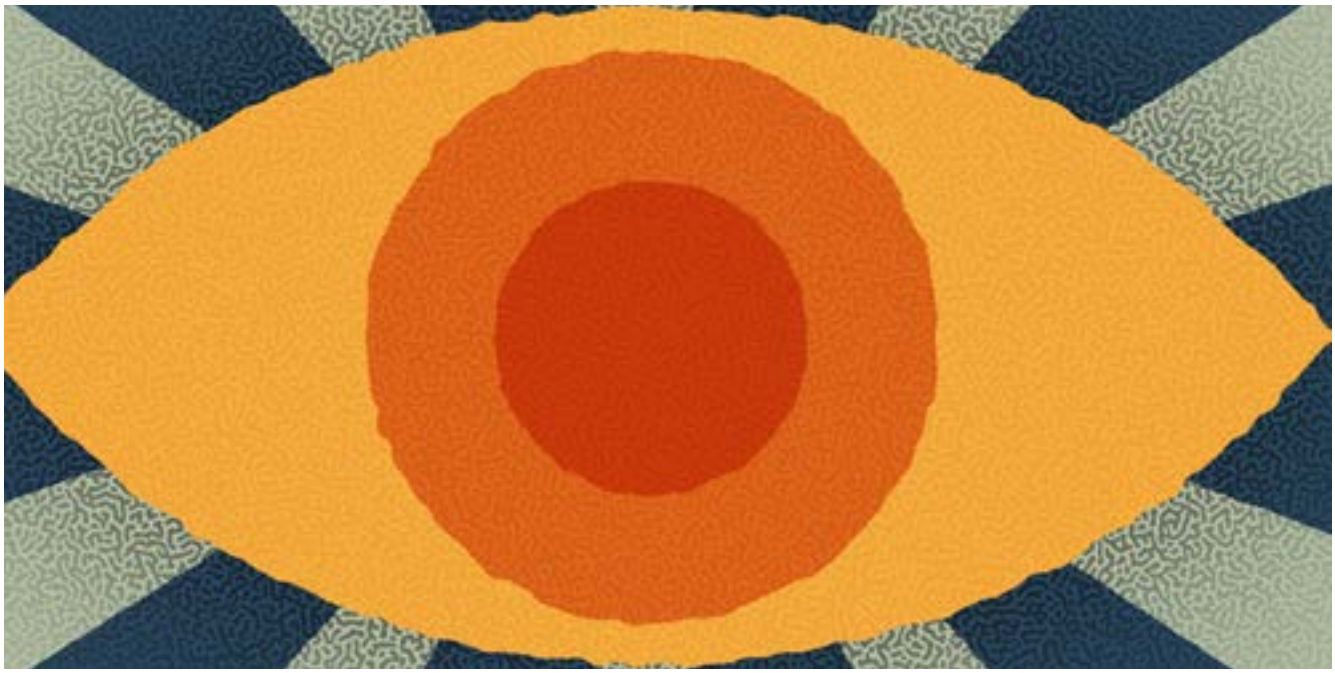

Tackling Arbitrary Digital Surveillance in the Americas

Essential Safeguards and Institutional Measures for State Security Activities to Fulfill Privacy and Information Rights

VERIDIANA ALIMONTI
Associate Director for Latin American Policy

May 2026

ELECTRONIC FRONTIER FOUNDATION

Author: Verdiana Alimonti

A publication of the Electronic Frontier Foundation, 2026.

EFF's Senior Speech and Privacy Activist, Paige Collings, copyedited this guide. EFF's Senior Counsel, David Greene, reviewed its content. EFF's Design Manager, Kim Carlson, formatted this guide. EFF's Senior Translations Manager, Carlos Wertheman, translated it into Spanish.

View this report online: https://www.eff.org/wp/tackling-arbitrary-digital-surveillance-americas

CONTENTS

INTRODUCTION

Across the Americas, poor accountability, feeble control mechanisms, and insufficient legal frameworks constantly lead to human rights violations in the context of public security, law enforcement, and intelligence activities. The increased capabilities of digital surveillance are a central part of current abuses, such as the ability to profile and classify individuals; monitor people's movements, relations and routines; tap into different kinds of communications; and infer or presumably predict behaviours with harmful consequences to people.

In response, the Electronic Frontier Foundation has compiled this guide focusing on data privacy and access to information guarantees to provide concrete, actionable guidance to governments in the Americas to curb the vicious cycle of state digital surveillance abuses. This document outlines which safeguards and institutional measures should be in place to protect individuals across the region; and details the rules, parameters, and standards established within the Inter-American Human Rights System as an input to overcoming current pernicious practices and trends. While it pinpoints essential required guarantees, it does not intend to be exhaustive or exclude other important measures not explicitly mentioned on these pages.

This guide builds upon a comprehensive legal foundation pertaining to the protection of individuals in the face of state digital surveillance and security-related activities. Recent findings from the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights ("IACHR", "Inter-American Commission" or "Commission") concluded that:

> *"[D]igital surveillance technologies have become a systemic threat to human rights across the Americas, fundamentally altering*

> *the relationship between states and their citizens. The evidence presented in this report demonstrates that surveillance practices previously considered exceptional under international human rights law have become increasingly normalized, creating a permissive environment for continuous violations of fundamental rights."*

The Special Rapporteur emphasized that the systematic nature of surveillance across the region reveals fundamental gaps in legal frameworks, oversight mechanisms, and accountability systems that must be addressed holistically. As the Rapporteur pointed out, the result is not only individual rights violations but the systematic erosion of democratic institutions and the rule of law.

Over a decade ago, the Inter-American Commission's report on citizen security and human rights similarly stressed human rights as essential limits to prevent that the powers granted by law to state agents to defend everyone's security are, instead, used by security forces to subjugate people's rights. Therefore, the guarantees enshrined in the American Convention on Human Rights serve as guide for security forces' activities in their compliance with human rights.

Furthermore, the Inter-American Court of Human Rights ("Inter-American Court" or "Court") has interpreted the Convention to establish crucial parameters for fulfilling conventional rights and principles in the face of state surveillance. Particularly, the Court's sentence in the Case of Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia (*CAJAR v. Colombia*) elaborated on conventional guarantees to set forth fundamental rules and criteria to ensure privacy and information rights in state security actions. While this case addresses intelligence activities more specifically, the safeguards the ruling lays down are a critical baseline for state digital surveillance and security-related activities more broadly.

Three other important references given the scope of this guide are the Necessary & Proportionate Principles on the application of human rights to communications surveillance, the Compilation of Good Practices to guarantee human rights by intelligence agencies, and the Tshwane Principles on national security and the right to information. Throughout the document we highlight relevant connections with the Necessary and Proportionate Principles, which should be considered by readers together with this guide.[1]

Taking concrete steps to implement what follows should not be seen as an act of goodwill, but as states' duty under their commitments to international human rights law.

---

1 The 13 Principles are: Legality, Legitimate Aim, Necessity. Adequacy, Proportionality, Competent Judicial Authority, Due Process, User Notification, Transparency, Public Oversight, Integrity of Communications and Systems, Safeguards for International Cooperation, and Safeguards Against Illegitimate Access and Right to Effective Remedy.

1. Data Privacy Protections in the American Convention on Human Rights

The right to private life has a comprehensive scope under the American Convention. **Article 11 prohibits any arbitrary or abusive interference in a person's private life, including the privacy of their family, home, correspondence, and communications.** This protection encompasses both what people communicate and the metadata unfolding from the communication or digital interaction process.

The protection of private life directly relates to safeguarding personal autonomy, personal development, and the right to establish relationships with other people and the external world. The extent of information that institutions know about someone and how they process such data can deeply affect the course of a person's life and their social interactions.

In this sense, the Court stressed that private life includes the way individuals see and decide to project themselves towards others. It has an intrinsic connection with dignity and self-determination, upholding people's ability to freely choose the options and circumstances that give meaning to their existence based on their preferences, values, and convictions.

Accordingly, the Court emphasized that self-determination encompasses people's freedom to decide when and how much to reveal matters of their personal lives, including what type of information others may know about them. The ruling *CAJAR v. Colombia* specifically noted the importance of these guarantees to safeguard children's rights, highlighting privacy as a critical determinant for the full development of their personality and future life.

However, the right to private life is not an absolute right, and may be restricted provided limitations are not abusive or arbitrary. For that, permissible interferences must be properly established in law, seek a legitimate purpose, and be suitable, necessary, and proportionate in a democratic society to fulfill specific legitimate aims. This is known as the three-part test.

Meeting these requirements involve a pivotal set of steps, measures, and guardrails that the Inter-American Court, the Inter-American Commission, and the Office of the Special Rapporteur for Freedom of Expression have stressed, and that we outline below.

2. Vital Privacy Safeguards Under State Digital Surveillance

Citing the European Court of Human Rights, the Inter-American Court's sentence in the case *CAJAR v. Colombia* reiterated that the mere existence of legislation allowing for a system of secret monitoring of people's communications amounts to an interference with the right to privacy. It also affects the right to freedom of thought and expression, as the right to privacy is deeply interlinked with the free development and exchange of ideas.

The Office of the IACHR Special Rapporteur for Freedom of Expression underscored the urgent need, in the Americas, for comprehensive mechanisms to prevent surveillance abuses before they occur, detect them when they happen, and provide effective remedies to victims and punishment to responsible agents.

The safeguards required to rein in abusive digital surveillance encompasses laws with clear limits and definitions, guardrails based on solid necessary and proportionate analysis, concrete controls, and empowered independent oversight.

THE BLACK BOX OF INTELLIGENCE ABUSES

While state surveillance is generally shaded in secrecy, there's a higher normalization in concealing public interest information, such as regulations, protocols, statistics, budget expenditure, and technologies in use, when they relate to intelligence agencies or activities. Also, knowing you were targeted by intelligence surveillance, even after any scrutiny or suspicion is over, is significantly harder, if not impossible. The Court's ruling in *CAJAR v. Colombia* is of special importance for stressing that intelligence activities don't fall outside human rights obligations, and for specifying both their scope and legitimacy test.

The ruling **defines intelligence activities** in general terms as actions designed to collect, analyze, and disseminate information to support decision-making by entities responsible for implementing security policies. It distinguishes the tasks of intelligence agencies from those proper to public safety, emphasizing the greater risk of arbitrariness and the violation of human rights when the same institution conducts both types of tasks. In this sense, intelligence services must not hold powers of arrest, detention, or law enforcement over individuals.[2]

2 Relatedly, the Inter-American Commission emphasized that states should establish a clear distinction, in their domestic legal framework, between functions of national defense, often undertaken by military forces, and those of citizen security, handled by police forces. Considering the nature of each force and the region's negative

Intelligence agencies must not conduct pre-trial investigations either, which would implicate the erosion of due process guarantees. While both criminal investigations and intelligence operations work to find and process information, and both may share methods to capture and analyze data, they pursue essentially different purposes. Intelligence services do preventive work, not direct enforcement of criminal laws.

As the Court puts it, such preventive work aims at the security and protection of society and the population. It clearly states **what must be the ultimate purpose of intelligence activities:** "[they] must necessarily be conducted for the ultimate purpose of protecting the people living in the national territory, [which] includes safeguarding their rights and freedoms." Therefore, the multiple tasks these activities involve are only useful and necessary to the extent they serve to satisfy this foundational goal. On the contrary, if intelligence actions systematically endanger people's lives and freedoms, persecute and strive to quash criticism, or in other ways jeopardize people's rights and democratic societies, then they lack their primary legitimate ground and are not compatible with international human rights law.

2.1. Clear and Precise Legal Framework

Any limitation to privacy and related guarantees must be prescribed by law, enacted by the legislative branch, and accessible to the public. Some important guidance unfolds from this basic principle:

- The legal framework authorizing and regulating state surveillance, including intelligence activities, must never be kept confidential.
- The law must define the scope of surveillance activities, their intended purpose, and the powers of competent agencies and authorities in a clear and precise manner, sufficient to ensure that individuals have advance notice of and can foresee its application *(see 3. Transparency and Participation)*.
- Robust legal protections must follow the pace of technological developments, and periodic reviews should result from a participatory legislative or regulatory process.

The Court stated that intelligence laws must establish, as precisely as possible: the different threats that could trigger the need for intelligence activities, along with a clear and exhaustive specification of the powers granted to state agents conducting

background relating to military intervention in internal security matters, such a framework should exclusively entrust functions pertaining to prevention, dissuasion, and legitimate repression of violence and crime to police forces, commanded by legitimate authorities of a democratic government. IACHR, Informe sobre Seguridad Ciudadana y Derechos Humanos, 2009, Recomendaciones específicas (B), item 10. Available at https://hchr.org.mx/publicaciones/nforme-sobre-seguridad-ciudadana-y-derechos-humanos-2009/

these activities. The threats laid out in domestic law must respond to factors or situations that can, rationally and specifically considered, jeopardize legitimate aims. The law should indicate, then, both legitimate aims and potential specified threats against them *(see 2.2. Legitimate Aims)*.

Domestic legislation must also provide a "well defined, comprehensive system to authorize, oversee and supervise intelligence activities in concrete situations." Drawing on intelligence actions and strategies to obtain and compile information, such legislation must set out, as precisely as possible:

- the types of intelligence measures and actions authorized for collecting and compiling information;
- the permissible aims justifying these measures;
- the categories of persons and activities on which agents may collect and compile information, always based on the identification of threats to legitimate ends priorly defined;
- the threshold of suspicion to justify the use of information collection and compilation measures, following necessary and proportionate standards;
- time limits for carrying out information-gathering measures and strategies; and
- procedures for authorizing, reviewing, and overseeing such measures and actions.

If domestic law authorizes **information-sharing among national or foreign intelligence and security agencies**, it must also outline clear parameters for such exchange, including permissible purposes, authorized entities, and applicable safeguards.

The following sections on "legitimate aims," "adequate, necessary, and proportionate," and "additional safeguards for personal data processing" detail important aspects on how domestic legislation should consider or address certain concepts and required provisions.

2.2. Legitimate Aims

The activities of security forces must pursue aims that are legitimate and necessary in a democratic society. This condition applies to state surveillance operations and the way they interfere with privacy and data protection. Generally, the American Convention considers as legitimate ends those of preserving national security, maintaining public order, safeguarding public health, and protecting human rights.

Yet, in the ruling *CAJAR v. Colombia*, **the Court stressed the dangers of using vague and unspecified notions to justify intelligence actions, and clarified some important aspects for circumscribing the scope of legitimate aims**. For instance, preserving national security may involve the protection of the very existence of the nation, its territorial integrity, or its political independence against specific defined threats. In turn, protecting human rights must refer to situations that constitute a concrete risk to effectively exercising or ensuring certain rights.

A critical foundational assessment for any of the legitimate ends the Convention mentions is their connection to upholding democratic societies. As the Court pointed out:

> *"[T]hese goals become 'legitimate aims' to the degree that they correspond to the purpose that ultimately underlies and guides the existence of a rule of law, that is (...) 'the protection of the essential rights of man and the creation of circumstances that will permit him to achieve spiritual and material progress and attain happiness'."*

This relates to what we noted above for intelligence activities, and which broadly applies to state security forces—their ultimate purpose under international human rights law is to protect people, their rights and freedoms within a democratic society. **If state security practices stray from that, then they are the threat to what they were supposed to protect, and must be tackled as an illegitimate and abusive exercise of power.**

Two crucial and interlinked conclusions unfold:

- First, legitimate aims **proscribe any security activities with discriminatory purposes**[3] based on race, color, sex, language, religion, political or other opinions, national or social origin, economic status, birth, or any other social condition. Intelligence operations must not have the goal to promote, benefit, or affect a particular activity, person or group based on such attributes.
- Second, security agencies **must not conduct activities with the intent of neutralizing, persecuting, or attacking opposition or dissent.** Political pluralism is vital for democracy, a value that Articles 13, 16, and 26 of the American Convention undergird.

3 See more about inter-American standards on equality and non-discrimination at www.eff.org/document/human-rights-standards-government-use-ai-latin-america-appendix (section 4.3. Equality and Non-discrimination).

2.3. Adequate, Necessary, and Proportionate

Any digital surveillance operations by state security forces must be necessary in a democratic society. This implies a proportionality test based on criteria to be properly specified in domestic legislation. **Competent authorities should carry out this analysis before authorizing or implementing surveillance tasks in concrete cases, including as part of intelligence activities.**

The analysis should consider the legal basis underpinning surveillance activities, the specific legitimate aims they pursue, and whether they fulfill the following conditions:

- surveillance is adequate to address specific threats or harms to legitimate aims;
- surveillance is not just useful, but strictly necessary, and the particular actions or methods employed are essential to tackle specific threats or harms to legitimate ends, meaning that there's no viable, less invasive alternative available capable of achieving the same objective;
- surveillance actions are strictly proportional—that is, the inherent sacrifice of restricting rights is not excessive or disproportionate relative to the gain of safeguarding specific legitimate aims in the concrete case.

The power to authorize digital surveillance measures lies with the judicial authority, who should rigorously conduct the proportionality analysis *(see 2.4.(i) Prior Judicial Order)*.

These requirements are in line with principles 3, 4, and 5 of the Necessary and Proportionate Principles on the application of human rights to communications surveillance, which raise additional critical guidance. Among others, it's important that:

- The information accessed is confined to what is relevant and material to the threat or serious crime, and that any excess information collected is not retained.
- Only the competent specified authorities have access to the information, and use it only for the purposes and duration for which the judicial authority authorized.

2.4. Essential Controls

(i) Prior Judicial Order

According to the Court, **the effective protection of privacy and freedom of thought and expression requires a prior judicial order to any communications surveillance measure.** It is also mandatory as a general rule to obtain a proper judicial

authorization for searches or raids of private homes or facilities.

As the Court extensively exemplified in *CAJAR v. Colombia*, **communications and digital surveillance measures requiring a previous judicial order encompass** interception, any kind of communications monitoring or surveillance—either by telephone, data transmission, or other networks—electronic recording, including audiovisual media, the collection of data held by private individuals or companies, as well as access to databases and non-public information systems that store and process personal information, tracking users in the network or locating electronic devices. As such, the Court stated that techniques or methods for gaining access to computer metadata and system data, such as email, metadata from "Over the Top" applications, location data, IP addresses, cell phone towers, cloud-based data, GPS, and Wi-Fi would demand a prior judicial order.

Current digital surveillance technologies are capable of processing a scattered and massive amount of data, making it easier and faster to categorize and profile individuals and groups with significant impact on their lives. The need to strengthen protection for sensitive personal data underscores how essential judicial orders are for authorizing digital surveillance.

The Court highlighted that **sensitive personal data** affects "the most intimate aspects of natural persons," and may include data related to an individual's personal health, sex life or sexual orientation, religious, philosophical or moral beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, political opinions, racial or ethnic origin, financial account information, official documents, information collected from children, or personal geolocation.

The work of journalists and lawyers also requires a reinforced level of protection as to surveillance operations. The Court pointed out that it's imperative to limit intelligence activities to safeguard the secrecy of journalists' sources and to protect the confidentiality of all communications between lawyers and their clients within their professional relationship.

The Court emphasized that requiring judicial authorization for digital surveillance is consistent with the role of judges as guarantors of human rights in a democratic system. The judicial authority must be independent and, as such, is able to ensure objective oversight of other public entities and authorities as to their compliance

with the law.[4]

As the Court pointed out, the judicial authority is responsible for considering the circumstances of the specific case, assessing compliance with pre-established requirements and the proportionality test.

In this sense, the prior judicial order must:

- be fully substantiated, in order not to be arbitrary, posing rational arguments to demonstrate that has weighed all constitutional, legal, and conventional requirements, including the three-part test (see previous sections), along with other material that, as relevant, justifies the decision to authorize or deny the surveillance measure;
- define limits as to nature, scope, and duration of the measure authorized based on necessary and proportionate criteria.

(ii) Step-by-step Records

The Court has further detailed **specific recording controls** for intelligence activities that should inspire the implementation of procedures for the effective supervision of security forces' surveillance operations in general. As the Court underlined, establishing effective controls to surveillance actions is needed to avert abuses or arbitrary practices by authorities.

Particularly, the Court held that **state authorities should formalize intelligence activities through step-by-step processes**. This means that:

- Authorities must duly record each stage of their operations, including a timeline and a log of access to electronic systems.
- When agencies process personal data, they must ensure important safeguards ***(see 2.6. Additional Safeguards for Personal Data Processing)***, which means, as much as possible, keeping records indicating:
    - the identity of the people responsible for data processing;
    - the purposes for processing the information compiled, indicating the

4 In examining the concrete case in the ruling *CAJAR v. Colombia*, the Court stressed that the full spectrum of surveillance actions "took place in the absence of authorization or control by any judicial authority, even though it was a judicial prerogative to examine whether the measures were proportional in the particular case and to rule on the means, times, scope and limitations to be put in place for safeguarding the rights of the persons affected". Therefore, the Court concluded that "[t]his failure of judicial authorization was incompatible with the American Convention, inter-American case law and the international standards detailed above (supra paras. 547, 548, 551 and 553)". Case of Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia, Preliminary Objections, Merits, Reparations and Costs, Judgment of October 18, 2023, para 624.

origin and category of the data;

- the legal basis for the operations;
- the retention period for the material;
- the data processing methods used.

- Authorities must also report operations in chronological records of access, modification, queries, erasure, and data-sharing along with the names of all persons who gained access to them.

Accordingly, **domestic laws and regulations** must stipulate such specific processes for controlling surveillance activities. The Court highlighted that **agencies must include these processes in regular reports they send to oversight bodies** *(see 2.5. Independent Civilian Oversight)*.

(iii) Notification Systems

The Office of the IACHR Special Rapporteur for Freedom of Expression stated that the detection of human rights violations in the context of digital surveillance **requires notification systems that inform individuals when they have been subjected to surveillance**. In this sense, the Special Rapporteur recommended Member States of the Organization of the American States (OAS) to provide notification mechanisms for individuals targeted by surveillance.

The Special Rapporteur's recommendation connects with principle 8 of the Necessary and Proportionate Principles on the application of human rights to communications surveillance. The principle indicates that notice should occur with enough time and information to enable individuals affected to challenge the decision or seek other remedies. It also states that delay in notification should only occur when such notice would critically jeopardize the purpose for which the surveillance was authorized, or there is an imminent risk of danger to human life.

Notification is a crucial measure for ensuring the right to an effective remedy in case of surveillance abuses *(see 4. Remedy and Reparation)*. Accordingly, the Court held that the need to ensure the right to an effective remedy led international standards to call for states to notify persons affected by surveillance after its completion. Without notice, people may never become aware of arbitrary or disproportionate information-gathering procedures impinging on their rights, which poses critical barriers to the investigation of human rights violations, adequate redress, and non-repetition.

2.5. Independent Civilian Oversight

A fundamental piece in the architecture of safeguards is ensuring independent and empowered oversight of state digital surveillance. **State surveillance requires not only rigorous internal supervision of the body conducting the surveillance, but also external oversight from an independent institution.** This should exist in addition to prior judicial orders for surveillance measures and other procedures of judicial control.

The Court detailed this requirement for intelligence activities, stressing it must be a civilian institution independent of both intelligence services and the executive power, reporting to the legislative, administrative or judicial authorities.

The institution should have technical know-how and all the powers needed to perform its duties, which includes full, direct access to the information and data required to accomplish its mission. Therefore, the independent institution should have the power to monitor:

- compliance with the legal framework applied to agencies' activities, including human rights instruments;
- how efficient and effective their activities are, with related performance assessments considering the legitimate aims pursued;
- agencies' financial and budgetary status, and fund management;
- agencies' administrative methods and practices.

Relatedly, the Inter-American Commission recommended states to establish independent control and supervision mechanisms for citizen security. It has also held that states should strengthen parliaments' technical capacity to assess and carry out political control over public security policies.

The Office of the IACHR Special Rapporteur for Freedom of Expression highlighted that efforts to establish an independent civilian oversight authority should include considering the role of **vulnerabilities equities processes (VEPs).**

As the Special Rapporteur explained, VEPs are governmental processes through which a state decides whether to disclose newly discovered software vulnerabilities with affected companies for patching, or to withhold them for operational purposes. State exploitation of vulnerabilities includes law enforcement activities and criminal investigations, intelligence collection, and offensive cyber operations. The analysis this decision comprises is critical, as keeping secrecy over software vulnerabilities can enable its exploitation by malicious actors or surveillance abuses, jeopardizing the security of the broader digital ecosystem. The Special Rapporteur pointed out

that genuine oversight necessarily requires the participation of independent, expert representation in the public interest in VEPs, a role that the independent civilian authority would fulfill.

2.6. Additional Safeguards for Personal Data Processing

The Court held that **states should adopt policies to prohibit personal data[5] processing except when it is grounded in law or based on the free and informed consent of the person affected.** In any case, it must follow the terms of the American Convention, regarding legitimate aims and lawful means. Data processing operations include data collection, storage, analysis, and disclosure, among others.

States must also adopt positive measures to inform people about:

- their data-related rights *(see 2.7. Right to Informational Self-Determination)*;
- the legal conditions that allow for the processing of personal data;
- and when state agencies collected, stored, processed or disclosed their personal data *(see 2.4.(iii) Notification Systems)*.

Moreover, data protection guarantees demand from authorities that:

- They only collect information that is **truthful, relevant, and necessary** for strict compliance with their duties, based on the applicable legal framework.
- Authorities must exercise their power to process personal data in conformity with **the purposes that justified the collection**, and only for the **amount of time necessary** for fulfilling these purposes.
- The way state institutions manage personal information must ensure that they are **kept accurate, complete, up-to-date, and secure**.
- The latter requires that authorities employ the appropriate, reasonable mechanisms to **prevent unauthorized access, loss, destruction, damage, or disclosure**.

The Court indicates that free and informed consent requires that the data subject has sufficient information about the data to be collected, how the collection will be, for which purpose the state will use the data, and any potential disclosures—leaving

5 The concept of personal adopted by the Court is "information that identifies, or can be reasonably be used to identify, a natural person, whether directly or indirectly," which includes the different "factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity [...] expressed in a numerical, alphabetical, graphic, photographic, alpha-numerical, audio, electronic, visual or any other manner." Case of Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia, Preliminary Objections, Merits, Reparations and Costs, Judgment of October 18, 2023, para 572.

no doubt or ambiguity about the person's choice to consent:

> *The individual should have the ability to exercise a real choice and there should be no risk of deception, intimidation, coercion or significant negative consequences [...] from refusal to consent*.

Yet, state surveillance usually happens without the data subject's consent, given its nature and objectives. The same applies to intelligence activities in general.

Consequently, **the law governing state surveillance and intelligence activities**, approved by Congress and publicly accessible, must specifically stipulate powers to collect personal data and implement or keep related databases. According to the Court, this law should regulate, as specific as possible:

- the reasons for intelligence activities to create files with personal information, where such reasons should act as a constraint for the work of authorities;
- the kinds and types of personal data that authorities can hold in their files;
- the parameters for using, retaining, verifying, correcting, erasing, or disclosing personal data, in harmony with guarantees presented in previous sections.

State authorities cannot use their powers for discriminatory purposes, including in the context of digital surveillance and intelligence activities. As the Court emphasized, this means they are not empowered to compile information, preserve data, or develop records based exclusively on considerations of race, color, sex, language, religion, political or any other opinions, national or social origin, economic status, birth, or other social condition. The Court adds that if the protection of legitimate aims requires the **processing of sensitive data**, the law must set limits on the legitimate grounds allowed, the type of data authorities can collect, and the appropriate criteria for such processing, covering only information that is strictly and reasonably necessary for fulfilling agencies' legal mandate.

Security agencies must conduct regular assessments on whether they need to keep personal data in their files, and if so, check for accuracy. Through the **clearing of intelligence and security files:**

- authorities must delete personal data that is no longer relevant to their mandate;
- authorities can identify, classify, and take inventory of the various information, making it possible to verify whether their collection and retention are lawful;
- agencies keep data organized to facilitate that data subjects can exercise their data-related rights *(see 2.7. Right to Informational Self-Determination)*.

Importantly, the clearing of these files, that is, removing personal information that is no longer necessary, should not hamper the judicial or supervisory control of related data processing activities in the past or the ability for data subjects to confirm that such processing existed and obtain information about relevant related records.

In addition, **the Court highlighted the need for an independent institution to supervise the processing of personal data by intelligence agencies**. It must have access to intelligence files and have powers to destroy records or disclose the content to individuals concerned. Depending on the states' legal framework, this can be or not the same civilian oversight institution detailed in the previous section.

- Relatedly, the Office of the IACHR Special Rapporteur for Freedom of Expression recommended OAS Member States to ensure comprehensive data protection legal frameworks with independent oversight authorities, applicable also to law enforcement and intelligence agencies, with specific mandates to review surveillance databases and predictive analysis systems for compliance with human rights standards.

2.7. Right to Informational Self-Determination

The Court emphasized that it is imperative for people to have recognized their **right to access and control their personal information held in state files**. This right stems from the need to guarantee people's autonomy and self-determination, and encompasses the following dimensions:

- **the right to know** what data is stored in state records or databases, whether in hard copy or in magnetic, electronic, or digital format, the origin of the information, how it was obtained, the purposes of its use, retention period, whether the institution shares it with other entities or persons, and if so, what for, as well as the general conditions for the processing of their personal data;
- **the right to demand** the institution to **rectify, amend, or update** their personal information if it's inaccurate, incomplete, or out of date;
- **the right to demand the destruction, erasure or suppression**[6] of their data if

6 About the right to "erasure," the Court highlighted the Updated principles of the Inter-American Juridical Committee on privacy protection of personal data when they point out that: "The right is not absolute but rather contingent and contextual, and it requires a difficult and delicate balancing of interests and principles. Exercise of the right necessarily presents fundamental issues not just about privacy, honor and dignity, but also about the rights of access to truth, freedom of information and speech, and proportionality. [T]he national legislation of each State should establish, where applicable, the existence of the right to erasure, the requirements, deadlines, terms and conditions under which data subjects may exercise their rights to erasure, as well as the causes and reasons for which the exercise of such rights may be impeded." Case of Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia, Preliminary Objections, Merits, Reparations and Costs, Judgment of October 18, 2023, footnote 741

found that collection or retention was unlawful, or if there are no grounds to justify their permanence in government files or databases, so long as this does not impinge upon other rights as per a proportionate analysis and in accordance with applicable regulations;

- **the right to object to the processing of data** if it's harmful to the person, in view of their particular situation, or according to relevant regulations;
- **the right to receive data in a structured, commonly used, and machine-readable format and the right to request transmission** of those data without hindrance from the authority controlling the files, whenever possible and as per relevant legal provisions.

The Court found that the conjunction of these guarantees comprises an autonomous right—**the right to informational self-determination**—recognized in various legal systems in the Americas and protected by the American Convention. The Court highlighted in particular Articles 11 (the right to private life), Article 13 (the right of access to information, drawn from the content of Article 13(1)), and Article 25, as a dimension of judicial protection.

The right to informational self-determination serves to guarantee other rights, such as privacy, the protection of honor, safeguarding reputation, and in general, personal dignity. The Court underlined that this right covers any kind of personal data under the purview of any public institution and is equally applicable to records or databases held by private parties. Informational self-determination is not an absolute right and can be restricted or limited, provided restrictions follow the three-part test, as detailed below.

The Court emphasized that the effective exercise of the right to informational self-determination:

- Requires states to provide reasonable, swift, effective mechanisms or procedures, available free of charge, to process and resolve requests of data subjects to access and control their data.
- Through these procedures, controlling authorities, or supervisory and oversight entities, must respond to requests within a reasonable, predefined deadline, and under the responsibility of duly trained officers.
- Putting these mechanisms in place is a duty that derives from Article 2 of the American Convention. This provision requires Member States to enact regulations and adopt the procedures and practices conducive to give effect to conventional rights.

The Court has also recalled Article 25(1) of the Convention, regarding judicial protection, to **affirm states' obligation to provide for and implement a simple and rapid remedy able to offer effective protection to the right to informational self-determination whenever data-related requests by data subjects are totally or partially denied.**[7] Judicial authorities must be able to examine the information refused if they find this is necessary to deliver a decision. Additionally, the Court stressed the importance of an independent institution to supervise the processing of personal data by intelligence agencies with powers that include disclosing the content of personal data files to the individuals concerned *(see 2.6. Additional Safeguards for Personal Data Processing)*.

(i) Valid Restrictions of the Right to Informational Self-Determination within Surveillance and Intelligence Activities

According to the Court, valid restrictions to the right to informational self-determination under the American Convention must follow the criteria applied to the right of access to information. We outline below a summary of these requirements.

1st. Legality Principle

Any restriction to the right to informational self-determination, such as classifying a particular information held by intelligence authorities, **must be provided for by law** *(see 2.1. Clear and Precise Legal Framework)*:

- This law must be clear and specific, detailing as much as possible what type of information or documents are considered classified and the time limits that apply for their classification.
- The law must clearly determine that classification is exceptional, as it means blocking data subjects' right to access and control their personal data.

The **principle of maximum disclosure** remains valid in this context, deriving from the presumption that all information is accessible, subject to a limited system of exceptions. Consequently, the law must specifically set forth the permissible grounds for classifying any particular information, always based on its specific content. In this

7 In analyzing the concrete case in the ruling *CAJAR v. Colombia*, the Court stated: "This means that, if domestic judicial authorities should hear and adjudge motions for constitutional relief for informational self-determination regarding personal data contained in intelligence files, they must necessarily provide maximum protection of the right, and accordingly, must take into account the content of the American Convention, the interpretations of the Convention by the Inter-American Court in its full body of case law, and particularly, the standards set forth in this judgment." Case of Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia, Preliminary Objections, Merits, Reparations and Costs, Judgment of October 18, 2023, para 650.

sense, any restrictions must pursue a legitimate aim in a democratic society, as per Article 13(2) of the American Convention.[8]

Based on the above, **the legal framework must provide mechanisms for clearing and declassifying intelligence and security files,** allowing public access to documents and data for which classification is not justified, and identifying fixed time limits for automatic declassification.

These mechanisms must safeguard the confidentiality of sensitive data or information that, according to applicable law and regulations, cannot be disclosed without the data subject's consent. In any case, this protection should not block the data subjects' right to access and control their personal data when there's no other legitimate ground justifying the restriction.

2nd. Legitimate Aim in a Democratic Society

The Court underscored that a state cannot block access to any information simply because it generally relates to the protection of national security.

> *"[I]nstead, a law must be on the books to define the specific, narrow categories that need to be withheld to protect security objectives."*

As a consequence, a decision to classify a document merely because it is held by or is under the purview of intelligence or security authorities, regardless of its content, is **incompatible with inter-American standards**.

The Court identified some concrete conditions that could legitimize legal restrictions to accessing information for purposes of protecting national security in the context of intelligence activities. These include, among others, information about current defense plans, specific measures to counter specific threats so long as keeping the information secret is a condition for the measure to be effective, and information about national security matters provided by a foreign state or inter-governmental body with an express indication of confidentiality.

See more in ***2.2. Legitimate Aims*** above.

8 About applicable parameters, see Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression. The Inter-American Legal Framework Regarding the Right to Access to Information, 2012. Available at https://www.oas.org/en/iachr/expression/docs/publications/2012%2009%2027%20access%20to%20information%202012%20edits.pdf . See also Id. Derecho a la información y seguridad nacional, 2020. Available at https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf .

3rd. Proportionality Test (adequacy, necessity, and proportionality stricto sensu)

The decision to classify information in intelligence or security databases must fulfill the proportionality test. Here are the important parameters laid out by the Court:

- classification (i.e. the denial of information) must be the best or most appropriate means to achieve the legitimate goal;
- classification must be necessary and absolutely essential to achieve that legitimate goal, meaning that no other measure would be equally useful for meeting the goal and less injurious to the right of access to information and informational self-determination;
- classification must be strictly proportional, so that restricting these rights is not excessive compared to the benefits of keeping the information confidential to fulfill a legitimate aim.

The adequate application of the proportionality test **may often allow at least partial access** to certain files, documents, or data.

See more in ***2.3. Adequate, Necessary, and Proportionate*** above.

4th. Substantiated Decision

Competent authorities must deliver a well-founded decision consistent with due process guarantees when denying requests of access and control of personal information. This means they must provide a clear and complete justification of the grounds for the denial.

5th. Additional Requirements

- Authorities **cannot use classification or information under their control as a means to protect a concealed interest** in favoring or harming a particular activity or political ideology, or in any other way acting in a discriminatory manner ***(see 2.6. Additional Safeguards for Personal Data Processing)***.
- In any case, **authorities have the obligation to manage and process the information correctly and securely, preventing any unauthorized access, sharing, transmission, modification, or loss**. Authorities must make sure that personal data will not be disclosed or made available illegally to third parties.
- Authorities must also **conduct regular reviews to ensure that the justification for retaining personal data in their files persists, removing information that is no longer necessary**. Yet, the track record of logs and data processing operations relating to any personal information should remain available to judicial,

supervisory, and oversight authorities even after that information is removed. Data subjects may also obtain information pertaining to the track record of their personal data processing even after the processing is over and the related personal information is no longer available in the intelligence or security files.

- In cases of **human rights violations**, the classification of information under reasons of public interest or national security cannot be used to justify authorities' denial to provide information requested by judicial or administrative entities conducting investigations or within judicial proceedings.
- If the investigation of a punishable offense is underway, the decision to classify the information and, thus, deny disclosure **can never depend exclusively on a government body whose members are under suspicion of having committed the offense.**
- The classification of any particular information **must never be a measure of indefinite duration**. Classification and the denial of access may remain in effect so long as strictly necessary to meet the intended legitimate purpose, and this requires regular review of the continuing need.

3. Transparency and Participation

Security-related activities, including surveillance measures and operations, are not an exception zone for transparency standards and guarantees. On the contrary, their compliance with fundamental rights requires accountability, public oversight, and civic participation in defining related policies and applicable limits. As such, principles of maximum disclosure, good faith, and the three-part test to limiting rights apply to security entities just as they bound other public bodies, even when national security purposes are involved.

The Inter-American Human Rights System has devised critical guidance on transparency and participation in the context of security activities. Here we some important highlights.

The Office of the IACHR Special Rapporteur for Freedom of Expression underlined that **certain categories of information hold particular public significance**, given their importance to democratic scrutiny and the rule of law.

These refer to information about: violations of human rights and international humanitarian law, state surveillance, and acts of corruption and/or related to the management of public resources.

First, classifying information about serious **human rights violations** is incompatible with the American Convention. Rather, the state has proactive obligations in disclosing related information, conducting investigations, and providing redress to victims.

As for **state surveillance,** the Special Rapporteur stressed that it's essential for government institutions to ensure that individuals are duly informed about, at a minimum:

- the legal framework governing all forms of surveillance, both covert and overt, including indirect surveillance such as profiling and data-mining;
- the legitimate aims for surveillance;
- the procedures that authorities must follow to authorize and review the use of surveillance measures, including the selection of targets, data processing procedures and the threshold of suspicion required to initiate or continue surveillance measures;
- the type of personal data that authorities may process for security (including national security) purposes, and the criteria they apply for data use, retention, deletion, and transmission;
- the protocols for exchanging, storing, and destroying intercepted material;
- the entities in charge of conducting and supervising surveillance;
- statistics about state surveillance actions and the use of digital tools.[9]

In this sense, the Special Rapporteur directly recommended OAS Member States to require transparency in surveillance procurement and deployment. In addition to the previous points, public reporting on state digital surveillance should include:

- the disclosure of government contracts and the use of public funds for surveillance-related equipment and services;
- registries of surveillance vendors and disclosures regarding the contractor pool;
- disclosure of the tools the state purchased and their specifications.

Finally, national security cannot be invoked as a legitimate ground to directly, or as an indirect effect, **shield or conceal alleged irregularities or violations of the law,**

9 Principle 9 of the Necessary and Proportionate Principles on the application of human rights to communications surveillance details a minimum set of aggregate information that states should disclose. It also emphasizes that states should not interfere with service providers in their efforts to publish records of state authorities' data requests and the procedures they follow when responding to such requests. See at https://necessaryandproportionate.org/principles/ .

as well as the malfunctioning of public institutions, including on matters related to budget expenditure. In fact, the state must proactively disclose information that allows the public to know in a clear, complete, and timely manner how security institutions manage their finances and the applicable rules.

Partial Disclosure

The Special Rapporteur underscored that when a record contains both information that falls and does not fall under classification exemptions to the principle of maximum disclosure, the restriction of access applies only to the specific information protected, and not to the entire document.

Practical Accountability Measures in Security-Related Activities

The Inter-American Commission highlighted that state authorities have the duty to be transparent and consistent when **reporting the criteria used to earmark resources to public institutions involved with citizen security. They must also disclose performance indicators**, allowing the public to assess whether public spending in citizen security is achieving legitimate aims and pre-determined objectives. Moreover, the public should know about the systems and procedures in place to review security policies when indicators reveal issues and failures.

This relates to **states' duty to produce, organize, and disseminate information about security policies**, which is a positive obligation within a democratic model of citizen security. Among other relevant measures, the Commission recommended states to foster **observatories** at national and regional levels to produce, analyze, and publicize qualified information about citizen security.

The Commission also urged states to take effective measures to prevent institutional violence and excessive use of force based on ethnic or racial origin and racial profiling patterns. Relatedly, it emphasized the importance of having **public security policy indicators that can help to identify patterns of institutional and structural discrimination**.[10]

More broadly, the Commission recommended states to operationalize procedures to make effective the accountability of all authorities responsible for public security, through **internal and external control mechanisms**. It has also underlined that

10 "The information that the public authorities produce and circulate should highlight the plight of those sectors of the population that are most likely to have their human rights violated with implementation of policies on citizen security, especially when it comes to preventing interpersonal and/or social violence. This information should devote as a priority attention to the situation of women, Afro-descendents, the indigenous population, migrants, children and adolescents." [free translation] IACHR. Informe sobre Seguridad Ciudadana y Derechos Humanos, 2009, para 186. See also B. Recomendaciones específicas, item 18. Available at https://hchr.org.mx/publicaciones/nforme-sobre-seguridad-ciudadana-y-derechos-humanos-2009/

states should create the conditions for **meaningful social participation** in citizen security issues.

Additional Measures for Countering Digital Surveillance Abuses

In turn, the Office of the Special Rapporteur for Freedom of Expression recommended companies to establish **independent technical auditing processes** that allow qualified civil society organizations and human rights experts to examine surveillance technology capabilities and deployment protocols to verify compliance with human rights safeguards and contractual limitations on use. In the same vein, the Special Rapporteur stressed that detection of digital surveillance abuses requires, among others, **technical assistance for civil society organizations** to identify and document abuses.

4. Remedy and Reparation of Surveillance Abuses

While state digital surveillance in the Americas is fraught with challenges and shortcomings in safeguarding rights, hurdles to effective remedy and reparation of surveillance abuses stand out as the culmination of many entangled problems.

The lack of clear, complete, necessary and proportionate legal frameworks, insufficient legal safeguards, weak institutional control mechanisms, poor transparency, and little to no accountability combine in posing crucial barriers for people affected to seek and obtain redress. Even if challenges are more pronounced for certain surveillance practices, like those in the context of intelligence operations, security-related activities in general require heightened efforts to shed light on, investigate, punish, repair, and take measures to prevent repetition of state arbitrary surveillance.

In a recent report, the IACHR Special Rapporteur for Freedom of Expression stressed:

> *"Perhaps the most alarming finding of this report is the impunity that characterizes surveillance abuses across the region. Despite extensive documentation of illegal surveillance operations, no state in the Americas has successfully prosecuted those responsible for surveillance abuses or provided meaningful remedy to victims. This systematic failure of accountability mechanisms has created a permissive environment that encourages continued violations and demonstrates to both state and private sector actors that surveillance abuses will face no consequences."*

The Inter-American Court similarly highlighted in *CAJAR v. Colombia* that **Article 25 of the American Convention protects people affected by arbitrary intelligence activities in seeking effective redress, including compensation for damage**. This protection also applies to state surveillance abuses and disproportionate limitations to the right to informational self-determination. Such protection requires states to provide an appealable, simple, fast effective remedy from courts, whose decision must fully comply with the guarantees of Article 25.

According to the Special Rapporteur, the current state of impunity of surveillance abuses in the region could constitute a violation of the right to effective remedy undergirded by the American Convention.

The Office of the Special Rapporteur emphasized that addressing such impunity demands:

- the prosecution of perpetrators along with the recognition of specific harm caused to individuals;
- the provision of complete information about the scope and duration of surveillance to victims;
- the destruction of illegally obtained data, and
- guarantees that state authorities will not repeat these violations.

In this sense, the Special Rapporteur recommended OAS Member States to **establish legal mechanisms to ensure effective remedies** for victims of surveillance abuses, including provisions to address evidentiary challenges and jurisdictional gaps in digital surveillance cases.

In addition, the Inter-American Commission recommended that states **improve selection and training processes of state agents** involved with security activities (including police forces, the judicial power, and public prosecutors).

Finally, it is essential that states **assign adequate material resources to ensure** meaningful control mechanisms, robust independent oversight, rigorous judicial supervision, and institutional structures and procedures capable of fulfilling transparency and informational self-determination requirements. Together, these elements lay indispensable conditions to make effective remedy and reparation of surveillance abuses a lived reality rather than theoretical commitments on paper.

Conclusion

This guide aims to provide clear and actionable guidance for addressing a longstanding issue in the Americas: state arbitrary surveillance, now increasingly powered by digital technologies.

The current state of weak controls that prioritize overbroad claims of threats to national security and public order over the accountability of police and intelligence forces must not be normalized. Because of the persistent culture of secrecy and systemic hurdles for ensuring effective remedies to surveillance abuses, we can expect resistance from states in the region to this guide's safeguards. Yet, overcoming these obstacles is precisely what's needed to protect rights.

The Inter-American Human Rights System provides states with a robust foundation for tackling these challenges. From the American Convention on Human Rights to landmark rulings like *CAJAR v. Colombia*, the legal parameters are well-established.

States must implement clear and precise legal frameworks that:

- define surveillance powers and limitations;
- ensure all surveillance measures pursue legitimate aims without discriminatory ends;
- subject interference with privacy to rigorous necessity and proportionality analysis;
- require prior judicial authorization for digital surveillance measures;
- maintain detailed records of surveillance operations;
- establish independent civilian oversight institutions with technical expertise and enforcement powers;
- guarantee individuals' right to informational self-determination and proper notification;
- and provide effective remedies and reparation for victims of surveillance abuses.

These are not optional best practices but relevant obligations under international human rights law. The American Convention, interpreted by the Inter-American Court, establishes that states cannot invoke national security as a blanket justification for evading transparency, accountability, or respect for fundamental rights. When security forces stray from their ultimate purpose of protecting people and their freedoms, they become the very threat they were meant to counter.

The cost of inaction is measured in eroded democracy, chilled expression, and diminished trust between states and their citizens. Conversely, implementing these safeguards strengthens the rule of law, reinforces democratic institutions, and ensures that security activities genuinely serve the public interest. States that embrace these recommendations will not only comply with their international obligations but will also build more resilient, rights-respecting security architectures capable of addressing genuine threats without sacrificing the freedoms they exist to protect.

As the Office of the Special Rapporteur for Freedom of Expression has warned, the systematic impunity surrounding surveillance abuses across the region could constitute its own violation of the right to effective remedy. States must act decisively to close legal gaps, empower oversight bodies, ensure judicial independence, and establish meaningful accountability mechanisms. The guidance outlined in this brief offers a critical roadmap for doing so.

States that follow this guidance will affirm their commitment to a vision of security that protects both people and their rights—recognizing that these goals are not in tension, but fundamentally inseparable.