishes that intelligence activities must be carried out with respect for human rights, but sets very vague limits and lacks effective mechanisms for external control and oversight, thus allowing wide margins for abuse.

Similarly, Legislative Decree No. 1182 (known as the Stalker Law) requires operators to retain massive traffic and location data on all users for three years, without reasonable criteria of proportionality or necessity. In addition, recent reforms have expanded the circumstances in which the police can request this data, further weakening judicial guarantees and citizen control.[257]

In many cases, authorization to access information is granted by a higher-ranking official within the same entity that makes the request. This dynamic is found in countries such as Brazil (with ABIN and the police), Mexico (through the LGN), Peru (through the PNP and OSIPTEL), and Colombia (with the Armed Forces, the National Police, and the National Intelligence Directorate). This concentration of functions has raised concerns, as there is no independence between those who investigate and those who must authorize such measures, which can lead to abuse or lack of external control.

Consequently, legal frameworks should provide for a civil institution that is independent of intelligence services and the Executive Branch, with technical expertise, to monitor and hold accountable the authorities responsible for transparency and accountability.

II. Judicial oversight

As mentioned in the first and second chapters, judicial authorization of surveillance measures is a fundamental guarantee for preventing abuse, arbitrariness, and discretion on the part of the authorities. Therefore, the laws of **Paraguay** and **Peru**, which do not establish the requirement of prior judicial oversight, are particularly concerning.

Based on Legislative Decree No. 1182, known as the "Stalker Law," **Peru** authorizes the National Police to access real-time geolocation data without a prior court order in cases of alleged criminal flagrancy.

256 Article 291.

257 There is at least one relevant lawsuit related to this regulation: a lawsuit to obtain access to the PNP's internal protocol on how geolocation is requested and processed without a court order. Result: the request was denied, and the protocol remains confidential, reflecting a lack of transparency, institutional opacity, and absence of democratic control over this form of surveillance.

On the other hand, even if the legislation of countries in the region establishes the need for prior judicial control, significant challenges have arisen with the provision of exceptional mechanisms, as is the case in **Brazil**, **Mexico**, and **Paraguay**.

Thus, although **Brazil** requires judicial authorization for both metadata and geolocation information,[258] it also provides that if the court does not rule within 12 hours, the Public Prosecutor's Office or a police officer may request the data directly from telecommunications and telematics companies.

Similarly, ABIN—the main state entity authorized to carry out surveillance activities for intelligence purposes—does not have the prerogative to intercept communications without judicial authorization. However, it can access information obtained by other Sisbin[259] agencies through cooperation mechanisms established in current legislation.

In **Mexico**, although Article 16 of the Constitution establishes the need for federal judicial authorization to carry out the interception of private communications, the exceptional mechanism established in Article 303 of the CNPP empowers prosecutors to request access to retained data or real-time geolocation from telecommunications companies without first obtaining judicial authorization, but with the burden of requesting ratification of the measure within 48 hours of the original request.

This has led to the exception becoming the general rule and a significant number of requests made under the exceptional mechanism not being ratified by the federal judicial authority—or not even being submitted for ratification—thus allowing authorities to invade the privacy of telecommunications users illegally and with impunity, without the affected person or a judge even being aware of it.

In **Paraguay**, although Article 200 of the Criminal Procedure Code establishes that the interception of communications requires a well-founded decision by a judge, Article 228 grants both the judge and the Public Prosecutor's Office the power to request reports from public or private individuals or entities. These reports may be requested verbally or in writing, specifying the relevant procedure, the name of the accused, the place of delivery, the deadline for submission, and the consequences of non-compliance. This allows access to data held by telecommunications companies without the need for judicial authorization.

III. Proliferation of mass surveillance technologies

Based on the principles of necessity and proportionality, surveillance measures can only be considered legitimate if they are the least harmful alternative available to achieve a legitimate objective and if, after careful consideration, the impact on privacy and security is not excessive or disproportionate to the benefits obtained from the proposed surveillance.

The growing proliferation of surveillance equipment and systems such as fake antennas and spyware, which, in addition to being operated autonomously, without the need for collaboration from any entity and possessing extensive intrusive capabilities, contain measures to hinder their detection, is indicative of the lack of clarity and precision regarding the surveillance methods that can be considered compatible with the human rights standards recognized in the constitutions of the countries of the region.

---

258 In accordance with Article 10, § 1 of the Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014) and Article 13-B of the Code of Criminal Procedure.

259 ABIN is part of the Brazilian Intelligence System (Sisbin), which comprises various federal government agencies responsible for producing information relevant to intelligence activities. The operation of SISBIN is regulated by Law No. 9,883/99 and Decree No. 11,693/23.

The problem is exacerbated when there is not only a lack of regulation of these new technologies, but also a tendency on the part of some countries in the region to legitimize mass and indiscriminate surveillance measures that are incompatible with international human rights standards.

For example, in **Chile**, the recent enactment of Anti-Terrorism Law No. 21,732 of February 2025 is causing concern. This law authorizes the use of technologies such as *IMSI Catchers* and aims to "determine, record, and monitor" data that allows for "singling out or identifying one or more devices" or facilitating their geolocation.[260]

Among the risks identified in the use of this type of mass surveillance technology, it is noted that it is not only indiscriminate surveillance technology, but also extremely disproportionate, as it captures the signal of all devices near the fake antenna, thereby impacting the privacy of third parties who are in no way related to the ongoing criminal investigation, and which in practice legitimizes so-called "miracle fishing."

In **Colombia**, Article 15 of Resolution 5839 of 2015 of the National Police establishes the functions of the Police Cyber Center, which include, in point 12, the "conduct of 24/7 cyber patrols on the web for the purpose of identifying threats from and to the detection of common factors in incidents of which they are aware, as well as the violation of the availability, integrity, and confidentiality of information circulating in cyberspace."

Similarly, in **Mexico**, Article 9, section XXXVII, of the National Guard Law empowers this militarized institution to carry out *"surveillance, identification, monitoring, and tracking on the public Internet network on websites, in order to prevent criminal conduct."* The vagueness with which this power is described does not allow for a clear determination of its scope. However, it could be understood that this power is intended to provide a basis for open-source investigation and profiling of Internet users.

IV. Lack of transparency and corruption in the acquisition of surveillance technologies

At the global level, and in the region, the processes for contracting communications surveillance equipment and systems have been characterized by opacity, discretion, and the absence of adequate regulation and controls to inhibit corruption, illegal surveillance, and impunity.

For example, in **Paraguay**, the Itaipú Technology Park Foundation (PTI) is ongoing with a controversial tender launched in April 2015 for espionage equipment valued at USD 12 million, which has been denounced for irregularities by Congressman Mauricio Espínola.[261] Among the bidding companies are ITTI Saeca and Technoma, both linked to the Vázquez Group and President Santiago Peña, as well as TSV SRL, a firm with a history of collusion and that has benefited from multiple state contracts.[262]

260. Available at: https://www.bcn.cl/leychile/navegar?idNorma=1211036

261 Ultima Hora (2025) Two firms linked to Peña, and one with a history, are competing in PTI. Available at: https://www.ultimahora.com/dos-firmas-ligadas-a-pena-y-una-con-antecedentes-compiten-en-pti

262 ABC Color (2025) Opening of bids for listening devices at the PTI postponed. Available at: https://www.abc.com.py/este/2025/04/11/postergan-apertura-de-sobres-de-ofertas-en-licitacion-de-aparatos-de-escucha-en-el-pti-en-la-que-compiten-firmas-ligadas-al-presidente-santiago-pena/

The tender includes a comprehensive espionage platform that incorporates technologies such as lawful interception systems, *IMSI Catchers* for tracking mobile devices, digital forensic analysis kits (such as *Cellebrite* or similar), facial recognition software, OSINT tools for monitoring social media and open sources, satellite geolocation equipment *(GPS Trackers)*, and acoustic surveillance technology. According to more than 130 protests, the technical specifications of the equipment are designed to exclusively favor the company ITTI Saeca.

In **Brazil**, given the regulatory vacuum, the Inspector General's Office (PGR) filed Direct Action of Unconstitutionality by Omission No. 84 before the Federal Supreme Court (STF) in December 2023, which was converted into Allegation of Breach of Fundamental Precept No. 1,143.263

The action questions the possible lack of legislation on the purchase and use of spyware and requests that the STF: (i) recognize Congress' failure to regulate the use of spyware; (ii) establish a deadline for its regulation; and (iii) implement provisional measures to ensure the protection of privacy and data secrecy. The case is still pending.

In 2024, Presiding judge Cristiano Zanin, of the Supreme Federal Court, convened a public hearing on ADPF 1.143, with the participation of 33 civil society organizations to contribute to the debate on the purchase and use of these surveillance technologies. InternetLab, together with Data Privacy Brazil, participated in the public hearing as a*micus curiae* and presented their arguments.264 They also highlighted that the absence of regulation on these tools undermines public trust in democratic institutions, as it opens the door to abuses of power.

In **Mexico**, through requests for access to information, investigative journalism, and information leaks, the following have been identified as the main irregularities in the procurement processes for surveillance equipment and systems: (a) discretion and awarding contracts to companies with irregularities (in direct award processes with companies without a track record or experience in the field); (b) overpricing in procurement (exorbitant amounts and unreasonable conditions); (c) contracts that seek to be hidden or obscured by vague descriptions of the subject matter of the contracts; (d) absence of controls to prevent the illegal acquisition of surveillance technologies; and (e) absence of documentation on the acquisition and use of surveillance equipment and systems.

Therefore, it is essential that the region require special procedures or authorizations that do not involve only the contracting authority and companies.

263 See: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814

264 InternetLab. (2024). Use of spy technologies: InternetLab and DataPrivacy Brasil contribute as amicus curiae and participate in public hearing in case before the Federal Supreme Court. InternetLab. https://internetlab.org.br/pt/noticias/uso-de-tecnologias-espias-internetlab-e-dataprivacy-brasil-contribuem-como-amicus-curiae-e-participam-de-audiencia-publica-em-caso-no-stf/

CONCLUSIONS

The cases outlined in Chapter Three represent only a small sample of a history of surveillance abuses by Latin American countries, whether in the form of mass and indiscriminate collection of our sensitive personal data, cyber patrols, the use of spyware against civil society, or many other abuses that have been reported.

Such practices **dismantle civic space**, especially digital space, impacting our freedoms and autonomy. For example, the case of Colombia is representative of the way in which public security and intelligence agencies contract private services to profile and monitor millions of people on digital platforms, under the pretext of crime prevention and investigation, but with the aim of collecting information for the purpose of controlling and repressing criticism of the government, as well as spreading disinformation. Such contexts create a climate of digital mistrust that restricts expression, as people self-censor or limit their digital participation.

Similarly, the **use of intrusive state surveillance measures** (in theory exceptional) has been normalized with populist rhetoric that "we have nothing to hide" in order to control, censor, and repress citizens. The case of Brazil is emblematic in terms of the use of geolocation systems, both through the exploitation of SS7 and through license plate identification systems, highlighting the extent to which the privacy and freedom of movement of millions of people can be affected, drawing up exhaustive profiles based on their movements and routines, including journalists, activists, public officials, and individuals associated with criminal investigations against relatives of then-President Bolsonaro.

By undermining activities such as journalism, the defense of human rights, and the integrity of democratic institutions, **illegal surveillance often harms society and its democratic aspirations**, allowing those who engage in surveillance with impunity to exercise undue control and influence over society and its institutions. The case of El Salvador is a clear example of how surveillance of journalists compromises their sources, putting at risk the disclosure of their identity and even their physical safety. In Mexico, there is abundant evidence of the repeated illegal use of communications surveillance tools against journalists, human rights defenders, activists, and political opponents.

In addition, it is crucial to recognize that illegal surveillance is often accompanied by other forms of intimidation, ranging from attacks on reputation, extortion, raids, infiltration, or psychological operations to encouraging or facilitating physical attacks, including murder.

RECOMMENDATIONS TO THE STATES

In order to avoid legal uncertainty and discretion in the deployment of surveillance measures, legal frameworks need to establish fundamental aspects more precisely, such as the identification of the competent authorities. In addition, the parameters and material limits that must inform requests for authorization of surveillance measures and the judicial decisions resolving such requests should be defined more precisely, in order to ensure greater predictability regarding the scope of these measures.

The rules governing surveillance in regional legal frameworks were designed with telephone tapping technologies and other forms of targeted surveillance in mind, which required the cooperation of private parties, especially telecommunications companies. As a result, traditional methods of communications surveillance provided considerably less information about the persons under surveillance and inevitably produced witnesses, such as telecommunications companies.

However, the proliferation and everyday use of increasingly sophisticated and invasive mass surveillance technologies indicate that current regional legal frameworks have not been able to ensure their rational use or even the possibility that such technologies may be compatible with the principles of necessity and proportionality set out in Chapter One.

Consequently, we require political will at the State level to ensure compliance with the principles of legality, necessity, and proportionality, in line with international human rights standards for communications surveillance, requiring that all national legal frameworks provide for:

- **Laws with clear, precise, and detailed** definitions of the empowered authorities, the procedure and circumstances in which surveillance measures may be carried out, as well as a record and control of the deployment of state surveillance measures.

In line with the principles of legality, legitimate purpose, necessity, and proportionality mentioned in Chapter One, sufficient clarity is required to prevent abuse in the acquisition and use of such surveillance technologies, where they are targeted at specific individuals and limited to circumstances where there are indications or probable causes of the commission of a crime or a threat to national security.

- **Effective regulation of the procurement processes** for communications surveillance equipment and systems, including registration and control.
- **Transparency** measures, because even though communications surveillance is often related to the investigation of crimes and threats to national security, for which a certain degree of secrecy is necessary for effectiveness, transparency is essential to prevent and detect abuses, as well as to assess, on the basis of evidence, whether the public interest objectives that are frequently invoked to justify communications surveillance are achieved or whether the deployment of such measures involves acts of corruption or inadequate controls against potential abuses.

The fact that many of these technologies are used autonomously by the attacking authority, coupled with their anti-forensic and anti-detection features, poses a huge challenge to preventing their illegal use. Therefore, establishing obligations to publish statistical reports with disaggregated information on their use is particularly relevant to prevent, detect, and remedy abuses committed through illegal communications surveillance.

- Provision of **safeguards** such as judicial oversight, independent oversight, and the right to notification.

In this context, actions such as those taken in Brazil are welcome, where civil society organizations requested during the public hearing on ADPF 1.143 that, if the STF does not declare the use of spyware by public bodies to be totally unconstitutional, strict rules be established to prevent its abuse. They also defended the requirement of prior judicial authorization for any monitoring; the restriction of the use of spyware only when no other investigative means are available; the protection of the secrecy of communications; and the implementation of mechanisms to ensure the traceability of the chain of custody of intercepted data.

In Latin American countries, with a legacy of authoritarianism and repression of dissent, we must change narratives and public perception towards a shared understanding where we equate our privacy with our security, because surveillance without controls by Latin American authorities plagued by impunity and corruption only implies greater control to inhibit criticism of the government and generate fear, rather than providing greater security to the population.

AlSur

www.alsur.lat