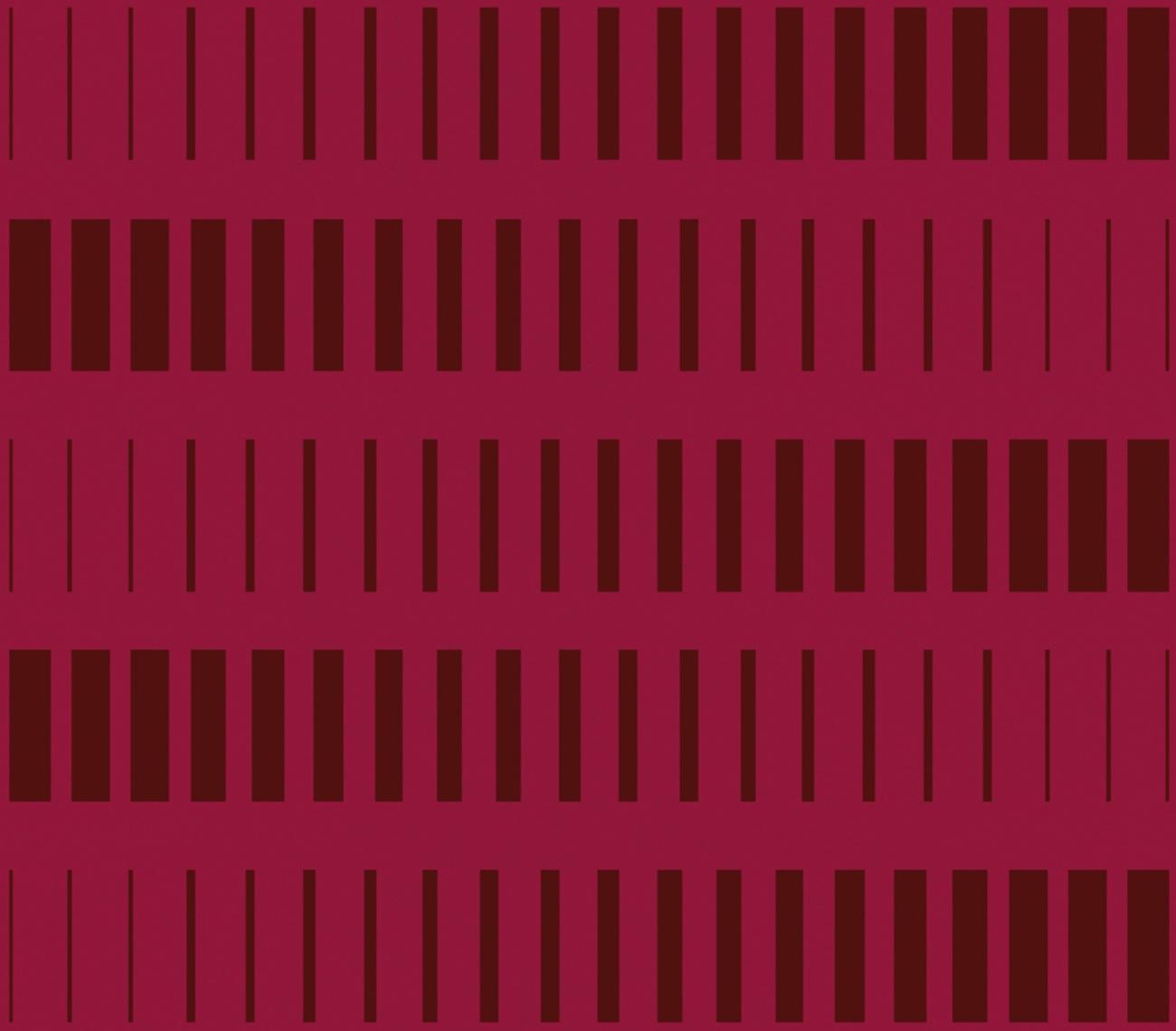

Intrusive Intelligence

Interception and Monitoring Technologies in Argentina, Chile and Uruguay

TECHNICAL AND COMMERCIAL MAPPING

Lucas Domínguez Rubio

Intrusive Intelligence

Interception and Monitoring Technologies in Argentina, Chile and Uruguay

Technical and Commercial Mapping

Lucas Domínguez Rubio

December 2025

SOCIALTIC

OPEN TECHNOLOGY FUND

DOI + ISBN pending

English-language manuscript completed on 1 December 2025.

Spanish version completed in December 2025.

ISBN XXX-X-XXXXX-XXX-X

DOI: https://doi.org/XX.XXXXX/XXXX

PROOFREADING BY HERNÁN VILLASENÍN

DESIGN AND LAYOUT BY BRENDA MUÑOZ ROSAS

Summary

The market for surveillance technologies used by law enforcement and security agencies in the Southern Cone remains poorly documented, fast-evolving and opaque. Actual interception and analysis capabilities are seldom made public, and procurement processes are only partially visible through public records.

To address this gap, this report proposes a technical classification of interception and monitoring technologies available to security agencies and maps documented procurement patterns across Argentina, Chile, and Uruguay. Drawing on technical documentation, corporate brochures, procurement records, and commercial databases, the study identifies surveillance tools according to their operational capabilities and traces the main vendors and regional intermediaries involved in their distribution.

The classification organizes surveillance technologies into five categories: (i) intrusion software or spyware, (ii) signals interception technologies, (iii) network interception and intelligence platforms, (iv) network monitoring and traffic management systems, and (v) open-source intelligence (OSINT) tools. Using this classification as an analytical baseline, the report examines evidence of procurement by security agencies in the three countries and distinguishes between confirmed acquisitions, probable purchases, and documented negotiations based on the strength of available evidence.

The analysis reveals a regional trend toward integrated surveillance architectures: all three countries have incorporated, with varying degrees of intensity, nearly the full spectrum of available technologies. National profiles, however, differ significantly. Chile shows the broadest adoption, with confirmed acquisitions of highly intrusive tools, including commercial spyware. Argentina presents a more fragmented ecosystem, with multiple local intermediaries and a gradual accumulation of capabilities across agencies and levels of government. Uruguay stands apart: low probability of commercial spyware adoption, but sustained development of infrastructure-embedded capabilities — lawful interception and network monitoring — following a more institutionalized model oriented toward the network level rather than individual device infiltration. Cutting across all three cases is a structural dependence on a small number of foreign vendor countries, where local actors operate almost exclusively as distributors, limiting transparency and meaningful democratic oversight of high-impact surveillance tools.

The study combines a supply-side mapping of surveillance technologies with a demand-side reconstruction of procurement dynamics to identify regional patterns of technological adoption. Its findings show that these capabilities expand regardless of the political orientation of governments, within markets designed to leave little trace and against a regulatory backdrop that none of the three countries has adequately addressed.

Contents

1. Introduction

1.1. International context: from PRISM to Pegasus

The problem is well known. Numerous companies offer solutions to law enforcement and security agencies in opaque ways. Despite their significant political and social implications, these technologies are rarely adequately regulated. Although many types of abuse have been extensively documented throughout the region, their wider ramifications remain largely absent from public debate.

The term "cybersecurity tools"—whose conceptual bias is discussed later— usually refers to a variety of hardware and software deployed by security forces and intelligence organizations to monitor, extract, gather, or analyze communications data. This market has grown to extraordinary proportions in the last few decades.

Thirty years have gone by since Privacy International published the first report in 1995 on the international trade in surveillance technology[1]. By the time of that first report, central governments were already building telecommunications networks to be interceptable by design. The Communications Assistance for Law Enforcement Act (CALEA), passed by the United States in 1994, mandated that manufacturers and operators add lawful interception capabilities to their infrastructure. During that time, the European Telecommunications Standards Institute (ETSI) started releasing technical guidelines to specify how intercepted traffic should be handed over to law enforcement and security agencies. This was also the era of the so-called "crypto wars", a term coined after attempts by the United States and its allies to limit public access to strong encryption tools, either through export controls on cryptography technologies, or through the design of systems with built-in security flaws, called backdoors.

During the period when the above regulatory and technical framework was stabilizing, the internet was developing into a mass infrastructure. Between 1997 and 2001, the number of users went from 117 million to 489 million. According to estimates from the International Telecommunication Union, that meant an increase of around 318% in just four years. New layers of control over this now massive infrastructure were deployed in response to the terrorist attacks of September 11, 2001. In the United States, the US PATRIOT Act, which was passed within weeks, reshaped much of the surveillance legal framework and gave the government access to communications records and metadata (through secret orders, roving wiretaps and administrative requests marked as confidential). Meanwhile, new policies requiring the retention of traffic data were being established in Europe in the name of combating terrorism.

By the end of that same decade, another milestone fundamentally reshaped the communications landscape: smartphones gradually became the primary interface for everyday internet access. Their integration into everyday life brought together communication functions and mobile applications that extended into virtually every sphere of human activity.

The global conversation on security, privacy and technology first reached a turning point in 2013 when Edward Snowden leaked thousands of classified documents from the US National Security Agency (NSA) and disclosed the existence

---

1 Privacy International. *Big Brother Incorporated*. London, 1995. URL

of PRISM and other mass surveillance programs, such as XKEYSCORE, Boundless Informant and the so-called "upstream" interception systems[2]. PRISM was a codename for a program set up by the NSA in 2007 with the capacity to gather information from major U.S. technology companies , including Microsoft, Yahoo!, Google, Facebook (now Meta) and Apple. The leaks showed that user data from major platforms was being systematically intercepted, and that heads of state and leaders from other countries were being spied on, including German Chancellor Angela Merkel and some Latin American heads of state. Global diplomatic scandal ensued.

This was made possible, in part, by the Foreign Intelligence Surveillance Act (FISA). This act set out the procedures under which U.S. intelligence agencies could obtain information related to foreign threats in the name of national security—rather than as part of an ordinary criminal investigation. That framework served as the legal foundation for programs like PRISM, which required major technology companies to cooperate with the NSA by turning over user data. But the leaks showed that the scope of data gathering was far broader than officials had acknowledged, and there were domestic repercussions: it was no longer clear how strong the safeguards really were to prevent the collection of data on U.S. citizens.

While web traffic encryption was already increasing and was driven by various commercial needs, the technical reaction to the above disclosures was a coordinated shift towards encryption by default. Within a few years, the use of protocols that encrypt communication between browsers and servers—SSL/TLS (and later HTTPS)—went from being a costly exception to becoming a basic requirement.

As internet traffic became encrypted, the weakest link shifted to the endpoints: people's computers and phones. That reconfiguration displaced the focus toward the devices themselves. Beginning in 2012, smartphone-targeted spyware started to rise steadily. These tools were capable of infecting iOS and Android devices and capturing communications directly from the device.

It was in that context that, over time, Privacy International developed a database that grew to include 528 companies selling equipment for communications interception, video-surveillance, biometrics, geolocation, internet monitoring, packet inspection, forensic extraction, and intrusion software. Unfortunately, the Surveillance Industry Index (SII) was discontinued in 2016[3].

A second turning point in the conversation occurred between 2015 and 2017 with reports exposing the existence of commercial spyware developed by companies such as FinFisher, Hacking Team, and NSO Group. In this case, the scandal was not related to a single, government-run, mass surveillance program involving major global technology companies. Instead, this new phase was best represented by commercial spyware vendors like NSO Group. Leaks of internal documents and technical analyses revealed how these companies were selling highly intrusive tools—capable of taking control of computers and phones—to

---

2 See: Lyon, David. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1, no. 2 (2014). DOI. // Verble, Joseph. "The NSA and Edward Snowden: Surveillance in the 21st Century." *SIGCAS Comput. Soc.* 44, no. 3 (2014): 14–20. DOI. // Bigo, Didier, Gertjan Boulet, Caspar Bowden, et al. "Open Season for Data Fishing on the Web: The Challenges of the US PRISM Programme for the EU." *CEPS Policy Brief* 293 (2014). URL

3 Privacy International. *The Global Surveillance Industry*. London, 2016. URL

governments around the world, including authoritarian regimes, and how such tools were being deployed against journalists, activists, and political opponents[4].

The narrative changed. Large companies such as Facebook/Meta, Google and Apple publicly repositioned themselves around the language of privacy—what has been called "privacy washing"—through policy changes, marketing campaigns, and strategic lawsuits. In fact, Meta, one of the key companies identified as part of the PRISM program, sued NSO Group over the use of Pegasus against more than 1,400 users of its messaging platform, underscoring a shift in the attribution of responsibility. The focus shifted from governments and large digital platforms towards specific firms in the business of developing and marketing surveillance technologies[5].

Those two major turning points in the public conversation reveal only a small portion of a far more intricate landscape shaped by many different actors. It was private producers of surveillance tools, however, who started to draw attention.

In 2015, more than one million internal e-mails from Italian spyware producer Hacking Team were leaked[6]. Numerous investigative reports followed. Commercial spyware became a central focus of public debate. Researchers, activists, and journalists made painstaking efforts to identify companies and technologies in that ecosystem, but often without conclusive results; each investigation tends to uncover new connections among investment groups, resellers, security agencies, and multiple whistleblowing disclosures.

The difficulty lies in the fact that these companies and tools are constantly evolving. They change their names and locations as legislation advances in the different countries. Name changes, as well as intricate and opaque corporate structures, help them evade national and transnational regulations. They can associate either with large holdings or with regional resellers. In many cases, European company executives have relocated their operations to jurisdictions with weaker regulatory frameworks or use intermediaries for illegal operations in their own countries[7].

---

4 Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. Citizen Lab Research Report No. 113. University of Toronto, 2018. URL // Amnesty Tech. *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector.* Amnesty International, 2021. URL // Kaster, Sean D., and Prescott C. Ensign. "Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware." *Thunderbird International Business Review* 65, no. 3 (2023): 355-64. DOI

5 In light of the fact that Meta had first-hand knowledge of the attacks carried out via Whatsapp, their own diagnosis acquires a more troubling significance: "While these 'cyber mercenaries' often claim that their services only target criminals and terrorists, our months-long investigation concluded that targeting is in fact indiscriminate and includes journalists, dissidents, critics of authoritarian regimes, families of opposition members and human rights activists." Dvilyanski, Mike, David Agranovich, and Nathaniel Gleicher. *Threat Report on the Surveillance-for-Hire Industry.* Meta, 2021, p. 2. URL

6 "WikiLeaks - The Hackingteam Archives." 2015. URL

7 Lighthouse Reports. *Surveillance Secrets: How First Wap Tracks Phones Around the World.* Lighthouse, 2025. URL

The picture becomes even more obscure when it comes to identifying actual purchases in countries with legislation that allows governments to evade accountability in the acquisition of intelligence tools[8].

Following Privacy International's groundbreaking reports, a thorough investigation set out to identify the companies offering interception and intrusion technologies at the global technology trade fair for law enforcement and security agencies[9]. The picture revealed a tangle of names, connections and overlapping interests. It is no coincidence then that the most recent long-term investigation attempting to map this complex network invokes the image of a mythical beast, one that must be traced through a dense and intricate web of business relationships. The investigation's database is visualized as a constantly shifting map of hubs, which includes "forty-nine vendors along with thirty-six subsidiaries, twenty-four partner firms, twenty suppliers, and a mix of thirty-two holding companies, ninety-five investors, and one hundred and seventy-nine individuals, including many publicly identified investors"[10].

Without offering a consolidated global count, Privacy International's first report in 1995 identified over eighty British companies, and dozens more in other countries, working in the field of digital security in the broad sense: physical counterintelligence equipment, signal jammers, CCTV, and other tools. In 2016, the same organization was working with a database of 528 surveillance companies listed in the Surveillance Industry Index. Narrowing down to more offensive tools, a 2021 report by the Atlantic Council documented 224 companies selling intrusion and interception capabilities at the world's leading surveillance technology trade fairs. Meanwhile, the Mythical Beasts project (2024) mapped 435 entities—including vendors, investment holding companies, and resellers—involved in the global spyware market across 42 countries.

---

8 Gjesvik, Lars, and Johann Ole Willers. "Beyond Control? The Political Economy of Private Interception, Intrusion, and Surveillance Markets." *Review of International Political Economy* 31, no. 6 (2024): 1840–64. DOI

9 DeSombre, Winnona, Lars Gjesvik, and Johann Ole Willers. "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets." *Atlantic Council*, November 8, 2021. URL

10 We recommend following the link to the dashboard to see the shapes this beast can adopt: Roberts, Jen, Trey Herr, Nitansha Bansal, and Nancy Messieh. *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights.* With Emma Taylor, Jean Le Roux, and Sopo Gelava. 2024. URL

Against this backdrop, a number of international initiatives have been trying to impose controls on the trade in these "cybersurveillance tools," where the concept of dual-use technologies takes on a specific legal and technical meaning. The term "Dual-use technologies" refers to technologies with civilian applications—such as communications or data processing—that can also be used for military, security, or intelligence purposes. Network traffic management technologies, for example, can also be repurposed to block content or intercept communications. The significance of dual-use technologies is closely tied to the increasingly central role private companies play in supplying governments with surveillance capabilities.

A key international mechanism for addressing this issue has been the Wassenaar Arrangement, a multilateral export control agreement established in 1996 to promote transparency and accountability in the transfer of weaponry and other dual-use products. Since 2012, this Arrangement has added the category of "intrusion software" and other cybersurveillance tools to the lists of regulated technologies[11]. It is worth mentioning that the Arrangement has been the subject of varied criticism. On the one hand, many reports have emphasized that its wording is suspiciously ambiguous, leaving room for doubts about its actual scope, and benefiting the proliferation of certain companies and technologies. On the other hand, relevant countries such as Israel, China and Russia have failed to sign the Arrangement while others, such as Italy, implement their own internal controls subject to geopolitical decisions of their governments. While the Arrangement has been criticized from the very outset for having failed to include certain technologies related to lawful interception or mobile signal exploitation, the Arrangement importantly incorporates mechanisms to require member states to monitor exports of such technologies, particularly when they pose a risk of repression or violation of human rights[12].

As a result of this agreement, in 2021, the European Union adopted Regulation (EU) 2021/821, which caused a decrease in the number of licenses granted for "cybersurveillance technologies", including interception of mobile communications, network surveillance systems, and tools for the generation or management of intrusion programs. Given the above discussion, however, it remains to be seen whether the companies interested in developing these types of technologies are rather choosing (or have already chosen) methods to circumvent those regulations.

---

11 Coalition Against Unlawful Surveillance Exports (CAUSE). *A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation*. Coalition Against Unlawful Surveillance Exports (CAUSE), 2014.

12 Bromley, Mark. "The EU Dual-Use Regulation, Cyber-Surveillance and Human Rights: The Competing Norms and Organised Hypocrisy of EU Export Controls." *Defence Studies* 23, no. 4 (2023): 644–64. DOI

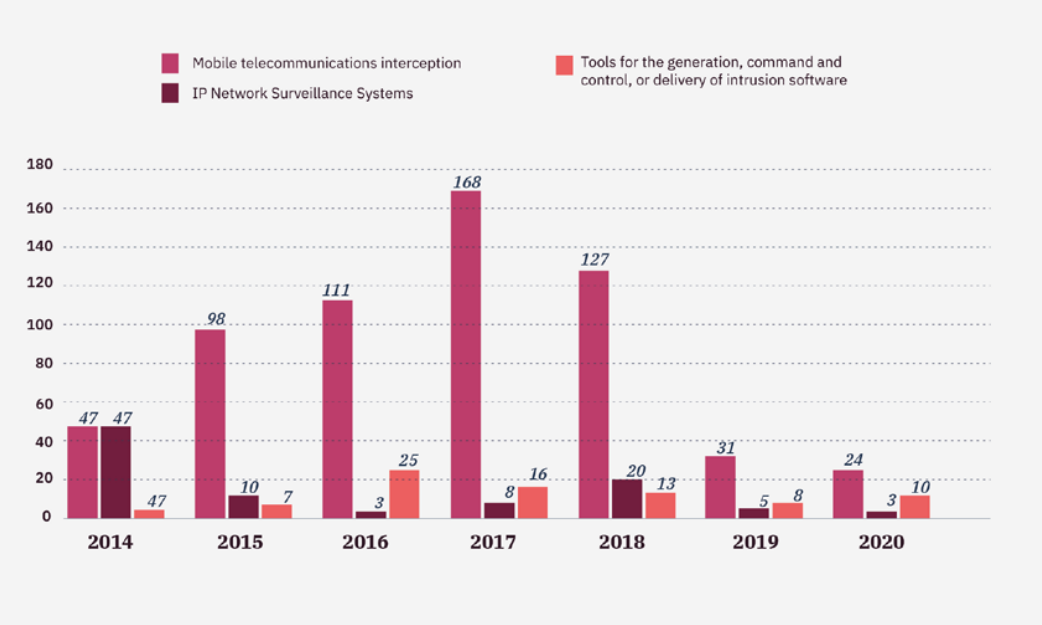

Chart published in: European Commission. Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. European Union, 2022. *URL*

Only two Latin American countries, namely Argentina and Mexico, have so far joined the Wassenaar Arrangement. By joining the Arrangement, those two countries agree to maintain national controls over the export of conventional weapons and dual-use technologies, and to cooperate on transparency and the open exchange of information regarding such exports in accordance with international security standards.

Another international initiative emerged after an executive order issued by the White House in 2023 restricted the use of commercial spyware by the United States federal government. Shortly afterwards, sixteen other countries joined a collective declaration recognizing this type of software as a threat to both national security and human rights. It emphasized that spyware is routinely misused, not only in authoritarian regimes, but also in democratic contexts. The United States' proposal went even one step further. It adopted a comprehensive approach that included export controls and sanctions against individuals involved in spyware operations[13].

However, this is no longer the current situation. While U.S. federal agencies are technically forbidden from using spyware, in October 2025, the current administration of President Donald Trump reinstated a contract with Paragon Solutions, despite reports showing that the company's spyware —Graphite— had been used against journalists, activists, and human rights defenders around the world. The United States Immigration and Customs Enforcement (ICE) is suspected to be using Graphite for its mass deportation operations[14].

---

13 The White House. "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security." *The White House*, March 27, 2023. URL

14 Panagiotopoulos, Vas. "ICE Signs $2 Million Contract With Spyware Maker Paragon Solutions." *Wired*, 2025. URL

The United Nations has taken varying positions on the issue. A UN proposal for its convention on cybercrime, submitted in September 2024, has given rise to serious concerns regarding the legitimacy of surveillance practices. In its draft, the treaty forces states to set up capabilities to access electronic data and to intercept real-time communications. The wording, however, does not expressly prevent states from outsourcing those capabilities to private spyware vendors and fails to sufficiently define the applicable safeguards. This could enable some states to invoke the convention in justifying the use of highly intrusive surveillance tools, which could in turn provide legal grounds for practices that would be otherwise deemed abusive or illegal[15].

To sum up, the Wassenaar Arrangement is merely one of several attempts at joint regulation, such as the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, launched by the United States in 2023, and the ongoing Pall Mall Process project, promoted mostly by France and the United Kingdom[16]. While long-term success of those initiatives remains uncertain, it is clear that the surveillance market is expanding and that those tools are geopolitically significant. Not only are governments around the world seeking to acquire these capabilities, but they are also seeking to regulate them in ways that serve their own interests, reducing human rights concerns to an "ethical" bargaining issue within policy debates. Leaked documents, journalistic investigations, technical reports, and freedom of information requests consistently confirm the expansion of those technologies.

Considering the above, this report seeks to map the surveillance technology trade for state use in Latin America and particularly in the Southern Cone, identifying the tools and companies involved in order to document currently observable capabilities. The purpose of this report is to help understand some of the tools currently in use while encouraging accountability from an industry operating behind a veil of secrecy.

---

15 Robertson, Kate. "A Global Treaty to Fight Cybercrime—Without Combating Mercenary Spyware." *Lawfare*, Lawfare, August 22, 2024. URL

16 Bromley, Mark, and Giovanna Maletta. Export *Controls and Spyware: Enhancing Oversight, Transparency and Restraint*. SIPRI, 2025. DOI

1.2. Supply of solutions: technical classification

Understanding the technical classification of the tools being marketed is essential to assessing the scope and risks of their deployment.

The range of solutions is broad and is largely the same for governments worldwide. In fact, there is a major international trade fair—ISSWorld—in which almost all vendors participate and which is attended by senior security officials from various countries. Given the variety of products and capabilities, the range of available solutions is extensive and attractive to security agencies[17].

As noted, the names of vendors, subsidiaries, parent companies, commercial partners, resellers and investors, form an intricate web partly designed to obscure connections, avoid regulatory pressure, and operate within legal grey areas[18]. When it comes to observing purchases, other problems emerge. On numerous occasions, procurement records (if any) reveal nothing. It must be considered that security agreements between countries sometimes enable agencies to share tools, allowing technologies to be deployed without the need for direct procurement.

Compounding this problem, manufacturers provide only very general descriptions of the products sold. And even when there is access to specific brochures, these typically provide limited technical detail.

In fact, there is constant, deliberate ambiguity around the terminology used to describe the functioning and capabilities of those tools. Ambiguity and euphemisms are key resources in a rhetorical strategy, which is often difficult to clarify without direct engagement between vendors and security agencies.

Illustrating this deliberate ambiguity, the term "digital forensics" can be used either to refer, expectedly, to physical data extraction devices, or as a euphemism for spyware and remote search and extraction capabilities. Similarly, the term "tactical interception" seems to refer to proximity interception hardware, although it is one of the many names used by companies to refer to lawful interception systems and may include spyware or other vaguely defined capabilities expanding the definition of lawful interception without the involvement of a service provider acting as an intermediary.

"Lawful interception" typically refers to a process with legal grounds whereby any communications network operator, or service provider, enables authorized officers to access the communications of individuals or organizations[19]. Under that umbrella term, however, network traffic intelligence modules and systems designed to target telecommunications signaling infrastructure are often included.

---

17 The Intelligence Support Systems World (ISSWorld) exhibit consists of a series of conferences and training sessions on lawful interception, electronic surveillance and digital investigation oriented to law enforcement, intelligence and defense agencies. DeSombre, Winnona, Lars Gjesvik, and Johann Ole Willers. "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets." *Atlantic Council*, November 8, 2021. URL

18 Roberts, Jen, Trey Herr, Nitansha Bansal, and Nancy Messieh. *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*. With Emma Taylor, Jean Le Roux, and Sopo Gelava. 2024. URL

19 Frost & Sullivan. *Lawful Interception: A Mounting Challenge for Service Providers and Governments.* London, 2011. URL

As a result, companies' web catalogues typically offer seemingly non-conflicting solutions, such as those related to open-source data mining or lawful interception, but they do so under broad and vague categories, when in fact they are marketing something else.

The same thing happens in public procurement processes and official gazettes. Public tenders use carefully selected language carefully selected to describe advanced surveillance technologies and cybersecurity while avoiding explicit terms which may give rise to controversy. Thus, what is known in technical circles as "spyware" or "intrusion software" can be toned down with language such as "forensic extraction modules" or "data exfiltration technology". Similarly, active intrusion tools, such as zero-click exploits, are presented as "vectors without user interaction", and mobile signal interception systems, known as IMSI catchers, are described as "cellular monitoring units". The use of those terms allows procurement documents to describe advanced technical capabilities, such as communication interception, or remote access, without making direct reference to intrusive surveillance practices.

That is why examining the technical functioning allows for the analysis of capabilities, implications, and classification of those technologies.

1.2.1. Spyware / Intrusion software

Spyware ranges from relatively simple to highly sophisticated software capable of covertly monitoring mobile phones, computers, or servers, providing access to the device and enabling surreptitious data exfiltration.

Physical access to the device may be required for its initial installation, as with parental control programs, tools used by companies for employee monitoring, or stalkerware—the term used to refer to spyware used in stalking situations. Other types of spyware only require the victim to click on a link to commence infection, whereas more advanced variants may be able to execute without any user interaction.

Currently, NSO Group's Pegasus software is the best-known example, although many others have circulated in Latin America, produced by Hacking Team (Italy), Mollitiam (Spain), Cy4gate (Italy), Intellexa (Cyprus/Israel) or FinFisher (UK/Germany) and other firms[20]. It is worth mentioning that this report only covers spyware used by law enforcement and security agencies as opposed to spyware used in relation to cybercrime (involving fraud or mass attacks for financial gain).

While there were prior cases, it was around 2015 when red flags on the issue first appeared. This happened after Italian firm Hacking Team's emails were leaked and the Inter-American Commission on Human Rights (IACHR) released a statement expressing its concern about the risks that these technologies posed for human rights[21].

---

20 A thorough inventory of spyware systems, active years, and date of their public disclosure can be found in a dataset returned by the investigation of Feldstein, Steven, and Brian Kot. *Global Inventory of Commercial Spyware & Digital Forensics.* 10 March 2023. DOI

21 Inter-American Commission on Human Rights (IACHR), Office of the Special Rapporteur for the Freedom of Speech, *Informe Anual de la Comisión Interamericana de Derechos Humanos 2015: Volumen II, Informe de la Relatoría Especial para la Libertad de Expresión,* OEA/Ser.L/V/II. Doc. 48/15, December 31, 2015, URL

These companies typically identify themselves as providers of "lawful interception" or "tactical interception" claiming they only sell to clients with legitimate surveillance needs, such as law enforcement and intelligence agencies[22]. In practice, these technologies have been repeatedly used to monitor human rights defenders, journalists, academics, politicians and even people from the corporate world. Examples from around the world are plentiful.

Nevertheless, those firms do not work alone. Spyware production is underpinned by a multimillion-dollar industry dedicated to detecting and marketing new vulnerabilities, producing exploits to take advantage of those vulnerabilities, and providing the necessary infrastructure for data exfiltration[23]. All of the above is part of a longer chain of attacks. That is why, while spyware-producing companies are especially located in Israel, Italy and India, companies within the circuit seeking vulnerabilities and producing exploits have occasionally been established in Latin America in order to recruit trained human resources in those countries.

In a few places, state use of spyware has been regulated under certain conditions. In those cases, euphemisms such as "remote acquisition of evidence", or similar, are used. Germany, France, Italy and Spain have, in different ways, set up frameworks allowing use of spyware in the context of complex criminal investigations under judicial authorization. According to a selection of critical references, in those places where state use of spyware was "normalized" under a legal framework, controversy was considerable. In Germany, the *Bundeskriminalamtgesetz* reform and the regulation of the *Online-Durchsuchung* ("online search") provide for governmental use of "state trojans" as an exceptional investigative measure subject to court order and reasonableness criteria[24]. In Italy, Legislative Decree 216/2017 incorporated c*aptatori informatici* (literally "information capturing devices") as a remote investigative technique for certain felonies. Spain has also regulated remote access to devices, online interception, and other technological measures through Ley Orgánica 13/2015. In France, the 2015 Intelligence Act allowed intrusive surveillance techniques under administrative supervision and by a specific authority. In all those cases, the analyses agree on one thing: even where there are formal legal frameworks, tension continues to exist regarding transparency, democratic control, and the risk of "normalizing" state malware as part of the ordinary investigative tools[25].

---

22 For example, NSO Group states that they only sell their products to legitimate security agencies without assuming any responsibility for the end-use of their products, and claim they have no access to data collected by their clients. NSO Group. *Transparency and Responsibility Report.* NSO Group, 2021. URL

23 For an analysis of the vulnerabilities market based on Italian firm Hacking Team's leaks, see: Burkart, Patrick, and Tom McCourt. "The International Political Economy of the Hack: A Closer Look at Markets for Cybersecurity Software." *Popular Communication* 15, no. 1 (2017): 37–54. DOI

24 European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, *The Use of Pegasus and Equivalent Surveillance Spyware: The Existing Legal Framework in EU Member States for the Acquisition and Use of Pegasus and Equivalent Surveillance Spyware* (Brussels, 2022). URL

25 Ramiro, André. "Democratic Oversight of Government Hacking by Intelligence Agencies: A Critical Analysis of Brazil and Germany." Weizenbaum Journal of the Digital Society 5, no. 2 (2025). DOI // J. J. van Berkel, A. van Uden and J.H. Goes, *Police Hacking Regulation Abroad: A Comparative Law Study into Legal Regulations and Safeguards Regarding the Quality of Data* (The Hague: WODC, 2023). URL

To sum up, even in formalized contexts, the use of such technologies continues to be highly controversial due to their intrusive nature and considerable risk of abuse. For example, Amnesty International classifies spyware as "highly invasive" based on the fact that, from a technical viewpoint, spyware is designed to leave no traces, operate covertly without further controls, and to obtain the largest possible amount of unfiltered data[26].

Overall, these technologies fail to incorporate safeguards to protect users' rights. They only protect the business model of manufacturers and vendors. In fact, according to a recent investigation, firms, such as Intellexa, keep direct access to the information collected by the purchasers of their spyware systems[27].

26 Amnesty International Security Lab, "Predator Files: Technical Deep-Dive into Intellexa Alliance's Surveillance Products", 2023. URL

27 Amnesty International Security Lab, "To Catch a Predator: Leak Exposes the Internal Operations of Intellexa's Mercenary Spyware", December 4, 2025. URL

Box 1: Spyware / Intrusion software

Spyware	
Intrusion	Remote intrusion in devices (phones, computers, servers)
Infection	Infection through exploitation of 0-day, 1-day, N-day vulnerabilities; phishing; physical installation (stalkerware, parental control); malicious traffic injection.
Type of attack	Active and targeted
Necessary infrastructure	Necessary infrastructure: everything connected to the different phases of the attack, ranging from infection to potential anonymization nodes to monitoring
Type of access	Remote control; customized spying; data exfiltration.
Collected data	Files, messages, location, camera access.
Examples in South America	Pegasus (NSO), Remote Control System (Hacking Team), *Night Crawler* (Mollitiam), etc.

Spyware: timeline

2007

- German law enforcement and security agencies first use the surveillance trojan "Skype Capture Unit," developed by DigiTask, also known as "Bundestrojaner" and "R2D2".

A PARTIR DE 2010

- Early expansion of commercial spyware (e.g., FinFisher).

2012

- First reports by Citizen Lab on FinFisher and Hacking Team.
- Spyware is included in the Wassenaar Arrangement.
- First reported uses of NSO Group's Pegasus in Panama.
- First reported uses of FinFisher in Paraguay.

2013

- First reported uses of Hacking Team spyware in Colombia, Mexico, Ecuador, and Honduras.
- NSO Group (Israel) and Hacking Team (Italy) come into contact with governments across South America, including Chile, Argentina and Uruguay.

2014

- Chile acquires spyware from Hacking Team.
- Argentina seeks legalization of "remote surveillance of computer systems" at the federal level and holds talks with NSO Group and Hacking Team.
- Mexico acquires FinFisher spyware.

2015

- Hacking Team's leak of e-mails.

2016

- Journalistic investigations and reports on spyware begin to emerge in South America.
- Mexico acquires NSO Group's Pegasus.
- Citizen Lab releases its first public forensic report on Pegasus and identifies NSO infrastructure stemming from a concrete case.

2017

- Early civil-society reports document spyware use against journalists, activists, and politicians, based on forensic samples from their devices.

2018

- First report by Amnesty International's Security Lab on NSO Group.

2019

- Public disclosure that Brazil had acquired Hacking Team's RCS years earlier.
- WhatsApp/Meta sues NSO Group.
- The Inter-American Commission on Human Rights (IACHR) raises concern about the risks posed by spyware for human rights.

2020

- First reported use of Pegasus in El Salvador.

2021

- Amnesty Tech and Forbidden Stories, together with a network of media outlets, publish The Pegasus Project: a massive leak and forensic verification of infections and targeting worldwide.
- Apple sues NSO Group over the exploitation of iOS/iMessage vulnerabilities to abuse Apple services and infect devices.
- Reports surface of spyware developed by Mollitiam and Cytrox being used in
- Mexico acquires REIGN spyware developed by Israeli firm Quadream.
- Amnesty International's Security Lab launches Mobile Verification Toolkit (MVT), a forensic analysis tool to consensually identify indicators of compromise (IoCs) on cell phones.

1.2.2. Signals Intelligence (SIGINT)

The term encompasses tools for the interception, monitoring, analysis, and geolocation of electromagnetic signals. This covers a wide variety of devices used by law enforcement and security agencies: signal inhibitors (jammers) to block or degrade communications along specific bands; spectrum analyzers to visualize and characterize signals across various frequencies; and direction-finding (DF) tracking systems, such as portable antennas capable of estimating the direction of signal emissions, among others.

This report examines two specific technologies used for the interception, monitoring, and tracking of mobile devices: IMSI catchers and geolocation tools exploiting the SS7 signaling protocol.

(1.2.2.a.) *IMSI Catchers and Cellular Signal Interception*

IMSI catchers are widely used by law enforcement and security agencies in many jurisdictions worldwide. Compared with other tools analyzed here, aspects of their commercialization tend to be relatively more visible than those of other interception technologies discussed here. They consist of cellular base-station transceivers with extended signal coverage that masquerade as legitimate cellular base stations in order to collect subscriber identifiers (such as IMSI values) from mobile devices connecting to them. This was possible under the GSM/2G protocol architecture, which required only the handset to authenticate with the network, but did not require the network to authenticate with the device. As a result, devices would trust any base station compliant with the protocol. In 3G and 4G, mutual authentication between the device and the network was introduced. However, in practice, many commercial IMSI catchers force devices to downgrade to 2G. Furthermore, recent research has shown that it is also possible to develop IMSI catchers on LTE/4G capable, at least under certain conditions, of identifying devices[28]. It is important to note that IMSI catchers rely on design weaknesses in GSM/2G and on the ability to downgrade 3G/4G connections to less secure modes, while taking advantage of protocol and implementation characteristics which allow the identification and tracking of devices[29].

---

28 In 5G, a concealed identifier (SUCI) was introduced, which encrypts the subscriber's permanent identity (SUPI) to prevent traditional IMSI catchers from directly obtaining it. However, recent research has demonstrated attacks known as "SUCI catchers", in which a fake antenna uses the 5G authentication protocol itself to test whether a given SUCI corresponds to a particular subscriber, or whether the same user is present at a given location. This enables additional forms of tracking despite the privacy improvements introduced in 5G authentication mechanisms. Merlin Chlosta, David Rupprecht, Christina Pöpper, and Thorsten Holz, "5G SUCI-Catchers: Still Catching Them All?," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks.* New York: ACM, 2021, 359–364, DOI

29 Audun Jøsang, Laurent Miralabé, and Léonard Dallot, "Vulnerability by Design in Mobile Network Security," *Journal of Information Warfare* 14, no. 4 (2015): 86–98, URL

Specifically, IMSI catchers capture both the subscriber identity associated with the SIM card (IMSI, International Mobile Subscriber Identity) and the device's international identifier (IMEI, International Mobile Equipment Identity).

When these antennas are deployed at strategic locations by security forces, they can, for example, identify all participants in a protest, disrupt services, or in some cases even downgrade connections from 4G to less secure standards, such as 3G or 2G, in order to intercept SMS messages[30].

This hardware is produced by a large number of manufacturers, and in some cases it is even produced locally in industrial facilities in countries that do not typically develop other forms of interception technology. However, a recognized group of manufacturers exports IMSI catchers around the world, such as: Almenta, L3Harris, Pat Systems, Pen-Link and Verint from the United States; Kavit, Pisces, Septier and Phantom from Israel; together with some others, such as Elaman (Germany), Neosoft (Switzerland), Tykelab (Italy), X-Surveillance (Netherlands), and Smith Myers and Revector (United Kingdom).

Box 2: How does an IMSI catcher work?

Definition	**A mobile or fixed antenna masquerades as a legitimate tower from the telecommunications provider to identify and track phones within a specific range.**
Connection	It broadcasts as a base station with a strong signal. Phones automatically connect to it as if it were a legitimate service provider antenna.
Identification	It captures IMSIs, IMEIs and, depending on the model, also session metadata.
Tracking	Using Direction Finding (DF), signal strength, and movement, it enables the tracking of specific targets.
Advanced capabilities	It can block connections, downgrade connection type (to 3G or 2G) and enable interception of calls and SMS.
Impact	It operates indiscriminately, recording data from all devices within reach.

30 Park, Shinjo, Altaf Shaik, Ravishankar Borgaonkar, and Jean-Pierre Seifert. "Anatomy of Commercial IMSI Catchers and Detectors." *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society* (New York, NY, USA), WPES'19, Association for Computing Machinery, November 11, 2019, 74–86. DOI

(1.2.2.b.) Telephonic Signaling Attacks

These tools typically operate through the signaling infrastructure of mobile networks and their global interconnection. They exploit vulnerabilities in the SS7 and/or Diameter signaling protocols used in mobile network infrastructure and international interconnections (2G, 3G and 4G)[31].

SS7 is the signaling system of the traditional telephone network and is used both in fixed-line telephony and in 2G/3G mobile core networks. In LTE/4G and in parts of 5G, the central signaling protocol shifts to Diameter, although SS7 remains necessary to interconnect those services with legacy networks and for certain roaming scenarios. The problem lies not only in vulnerabilities inherent to the protocols; it also lies in the deployment of infrastructure with insecure configurations implemented, and allowed, by telecommunications operators[32].

The technologies acquired by law enforcement and security agencies send messages typically intended for use in international roaming. These messages exploit vulnerabilities in the SS7 and Diameter protocols and can be used to obtain the location of mobile subscribers through signaling requests such as *sendRoutingInfoForSM* or *ProvideSubscriberInfo*. By issuing signaling queries, agencies can remotely track a device's location without the consent of the network operator, monitor users' movements across borders via roaming services, and determine when the subscriber is active.

These technologies can also send continuous requests that trigger denial-of-service (DoS) conditions, ultimately forcing a device to detach from the network and temporarily blocking communications. They can also manipulate signaling routes to divert calls or text messages. This is typically achieved by sending a forwarding instruction to the network to mislead the originating node and cause it to re-route traffic to a specific device controlled by the security agency. In this way, SMS messages can be intercepted, undermining their use as a second authentication factor (2FA). In practice, however, security agencies appear to rely on these tools primarily for the geolocation of specific phone numbers or subscribers[33].

Recent technical reports—including *Finding You* by Citizen Lab, based on data from the Mobile Surveillance Monitor (MSM), a global monitoring initiative tracking mobile surveillance threats—document the existence of private companies that sell this type of anomalous signaling access as a service to state actors seeking to geolocate targets on a global scale. In such cases, law enforcement and security agencies do not need to purchase equipment or software to carry out these signaling attacks.

---

31 Holtmanns, Silke, Siddharth Prakash Rao, and Ian Oliver. "User Location Tracking Attacks for LTE Networks Using the Interworking Functionality." *2016 IFIP Networking Conference* (IFIP Networking) and Workshops, May 2016, 315–22. DOI // Marczak, Bill, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert. *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*. Citizen Lab Research Report No. 133. University of Toronto, 2020. URL

32 Especially relevant are the datasets of the "Network Research Workbook". Not only do they report the quantity of suspected events; they also record the vulnerable infrastructure that enables these attacks: URL

33 Miller, Gary, and Christopher Parsons. *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure*. No. 171. Citizen Lab, University of Toronto, 2023. URL

Instead, they can acquire the service from one of these companies and pay for a set number of queries, which are routed remotely and produce near-immediate responses[34].

NSO Group also produces one of the best-known tools in this field, marketed under the name Circles. Other companies commercialize similar products in Latin America, including Ability (Israel), Pat Systems (United States), Rayzone (Israel), Telesoft (United Kingdom), Tykelab (Italy), Elaman (Germany), and Verint/Cognyte (United States/Israel).

34 Lighthouse Reports. *Surveillance Secrets: How First Wap Tracks Phones Around the World.* Lighthouse, 2025. URL

Box 3: *Signaling Attacks through SS7/Diameter — How do they work?*

<table>
<tr><td>What are SS7 and Diameter?</td><td colspan="4">SS7 and Diameter are protocols used among telecommunications providers to:
• identify which base station a phone is connected to and deliver the appropriate signaling data;
• activate roaming services;
• route calls and SMS.</td></tr>
<tr><td>How does the attack work?</td><td>1
The phone connects to its telecommunications operator as usual.</td><td>2
Telecommunications operators exchange SS7 or Diameter messages to manage each number’s location, calls, and SMS.</td><td>3
An attacker manages to send messages through vulnerable infrastructure impersonating a legitimate operator.</td><td>4
The network trusts these rogue requests and, depending on the request, returns specific information.</td></tr>
<tr><td>This enables the attacker to:</td><td>A.
Determine where a device is located

➜ The network responds with an approximate location.</td><td colspan="2">B.
In certain cases, using only internal control signaling, it is possible to obtain additional information about the traffic associated with that number.

➜ The attacker can send “normal” queries, but with surveillance intent—for example, messages requesting routing information or the status of a number. From these responses, the attacker can reconstruct when events occur, and determine when and from where the target communicates.</td><td>C.
Using the same control messages, it is possible to interfere with or redirect SMS messages, or affect voice calls.

➜ The attacker sends rogue SS7 messages instructing the network to change routing parameters (for example, where SMSs should be delivered).

➜ The network updates its records as if the request were legitimate. SMS messages then pass through infrastructure controlled by the attacker before reaching the user, or may never arrive at all.</td></tr>
<tr><td>Conclusion</td><td>The attack consists of querying the internal signaling network used between mobile operators, sending signaling messages through SS7 or Diameter.</td><td colspan="2">In other words, SS7 and Diameter do not carry the content of communications directly; they carry the internal signaling instructions that make those communications possible.</td><td>While these techniques can be used to deny service or intercept calls and messages, they are used primarily for geolocation.</td></tr>
</table>

1.2.3. Lawful Interception (LI) and Network Intelligence

So-called lawful interception technologies are built directly into a communications provider's infrastructure. Their stated purpose is selective interception carried out under formal legal authorization in accordance with national legal frameworks. Typically, these systems are purchased by law enforcement agencies—often also accessible to intelligence services—and deployed within telecommunications operators' networks. Providers must structurally comply with interception requirements in order to enable lawful surveillance. Meanwhile, law enforcement agencies acquire monitoring and analysis systems through which operators deliver intercepted data via standardized handover interfaces[35]. Innova (Italy), SS8 (United States), and Trovicor (Germany) are frequently cited as providers of lawful interception technologies[36].

Beyond the basic capabilities of lawful interception and regulatory handover interfaces, many of the commercial tools marketed today combine LI with intelligence analytics intended for investigative uses, sometimes marketed as "lawful intelligence" or "network intelligence." As a result, additional data sources can be incorporated, including those derived from communications monitoring conducted by service providers.

In operational terms, this often takes the form of a monitoring center for security forces that not only processes standardized lawful interception data but also reconstructs communications, enables search and filtering, and allows correlation and enrichment of data with location information, to generate dossiers, connections, profiles, timelines, and alerts. These applications of "network intelligence" are intended to transform large volumes of traffic data into investigative inputs. Network intelligence constitutes an analytical layer that adds correlation, enrichment, and advanced analytics to transform such data into patterns, profiles, trends, and anomaly detection outputs[37].

---

35 Under ETSI standards, these standardized modules are designated HI2 and HI3 for IRI and CC, respectively. HI2 and HI3 ("Handover Interfaces") are the delivery interfaces defined in lawful interception specifications: HI2: the channel used to deliver IRI (Intercept Related Information)—the event's metadata (for example, who is communicating with whom, when, from where, and relevant identifiers). (This does not necessarily include the communication's content)—; HI3: the channel used to deliver CC (Content of Communication)—the content itself (voice, data, or messages, depending on the case and scope of the authorization)—.

36 In today's technical and political landscape, the term SORM provider—System for Operative Investigative Activities, from Russian term COPM—is used to describe companies that design, install, or maintain communications' lawful interception platforms embedded directly within operators' networks to capture both content and traffic metadata. From a technical standpoint, SORM and lawful interception systems perform equivalent functions. SORM is historically associated with Russian state surveillance infrastructure, characterized by direct access to networks. By contrast, "lawful interception" typically refers to regulated and auditable lawful interception implemented in accordance with international standards. As a result, the term SORM is generally reserved for technologies of Russian origin, emphasizing the possibility that communications intercepted through such systems may be directly accessible by the Russian federal security service.

37 See for example specifications for those products in this segment: Brookcourt Solutions Limited, "Intellego XT Monitoring Centre - SS8," Digital Marketplace (G-Cloud 14), URL; Cognyte, "Network Intelligence Solutions," URL

These systems typically access network infrastructure, duplicate or divert traffic toward internal interception or mediation functions, perform packet inspection, and—depending on the product—enable real-time device tracking and access to traffic metadata.

Most such tools require cooperation from service providers and presuppose integration and mediation within the network, or privileged access to capture points. However, there is little public transparency regarding the scope of this cooperation and the actual extent of deployed capabilities. Methods are rarely documented, and some product specifications suggest they are designed to connect to infrastructure without the need for operator authorization[38].

Even when official documentation is readily available, descriptions of the capabilities of these tools are, once again, ambiguous. For example, in a 2013 product catalog, Italian firm Innova claimed that its EGO platform could capture IP communications by accessing network infrastructure and could decode and reconstruct the content of communications within its interface. To operate, EGO required connection to network infrastructure—providers, intermediate nodes, IP exchange points—in order to divert traffic toward the interception system[39]. Still, there is no verified public information about its methods or capabilities. As a result, the functionalities of EGO's various modules, which continue to evolve, remain unclear.

German company Trovicor is a long-standing supplier of lawful interception and offers components that connect to operators' core networks in response to requests from law enforcement and security agencies[40]. Similarly, US firm SS8 provides mediation and interception solutions capable of integration. Other companies, including Ericsson, Nokia, Utimaco, and Verint / Cognyte, have also offered (or integrated) products and components related to regulatory handover mandated in lawful interception[41].

---

38 It is reasonable to assume that they rely on techniques similar to those documented in systems such as those developed by Intellexa Alliance. Reported methods include deep packet inspection integrated with other interception tools, as well as metadata analysis systems capable of recording distinctive network traffic patterns generated whenever a specific phone receives a new encrypted message or a notification from a messaging app, for identification purposes. Regarding access to encrypted traffic, documented techniques include DNS manipulation and the use of SSL/TLS certificates between the user and the service being accessed, in cooperation with internet service providers. Amnesty Tech. "Predator Files: Technical Deep-Dive into Intellexa Alliance's Surveillance Products." Amnesty International Security Lab, October 6, 2023. URL

39 According to its product documentation, EGO, of Innova S.p.A., is described as a modular and scalable lawful interception platform that integrates interfaces for fixed-line and mobile telephony, IP data, email, MMS, and video communications. It supports the recording of conversations, metadata capture, and GPS location tracking, and includes a repository with time-stamping and digital signatures to ensure evidentiary integrity, supports case and user management, centralized auditing, and is designed to adapt to new network and transport formats through APIs. According to Innova's technical manual (2011) and follow-up on secondary sources, EGO "enables to intercept [sic], decode and restore on the same interface all types of IP communication, such as Video-communications, MMS..." Innova. "Investigations Instruments." Innova, 2013. URL

40 Trovicor. "Trovicor Intelligence Solutions." Trovicor, 2012. URL

41 Global Market Insights Inc. "Lawful Interception Market Size, Share, Trends & Forecasts 2034." 2025. URL

At the regional level, the government of Peru acquired a system from Israeli firm Verint/Cognyte, known as "Pisco", for approximately US$22 million, intended to intercept and monitor satellite, voice, and IP data communications. This has prompted claims about potential privacy violations affecting millions of citizens[42]. Media coverage of the project indicated that the acquired suite included products such as Reliant and Vantage, described as tools designed to "intercept, filter, and analyze large volumes of IP, voice, and satellite traffic[43]." These products are likely in use elsewhere in the region.

It is worth noting that, on numerous occasions, these companies offer different modules spanning lawful interception, network traffic analysis and monitoring. NarusInsight, for example, has been described as a high-capacity backbone capture platform. It is mentioned that intercepted traffic can flow into interception components such as NarusInsight Intercept Suite for storage and forensic or surveillance analysis, while other modules are marketed as supporting traffic intelligence for network management and security[44].

Alerts about these types of IP traffic interception technologies appeared early, dating back to the expansion of internet access at the turn of the century. In 2005, regulations previously mentioned, such as the U.S. Communications Assistance for Law Enforcement Act (CALEA), were extended to include broadband providers, requiring them to ensure interception capabilities in their networks[45]. Early warnings appeared around a landmark case involving Narus, which developed advanced deep packet inspection systems capable of analyzing vast amounts of traffic in real time[46]. As early as 2006, its technology became controversial when it was revealed that it had been used by the NSA in cooperation with AT&T to conduct large-scale communications surveillance[47].

More recently, research by Citizen Lab documented cases in which service providers redirected traffic through deep packet inspection modules, including traffic injection attacks for spyware installation. While such practices fall outside lawful interception according to European standards (ETSI), they do illustrate how capabilities at the network layer can be used for surveillance or manipulation[48].

---

42 Associated Press, *"In Peru, Govt Buys Secret Tool for Mass Surveillance"*, quoted in EFF – *Surveillance in Latin America: 2016 in Review*, January 2, 2017. URL

43 Bajak, Frank, and Jack Gillum. "With Cheap Israeli Spy Tools, Nations Are 'Monitoring Everyone.'" *The Times of Israel*, August 3, 2016. URL

44 IBM. "NarusInsight." IBM, 2009. URL // Sandvine. "PacketLogic 8000 Platforms™ Scalable Network Intelligence and Policy Enforcement Platform." Sandvine, 2019. URL

45 Electronic Frontier Foundation. "FAQ on the CALEA Expansion by the FCC." *Electronic Frontier Foundation*, 2007. Consulted December 8, 2025. URL

46 Staff, WIRED. "Stumbling Into a Spy Scandal." Tags. *Wired*, May 17, 2006. URL

47 According to the testimony of former AT&T technician Mark Klein, Narus STA 6400 devices were used to copy and monitor NSA-inbound traffic. "NARUS, Deep Packet Inspection and the NSA." *Privacy SOS*, 2013. URL

48 Citizen Lab documented—through internet-wide scanning, forensic analysis of second-hand PacketLogic equipment, and laboratory testing—DPI devices (PacketLogic) being deployed within operator networks—primarily within Türk Telekom and at points of Telecom Egypt—to redirect legitimate downloads toward malicious spyware installers. Marczak, Bill, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert. *BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?* Citizen Lab Research Report No. 107. University of Toronto, 2018. URL

In this context, the 2014 transparency report by Vodafone—one of the world's largest telecommunications companies—is worth mentioning. The report outlined how the company's procedures vary in response to government requests for customer data, depending on the regulatory framework of each country in which it operates. The report distinguishes between two types of requests for information:

(1) Communications information in connection with a specific event, which entails identifying a user (by phone number or IP address), call duration, device location, or other metadata, without accessing content.

(2) Requests for lawful interception (LI), which, according to Vodafone, are less common but typically require access to the content of communications[49].

As noted earlier, most of these tools typically rely on cooperation from Internet service providers[50]. Yet questions remain about implementation and use, particularly in the face of contractual opacity, authoritarian digital practices, or weak controls over security forces and intelligence agencies.

In this regard, academic research suggests that an actor with physical control over an international transit point or a major network node can significantly enhance its ability to observe or manipulate traffic passing through that point, even without full ISP cooperation[51]. That is why it is important to mention that serious questions arise about the actual possibility of using such tools without mediation by the relevant Internet service provider. Similarly, product descriptions of some of those tools suggest their independence from formal requests.

A widely cited 2014 paper titled "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" analyzed how the FBI can access communications by exploiting network vulnerabilities beyond traditional legal channels[52]. This reinforces the idea that access to communications can rely on other associated tools, combining infrastructure control, vulnerability exploitation, and intrusion capabilities. The Citizen Lab report cited above provides a clear example of this dynamic.

For these reasons, technical standards issued by the European Telecommunications Standards Institute (ETSI) on lawful interception specify that "law enforcement systems" should never be integrated directly into the architecture of the public network, preserving separation between network functions and monitoring

---

49 Vodafone and Hogan Lovells. Law Enforcement Disclosure Report. Vodafone, 2015. URL

50 Ericsson. *Regulatory Products: Communication Services UDM and Exposure*. Ericsson, 2020. URL // Sandvine. *Sandvine Datasheet: PacketLogic15000 Platform*. Sandvine 2019. URL // SS8. "Solutions: Compliant Mediation and Interception." SS8, 2021. URL

51 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian*, June 21, 2013, URL // Murdoch, Steven J., and Roger Dingledine. "Sampled Traffic Analysis by Internet-Exchange-Level Adversaries." *Proceedings of the PET '07 Workshop on Privacy Enhancing Technologies* (2007). The article proposes that an adversary controlling an IXP traversed by traffic between customer and server can analyze that traffic even without the cooperation of the original ISP. URL

52 In 2014, this paper explained "the viability and implications of an alternative method for addressing law enforcement's need to access communications: legalized hacking of target devices through existing vulnerabilities in end-user software and platforms. The FBI already uses this approach on a small scale; we expect that its use will increase, especially as centralized wiretapping capabilities become less viable". Bellovin, Steven M., Matt Blaze, Sandy Clark, and Susan Landau. "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet." *Northwestern Journal of Technology and Intellectual Property* 12, no. 1 (2014): 66. URL

functions[53]. In the United States, by contrast, there is no single equivalent body, such as ETSI, publishing a comprehensive lawful interception architecture. The framework centers on CALEA, which imposes functional obligations on operators, while technical specifications are developed within industry standardization bodies, often accredited by the American National Standards Institute (ANSI). These standards leave significant design discretion to manufacturers and operators as to how to integrate interception capabilities on specific networks. It is important to note that even when the products claim compliance with ETSI or ANSI standards, such certification alone does not guarantee suitability in South American jurisdictions, where legal, regulatory, and oversight frameworks may differ—or be less transparent.

Furthermore, there are cases where lawful interception requests could be subject to discretionary use. If law enforcement or intelligence agencies lack effective oversight, interception systems can be used outside formal regulatory mechanisms. For example, in 2008, CIPER published a report describing how lawful telephone interception operates in Chile. The report notes that, in addition to the formal process involving a court warrant and the cooperation of telecommunications companies, parallel or informal methods for obtaining communications have also existed. This illustrates that even when the system is technically well implemented, the absence of effective controls over its use can lead to improper access or discretionary practices[54].

In this regard, academic literature warns that tools for the interception, analysis, and retention of communications data—authorized by legislation in most countries—can be as politically consequential as those involving attacks designed to compromise devices[55].

---

53 ETSI, *Lawful Interception (LI): Concepts of Interception in a Generic Network Architecture* (ETSI TR 101 943 V2.2.1, 2006, URL

54 Peña, Cristóbal and Sebastián Minay,. "Así se hacen los cuestionados 'pinchazos' telefónicos legales." Investigación. *CIPER Chile*, October 29, 2008. URL

55 For example: White, Matthew. *Surveillance Law, Data Retention and Human Rights: A Risk to Democracy.* Routledge, 2024. DOI

Box 4: Some lawful interception solutions

Product	Manufacturer	Primary function	Reference
EGO	Innova (Italy)	IP traffic interception. Captures and decodes communications; it requires operator access.	*Innova – catalogue*
ULIS (Unified Lawful Interception Suite)	Thales (France)	Lawful interception suite for operators allowing transparent, real-time interception, data and multimedia communications.	*Datasheet*
NarusInsight Intercept Suite	Narus (US; acquired by Boeing in 2010)	Interception suite focused on real-time "precision targeting": IP traffic capture and reconstruction (including webmail) and packet-level, flow-level and application-level data collection for forensic analysis, surveillance and regulatory compliance.	*Press article*
Trovicor LI Solutions	Trovicor (Germany)	Lawful interception gateways integrated with operators' core.	*Company overview*
SS8 Intercept & Mediation	SS8 (U.S.)	Metadata mediation and analysis. Correlation and handover of communications and location data.	*Official webpage*
Verint *STAR-GATE* (or STAR-GATE Lite)	Verint / Cognyte (Israel/U.S.)	Interception on infrastructure. LI platforms and analysis tools.	*Verint STAR-GATE Mediation Device Configuration*
Ericsson LI-IMS	Ericsson (Sweden)	Regulatory lawful interception tools. LI regulatory compliance gateways integrated into operators' core networks.	*Ericsson solutions*

1.2.4. Traffic management and monitoring

Network traffic management encompasses deep packet inspection (DPI) and content filtering. Although these systems are widely used by Internet Service Providers (ISPs), their capabilities and uses make it necessary to examine them as surveillance-enabling technologies.

These tools enable the analysis and classification of data traffic by processing packets, communication protocols, URL requests, and DNS queries. They are typically used to optimize network performance, security, and usage analytics. They can also block domains or IPs, prioritize, degrade applications, or apply varied filtering policies. Among the most common techniques is deep packet inspection (DPI), which examines information at the top layers of the protocol stack—such as HTTP headers when traffic is unencrypted, or metadata from the TLS handshake when it is encrypted. There is also DNS query analysis, used to identify the visited domains; and flow analysis, which aggregates metrics such as traffic volume, duration, and destination.

Among the leading commercial tools in this category—both in Latin America and globally—are companies such as Sandvine (Canada/US) and Blue Coat (US), as well as solutions from Cisco and Palo Alto Networks. All are integrated into the infrastructure of operators or large-scale networks to enable network traffic management[56].

Because of their granular capacity to observe and control communications, the censorship and surveillance potential of these technologies has long been recognized for many years[57]. In fact, Citizen Lab documented the deployment of Blue Coat equipment, such as ProxySG, in Syria, Sudan, and Iran, in association with censorship, content filtering, and abusive monitoring of web traffic[58].

For these reasons, civil society organizations working on these issues routinely scrutinize those capabilities of operators[59]. In Latin America, there are hints of regional contracts involving multiple telecommunication companies. According to information published by AppLogic Networks, Sandvine reportedly signed an agreement worth roughly USD 12 million with large-scale Tier 1 backbone operators covering eleven countries in the region, with the purpose of implementing traffic analysis capabilities and network intelligence use cases—though the specific providers involved were not identified[60]. It is also worth noting that Sandvine faced regulatory constraints after being placed on the "Entity List" of

---

56 Privacy International. *Monitoring Centres: Force Multipliers From The Surveillance Industry.* April 29, 2014. URL

57 Fuchs, Christian. *Implications of deep packet inspection (DPI) Internet Surveillance for Society*. Centre for Science, Society & Citizenship, 2012. URL

58 Marquis-Boire, Morgan, Collin Anderson, Jakub Dalek, Sarah McKune, and John Scott-Railton. *Some Devices Wander by Mistake: Planet Blue Coat Redux*. Citizen Lab and Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, 2013. URL

59 Lara, Juan Carlos, and Francisco Vera. *Responsabilidad de Los Prestadores de Servicios de Internet.* No. 3. Policy Papers. Derechos Digitales, 2013. URL

60 AppLogic Networks. *Sandvine Wins USD 12 Million Network Intelligence Contract Covering 11 Latin American Countries.* AppLogic Networks, April 6, 2019. URL

the U.S. Department of Commerce in February 2024, accused of selling technologies used for political surveillance or repression, although it was later removed from the list in October 2024 following corporate reforms[61].

From our perspective, one useful way to approach these monitoring tools is to classify them based on the depth of traffic analysis. 1) Flow or metadata analysis tools: they do not capture full packets; rather, they collect information on sessions, time, volume, and destinations; they allow the analysis of connections, patterns, and attributions without accessing content. 2) Full packet capture technologies: if there is no encryption, the tool provides access to content and, in all cases, allows operators to reconstruct sessions. 3) Deep packet inspection (DPI): going beyond headers, DPI enables traffic identification and classification in order to record, block, or reprioritize traffic, and extract richer application-layer metadata.

This category partly overlaps with the previous one. The distinction between Internet monitoring tools (such as Blue Coat) and network-intelligence interception platforms (such as Innova, SS8, or Utimaco) is often defined in terms of intrusiveness, intended use, and the legal context in which they operate. However, that line is increasingly blurred as these technologies converge.

Sandvine is a revealing example. Tools originally built for traffic monitoring and management—such as Sandvine PacketLogic—have added features including deep packet inspection, automated metadata analysis, and techniques to classify traffic even when it is encrypted (without accessing content, but with capabilities that mirror elements of intelligence systems and point to potential use for network-level surveillance). As a result, from a technical standpoint, these two categories of technology are increasingly interconnected. In terms of use and intent, the boundary between corporate network monitoring and intelligence-oriented surveillance has also become increasingly undefined. Technical research has shown, for example, cases in which PacketLogic devices were used, at the ISP level, for redirection, injection, and deployment of spyware—illustrating the potential for abuse of these capabilities[62].

In conclusion, it is useful to distinguish four categories of tools:

(i) Lawful Interception (LI) refers to the selective, authorized interception of designated "selectors" or targets (such as users, IPs, IMSIs, or IMEIs). Its defining characteristic is the standardized handover from the service provider to the authority, transmitting associated data and, when applicable, the content of communications as well.

(ii) Network monitoring operated by the service provider and aimed at ensuring availability, performance, capacity, and fault detection.

(iii) Deep Packet Inspection (DPI) refers to a deeper packet inspection technique that enables classifying traffic and applying policies, including content-based filtering or blocking scenarios. For that reason, it often appears as an embedded "engine" within security, monitoring, or analytics solutions.

---

61 Light Reading. "US Adds Sandvine to Entity List over Surveillance Sales." *Light Reading,* October 2024. URL

62 Gjesvik, Lars, and Johann Ole Willers. "Beyond Control? The Political Economy of Private Interception, Intrusion, and Surveillance Markets." *Review of International Political Economy 31*, no. 6 (2024): 1840–64. DOI

(iv) Network intelligence builds on data generated in other ways through network monitoring while adding correlation, enrichment, and analytics to produce patterns, profiles, trends, and anomaly detection outputs.

It is worth noting that lawful interception is subject to clear technical standards including specifications on which kinds of data must be retained; there is no comparable standard that requires, or regulates, the systematic handover of an ISP's operational monitoring or DPI outputs (as produced by tools such as Sandvine, Allot, etc.) to law enforcement. However, there typically exists a legal or procedural framework defining when and why such information may be requested.

Box 5: Network Traffic Management: functions and risks

Aspect	Description / Primary function	Examples of tools	Lawful uses	Risks and controversies
Deep Packet Inspection (DPI)	It analyzes the content of data packets beyond headers, including at the application layer (HTTPS).	Sandvine PacketLogic, Huawei eSight, Blue Coat ProxySG	Traffic optimization, congestion management, malware or intrusion detection.	Privacy invasion, content censorship, mass surveillance, traffic discrimination, violation of net neutrality
Traffic filtering and blocking	It identifies and blocks URLs, IPs or domains based on predefined rules or blocklists.	Blue Coat, Palo Alto Networks, Cisco Umbrella	Anti-phishing protection, parental controls, and enforcement of corporate policies.	Censoring of political or social information, arbitrary content blocking, and restrictions on digital freedoms.
DNS query analysis	It examines domain name resolutions patterns to infer which sites users visit.	ZTE NetNumen, integrated ISP solutions	Improving network performance and security, detecting anomalies.	Tracing browsing behavior, creation of user profiles, non-consensual surveillance.
Flow analysis	It evaluates aggregated traffic statistics: volume, duration, destination, ports.	Cisco NetFlow, Huawei eSight	Capacity management, performance diagnosis, infrastructure planning.	Indirect identification of users or groups, correlation with surveillance metadata, de-anonymization
Encrypted traffic inspection	It intercepts or analyzes HTTPS traffic through metadata or certificates analysis.	Sandvine, Palo Alto Networks, Blue Coat SSL Visibility Appliance	Corporate security monitoring, detection of encrypted threats.	Privacy infringement, exposure of personal information, governmental or corporate abuse.
Technological convergence (monitoring and surveillance)	Integration of monitoring, intelligence and control functions in the same infrastructure.	Sandvine, Huawei eSight, Blue Coat ProxySG	Unification of network management systems, efficiency improvement.	Blurring of legal boundaries, dual-use (civil/military), mass surveillance disguised as technical management.

Box 6: Some network monitoring solutions

Tool / Manufacturer	Relevant functions	Documented presence or use in Latin America	Notes
Sandvine (Active Network Intelligence, PacketLogic, etc.) (Canada)	DPI, traffic classification, application-layer analysis, policies, traffic management, real-time analysis.	Used by operators—large (Tier-1) infrastructure providers—in several Latin American countries.	They have sold "use case" modules in 11 Latin American countries (*AppLogic Networks*). Their technology can be used either for optimization or for blocking/profiling.
Huawei eSight / Huawei network solutions (China)	Network management, monitoring, analysis, and traffic visibility	Huawei markets solutions for Latin American ISPs (for example, "Premium Wi-Fi 2.0" for ISPs in Latin America) (*es.hi-network.com*).	eSight is more oriented to network management (though it can include traffic-monitoring functions as well) (*Huawei Enterprise*). Given Huawei's extensive presence across Latin American networks, it would be easier to integrate DPI capabilities or other modules.
Blue Coat ProxySG / Blue Coat PacketShaper (US)	Web content filtering, SSL/ TLS inspection, application-layer control, reverse proxying, categorization.	Various products from Blue Coat have been deployed in the region, mainly Argentina, Chile, and Venezuela (*The Citizen Lab*).	Citizen Lab has also documented that ProxySG and PacketShaper devices have been used for censorship and surveillance (*The Citizen Lab*).
Allot (Service Gateway / DART; HomeSecure/ NetworkSecure/ WebSafe) (Israel)	DPI, traffic classification and identification, application analytics, analysis per application/ user/device, real-time analytics, and policy enforcement / congestion management	HomeSecure was selected by a Tier-1 fixed-line operator in Latin America in 2023, and Más Móvil Panamá regarding NetworkSecure (2025).	Dual-use technology: it can be used for optimization/QoE and cybersecurity, but it also enables filtering/ profiling/ blocking (for example, URL blacklists on account of "regulatory compliance"), depending on how policies are configured. *Allot* (outside Latin America, there have been reports of Allot's DPI being used in censorship-related contexts) *URL*

Box 7: Network monitoring vs. Network intelligence

The distinction between Internet monitoring tools (such as Blue Coat) and network interception and intelligence systems (such as EGO, Utimaco, and SS8) is often based on their ability to single out traffic using specific criteria centered around an individual—or groups of individuals—their post-processing capabilities for captured data, the level of intrusiveness involved, their intended purpose, and the legal frameworks in which they operate. Useful as this distinction may be, it is also increasingly blurred by the convergence of these technologies.

Tool type	Network monitoring	Network intelligence
Main purpose	Network performance, regulatory constraints, statistics	Investigation, profiling, geolocation, and interception.
Typical data	Metrics, logs, NetFlow (network flow records: protocols, ports, bytes transferred, duration), PCAP (packet capture for troubleshooting: headers + payload).	Enriched metadata, transcriptions, profiles, and historical correlation
Content vs metadata	Primarily metadata; packet capture, only occasionally for diagnostic purposes	Both, with an emphasis on correlating metadata and content when legally authorized.
Time	Real-time	Real-time + retrospective analysis
Integration with provider	Typically deployed by the ISP/ operator itself	Demanding data input from operators or lawful interception (LI) modules.

1.2.5. OSINT/WEBINT

Open-source intelligence (OSINT) tools monitor content across social media platforms and all kinds of websites. This includes images, text, video, and audio over time—enabling, in turn, biometric identification, detection of objects, locations, sentiment, profiles, connections, and much more. These tools can also be integrated with other WEBINT systems, designed to supplement data from other databases—private, police, social, or judicial in nature—as well as with information available on public websites and in the deep or dark web[63].

In addition, these intelligence tools can be used to generate patterns, identify behavior deemed suspicious, and monitor interactions on social media. Predictive features can also be layered into these tools. Among the best-known players in this market are Palantir Technologies (through its Foundry platform), Geofeedia (now part of Verint), and Social Sentinel (US). Some

63 Trottier, Daniel. *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Routledge, 2016. DOI

companies offer "government" editions alongside corporate products—called "enterprise intelligence"—with enhanced capabilities that, in principle, are not offered to the general public[64].

The neologism "cyber-patrolling", often misused to describe the deployment of OSINT tools, dangerously equates law enforcement activity aimed at crime prevention in the public sphere with intelligence work. In that sense, it operates as a biased and misleading euphemism with social and political implications, since social media platforms do not constitute the "public sphere". They are instead private and governed by specific contractual terms of service. For example, sharing images on social media does not mean consenting to having them processed using biometric identification tools.

In recent years, the use of commercial OSINT tools by law enforcement and security agencies has faced repeated scrutiny for the monitoring of social and political activities. For example:

- In the United States, Dataminr, which uses real-time analysis of X (formerly Twitter) and other open networks, has been flagged for providing information to police during the 2020 Black Lives Matter protests, despite restrictions imposed by the platforms themselves on the use of data for surveillance purposes[65].
- Similarly, Voyager Labs, a company specializing in behavioral analytics and AI-powered social media mining, was sued by Meta for automatically accessing and collecting information from millions of profiles in order to offer monitoring services to government agencies[66].
- Also in the United States, a third controversial case involved the Social Sentinel system. Initially deployed by at least 39 U.S. universities to monitor social media posts in order to detect potential threats or risky behavior, it was revealed by journalistic investigations to have been used, in several instances, to monitor student protests and political activities, raising criticism against its lack of transparency and its impact on freedom of expression[67].

In 2022, CELE (Center for the Study of Freedom of Expression and Access to Information in Latin America) coordinated a comparative study in Argentina, Brazil, Colombia, Mexico, and Uruguay on state use of OSINT tools for surveillance as part of their domestic security policies. According to the report, documented cases show that states conducted open-source–based intelligence activities between 2017 and 2020, and that they likely continued to do so thereafter[68].

---

64 Brennan Center for Justice, "Third-Party Vendors of Social Media Monitoring Tools for Law Enforcement Agencies." December 15, 2021. URL

65 Sam Biddle, *"Dataminr Fed Police Real-Time Tweets from BLM Protests."* The Intercept, July 9, 2020. URL

66 Sam Levin and Johana Bhuiyan. "Meta Alleges Surveillance Firm Collected Data on 600,000 Users via Fake Accounts." *The Guardian*, January 12, 2023. URL

67 Ari Sen and Derêka Bennett, "Tracked: How Colleges Use AI to Monitor Student Protests, *The Dallas Morning News*, September 20, 2022. URL

68 CELE, *Intelligence based on open sources (OSINT) and human rights in Latin America: a comparative study in Argentina, Brazil, Colombia, Mexico and Uruguay.* CELE, 2023. URL

As these reports highlight, the use of such tools is contentious for reasons not yet fully examined. Not only may they potentially violate the terms and conditions accepted by users; the systematic collection, storage, and large-scale analysis of data may also infringe fundamental rights[69]. By enabling the creation of databases that profile citizens, activists, or journalists on ideological or political grounds, such tools may restrict freedom of expression and association and foster risks of selective surveillance and self-censorship (commonly referred to as the chilling effect)[70]. In light of several relevant cases, the Inter-American Commission on Human Rights has expressed concern about the systematic and insufficiently transparent use of this kind of continuous monitoring of digital spaces and the profiling of individuals[71].

---

69 Ucciferri, Leandro. *Seguidores que no vemos – Una primera aproximación al uso estatal del Open-source intelligence (OSINT) y Social media intelligence* (SOCMINT). ADC, 2018. URL

70 Jon Penney, "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study", *Internet Policy Review*, 2017. URL

71 Díaz Charquero, Patricia, and Jorge Gemetto. *Ciberpatrullaje: Los Límites Borrosos de La Vigilancia Policial En Uruguay.* Datysoc, 2022. URL // Schatzky, Agustina Del Campo, Morena, and Mmdg. "Cyber Patrol or Intelligence?" CELE, October 8, 2020. URL

Box 8: Some worldwide OSINT/WEBINT tools

Tool / Manufacturer	Use by law enforcement	Notes / sources
Babel Street / BabelX (US)	Multi-platform social media monitoring, sentiment analysis, and cross-lingual searches.	"Third-Party Vendors of Social Media Monitoring Tools for Law Enforcement". *URL*
Digital Stakeout (US)	Social media and dark web monitoring, user-defined alerts, and visualization of public data.	Brennan Center. *URL*
Skopenow (US)	Automated extraction of social media data, and alerts regarding changes to or activity on public profiles.	Brennan Center. *URL*
Cobwebs / Tangles (Cobwebs Technologies, Israel)	Web intelligence (WEBINT/ OSINT) platform conducting real-time monitoring and network analysis of social interactions and connections.	Brennan Center; official website Cobwebs. *URL*
Cognyte (Israel / US)	A situational intelligence and social network analysis platform—successor to Verint Intelligence Solutions—providing solutions to law enforcement and defense agencies.	Cognyte corporate information. *URL*
i2 Analyst's Notebook (i2 Group) (UK)	Criminal activity and connections intelligence visual analytics tool, used by law enforcement and military forces in more than 150 countries. It functions as an analytics engine connected to other OSINT sources.	IBM Security / i2 Limited. *URL*
Palantir / Palantir Technologies (US)	Analytics platform for large volumes of data (Foundry, Gotham), used by defense, law enforcement, and intelligence agencies.	Public information and reports. *URL*

Tool / Manufacturer	Use by law enforcement	Notes / sources
PenLink (US)	Platform for the interception and analysis of communications and OSINT data to support criminal investigations.	Official site: *URL*
Social Links (Ukraine / global)	OSINT platform for law enforcement, integration with Maltego and search capabilities across social media, the dark web, and open sources.	Official site: *URL*
Voyager Labs / Voyager Analytics (Israel)	AI-based social media analytics platform for police intelligence, identification of threats and social connections	NYT report and corporate site. *URL*
ShadowDragon (SocialNet, OIMonitor) (US)	Digital surveillance of social media, pattern detection, matching of handles, and automated alerts.	Wikipedia. *URL*
Dataminr (First Alert) (US)	Real-time early event detection, with alerts triggered by social media posts and crisis signals.	Criminal Legal News. *URL*
Pagefreezer (Canada/US)	Monitoring and archiving of digital content (web, social media, messaging) for state agencies.	Official site: *URL*
Kaseware (US)	Criminal investigation and analysis platform with OSINT modules and case management.	Official site: *URL*

Box 9: Intelligence categories

Category	Definition	Tool examples
SIGINT *(Signals Intelligence)*	Intelligence derived from the collection and analysis of electronic signals — communications and non-communicative signals (such as radar and telemetry).	Jammers / inhibitors; IMSI Catchers; exploitation of SS7 and Diameter telephony protocols; etc.
COMINT *(Communications Intelligence)*	SIGINT subcategory focused on intercepting and analyzing communications.	Telephone wiretapping systems, VoIP interception tools, and satellite communications monitoring.
OSINT *(Open Source Intelligence)*	Collection and analysis of information from open sources: news media, publications, social media platforms, and public databases. Sometimes SOCMINT (Social Media Intelligence) is set apart, focusing specifically on social media.	Maltego, OSINT Framework, Google Dorks, TheHarvester, Palantir Foundry.
WEBINT *(Web Intelligence)*	Focused on the web (including the deep and dark web). It enables the collection and analysis of online digital data, not limited to open sources.	Social Sentinel, Echosec, Geofeedia (Verint), DarkOwl, SpiderFoot.

Box 10: Technologies and companies

Spyware
NSO Group (Israel)
Paragon Solutions (Israel)
Saito Tech (formerly Candiru) (Israel)
Intellexa Consortium
RCS Labs (Italy)
Memento Labs (formerly Hacking Team) (Italy)
Quadream (Israel)
MerlinX Ltd (Israel)
Gamma Group (Germany / UK)
Interionet (Israel)
Mollitiam (Spain)
Movia (Italy)
Negg Group (Italy)

SS7-Diameter Explotation
Ability (Israel)
PAT Systems (US)
Rayzone (Israel)
Telesoft (UK)
Tykelab (Italy)
Elaman (Germany)
Verint (US.-Israel)
Cognyte (Israel)
Circles Technologies (related to NSO Group) (Israel)

IMSI catchers
L3 Harris Technologies (US)
Septier (Israel)
BAE Systems (UK)
Cobham (UK)
Cognyte (Israel)
Jacobs (US)
Verint (US- Israel)
Rohde & Schwarz (Germany)

Lawful Interception (LI)
Innova (Italy)
Narus / NarusInsight (US)
Trovicor (Germany)
Utimaco (Germany-US)
SS8 Networks (US)
Procera Networks (US)
Group 2000 (Netherlands)
AQSACOM (France)
Squire Technologies (UK)
Subsentio (US)
VOCAL Technologies (US)
Thales (France)
BAE Systems (UK)
Septier (Israel)

DPI
AppLogic Networks (formerly Sandvine) (Canada)
Huawei Technologies (China)
Cisco Systems (US)
Qosmos (parte de Enea)
NICE Systems (Israel-US)
Geedge Networks (China)
Blue Coat Systems (US)
VAS Experts (Russia)
ZTE (China)
A10 Networks (US)
Narus (US)
Rohde & Schwarzl (Germany)
Allot (Israel)
Palo Alto Networks (US)
Check Point (Israel)
Hewlett Packard Enterprise (US)
IBM (US)

OSINT
Babel Street / BabelX (US)
Digital Stakeout (US)
Skopenow (US
Cobwebs Technologies / Tangles (Israel)
Cognyte (Israel)
i2 Analyst's Notebook / i2 Group
Palantir (US)
PenLink (US)
Social Links (US)
Voyager Labs / Voyager Analytics (UK -Israel)
Clearview AI (US)

1.2.6. Extraction tools and forensic analysis

These are digital forensics tools designed to extract and analyze data from mobile devices and other electronic media. Many of them incorporate constantly developing exploits that force access to a device. Platforms specialized in mobile phones—such as UFED (Universal Forensic Extraction Device) by Cellebrite, XRY by MSAB, or Magnet AXIOM—enable full file system extractions, the recovery of deleted data, and, in certain cases, privileged access to locked devices, and associated backups and cloud services.

Alongside these solutions, there are general-purpose forensic suites such as EnCase and Mobile Investigator (OpenText), FTK (Exterro / AccessData), as well as FRED workstations (Digital Intelligence). These platforms combine data acquisition capabilities with advanced post-collection analysis of digital evidence. Their use by security forces is typically governed by applicable procedural legislation and, in principle, requires a specific legal basis, which may include warrants, the device owner's consent, or other measures provided by law.

Although no abuse has so far been identified in South America, the risks involved remain the subject of debate. Various international reports note that the above companies market their products in countries where human rights violations have been reported[72]. In practice, in the United States, extraction is often carried out without a warrant[73]. In Brazil, indiscriminate use has been documented[74]. In Serbia, there are recorded cases of these tools being used to unlock devices in order to install spyware and thereby enable ongoing surveillance[75].

For this reason, the debates around them are extensive. Commercial forensic tools are generally not subject to independent audits and do not allow for the establishment of standards of reliability, transparency, and admissibility. Law enforcement and security agencies often place their trust in these products with little evidence to support it. It can also be argued that the use of exploits against unpatched vulnerabilities may produce uncontrolled changes to the device, undermining the chain of custody of information and, consequently, the validity of digital evidence presented in court[76]. Moreover, it has been shown that the tools themselves can contain security vulnerabilities that may be ex-

---

72 Pisanu, Gaspar, and Verónica Arroyo. *Surveillance Tech in Latin America: Made Abroad, Deployed at Home.* 2021. URL

73 Koepke, Logan, Emma Weil, Urmila Janardan, Tinuola Dada, and Harlan Yu. *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones. Upturn,* 2020. URL

74 Ramiro, André, Amaral, Pedro, Canto, Mariana, and Pereira, Marcos César. *Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil.* Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), 2022. URL

75 Amnesty Tech. *A Digital Prison: Surveillance and the Suppression of Civil Society in Serbia.* Amnesty International, 2024. URL

76 P. Dimpe, "Impact of Using Unreliable Digital Forensic Tools," *Proceedings of the World Congress on Engineering and Computer Science* (San Francisco: IAENG, 2017), 118–125, URL

ploited through data stored on the phone—potentially altering the evidence or disrupting the proper functioning of the forensic tools[77].

As the Serbian case cited above illustrates, the fact that these tools can operate without leaving traces on the device further increases the risk of illicit use for illegal purposes. And, as documented, these tools can readily become instruments of repression.

1.2.7. Video-surveillance and biometrics

Compared with other technologies, the rapid advance of video-surveillance systems and biometric technologies across the region has been subject to broader analysis and public debate, resulting in greater awareness of the companies involved[78]. These include IDEMIA (formerly Morpho), Crossmatch, AnyVision, Hikvision, Dahua, Huawei, ZTE, NEC, and NtechLab[79]. Their deployment, however, is harder to track. Because these products are also marketed through private companies, commercial offers and import records do not always accurately reflect their use by state bodies; and even the permits required for installation remain the subject of ongoing debate.

77 There are documented cases of vulnerabilities prone to exploitation in UFED and EnCase. URL

78 Díaz Charquero, Patricia, *Fuera de control: Ampliación del informe y resultados del litigio sobre uso policial del reconocimiento facial automatizado en Uruguay.* Montevideo: Datysoc, 2022. URL // Maguire, Méabh, and Ángela Alarcón. *Remote Biometric Surveillance in Latin America Are Companies Respecting Human Rights?* Access Now, 2023. URL

79 Asociación por los Derechos Civiles (ADC). *Tecnologías de Vigilancia En Argentina.* ADC, 2021.

Scope of the report discussed — convergence of capabilities

The deployment of forensic extraction devices, biometrics, and video-surveillance technologies has been examined in greater depth in recent studies and reports on the region[80]. As a result, this report does not focus on them. Rather, it references them only in passing, without adding new information or providing a detailed analysis.

Also excluded from this categorization are tools used for targeted or tactical surveillance operations (such as microphones, cameras, and similar devices), as well as countermeasure systems (including signal jammers and equipment designed to detect and neutralize various types of surveillance devices).

Specifically, this report focuses on interception and monitoring products intended for security forces and intelligence agencies: (1) intrusion software, or spyware; (2) signals interception tools (SIGINT), with particular attention to IMSI catchers and technologies exploiting SS7 and Diameter telephony protocols; (3) lawful interception and network intelligence related to IP communications; (4) network monitoring; and (5) open-source intelligence (OSINT) tools.

While an increasing number of platforms now integrate multiple capabilities, and many surveillance tools can generally fall within more than one of the proposed categories, this classification remains useful for understanding the different types of solutions available from a technical standpoint.

A prominent example is Intellexa's Nova Suite, whose functionalities reportedly include infiltration exploits, signals intelligence (SIGINT) capabilities, open-source intelligence (OSINT) analysis, and active geolocation (through SS7/Diameter)[81]. In practice, these tools are often used in combination to achieve the infection of a targeted device, in a process that involves prior stages of reconnaissance and compromise (through OSINT and WEBINT technologies) before the actual infection. Thus, companies such as Cobwebs Technologies or Cognyte reportedly provide tools necessary to install Cytrox spyware. At the same time, some companies, including Black Cube, Bluehack CI, and Belltrox, offer bundled solutions that integrate multiple capabilities into a single suite[82].

Overall, the mapping conducted for this report suggests that many contemporary surveillance capabilities are less focused on direct access to the content of communications and more focused on a systematic analysis of metadata, traffic patterns, and network behavior. Techniques such as DPI, fingerprinting, and anomaly detection can be used to infer connections, routines, and usage profiles when data are encrypted. This shifts the focus of surveillance away from content and toward the "how, when, and with whom" of communications, significantly expanding the population reached, while lowering the legal and technical barriers to deployment.

For this reason, even though OSINT/WEBINT is often presented as a less intru-

---

80 Pisanu, Gaspar, and Verónica Arroyo. *Surveillance Tech in Latin America: Made Abroad,* Deployed at Home. 2021. URL

81 Amnesty Tech. "Predator Files: Technical Deep-Dive into Intellexa Alliance's Surveillance Products." *Amnesty International Security Lab*, October 6, 2023. URL

82 Dvilyanski, Mike, David Agranovich, and Nathaniel Gleicher. *Threat Report on the Surveillance-for-Hire Industry*. Meta, 2021. URL

sive form of collection, the table below highlights its strategic role as a form of amplification of the rest of the techniques. Automated scraping, the use of API aggregators, and the processing of large volumes of data make it possible to turn public or semi-public information into inputs for profiling, segmentation, and behavioral prediction systems. When integrated with biometrics or network intelligence, OSINT ceases to be merely an auxiliary resource and instead becomes a central component of scalable surveillance architectures with a relatively low political cost.

Therefore, the cross-cutting concern is not about each technology in isolation; it is rather the potential for integration. The table below illustrates how OSINT, network interception, spyware, forensic analysis, and biometrics can combine into coherent systems that enable ongoing, targeted, or mass surveillance. Their convergence transforms single tools into broad infrastructures, where the boundaries between case-specific monitoring and population-level intelligence become increasingly blurred. The risk, therefore, is systemic: the consolidation of open-ended surveillance systems with continuous expansion capabilities and limited accountability.

Table 1: Digital surveillance tools: categories

Category	Spyware	SIGINT	Network intelligence interception	Network monitoring
Access type	Remote device intrusion	Interception of physical radio-frequency signals	Digital packet analysis on IP networks (TCP/IP, HTTP, VoIP, etc.)	Network traffic capture
Location of the attack	Device (mobile/PC)	Signals, telephony network infrastructure (core, antennas, SS7 gateways, etc.)	Network core, backbone, ISP	Network core, backbone, ISP
Techniques	Exploitation of vulnerabilities (0-day, 1-day, N-day), phishing, physical installation (stalkerware), remote management (C2)	Capture and analysis of radio-frequency signals, manipulation of GSM / SS7 / LTE / Diameter protocols.	Metadata analysis, duplication of IP traffic, Fingerprinting, Sniffing, Deep Packet Inspection (DPI), mirror ports, SSL/TLS interception, protocol reconstruction, packet injection, etc.	Deep Packet Inspection (DPI), pattern analysis, anomaly detection, fingerprinting, SSL/TLS interception
Interaction with target	Concealed, targeted	Concealed, targeted (in the case of SS7 protocol exploitation), partially targeted (in the case of IMSI catchers).	Concealed, targeted	Passive, non-targeted (not user-specific)
Required infrastructure	Servers, vulnerabilities, exploits, deployment or installation techniques, and anonymization nodes of operators.	Rogue antennas, access to mobile infrastructure, and specialized frequency analysis equipment.	Access to ISP, routers, and monitoring servers	Specialized network equipment and monitoring servers
Purpose	Device takeover, targeted espionage, remote control, and access to the camera and microphone	Identifying and tracking devices, tapping calls, and locating users.	Intercepting traffic, analyzing patterns, and reading or reconstructing communications	Observing usage patterns, detecting anomalies, and filtering traffic.
Type of collected data	Files, messages, location data, camera feeds, and microphone recordings.	Calls, SMS messages, antenna-based positions, metadata	IP traffic, protocols, domains, patterns.	IPs, protocols, domains, patterns, traffic
Companies with products deployed in South America	Pegasus (NSO Group), Galileo (Hacking Team), Invisible Man / Night Crawler (Mollitiam), FinFisher.	IMSI catchers, SS7 signaling attacks, EGO (Innova), Hydra (Cy4gate), ULIS (Verint), NiceTrack, Palantir platforms, SkyLock / Engage GI2 (Verint)	Innova S.p.A. (Italy), Pat Systems (US), Cy4gate (Italy), Rohde & Schwarz (Germany)	Blue Coat, Sandvine, Huawei eSight, Network Critical Limited
Argentina	Some probability of: Night Crawler / Invisible Man (Mollitiam), Epeius (Cy4gate), RCS (Hacking Team), Pegasus (NSO group).	As a minimum: PICSIX (Israel), TITAN ([US]), Kavit (Israel), Pat Systems (US), Cy4gate (Italy), Rohde & Schwarz (Germany)	Pat Systems (US), Cy4gate (Italy), Rohde & Schwarz (Germany), Ericsson (Sweden), Nokia (Finland), Innova S.p.A. (Italy)	Blue Coat (US), Sandvine (Canada), Ericsson (Sweden), Nokia (Finland), Innova S.p.A. (Italy
Chile	Pegasus (NSO, Israel), Phantom / Remote control System - Galileo (Hacking Team, Italy)	Almenta Group (US), NSO / Circles (Israel), ELT Group / Cy4gate (Italy), RCS Labs (Italy), Pat Systems (US) Rohde & Schwarz (Germany)	Innova S.p.A. (Italy) Cognyte (Israel) Pat Systems (US) ELT Group / Cy4gate (Italy)	Blue Coat (US) Sandvine (Canada) CISCO (US) Palo Alto Networks (US)
Uruguay	Little probability of Galileo by Hacking Team (Italy) or Pegasus by NSO (Israel).	Innova S.p.A. (Italy).	Teleimpresores SA (Uruguay), Digitro Tecnologia Ltda. (Brazil), Innova S.p.A. (Italy), Nokia (Finland), Huawei (China)	Nokia (Finland), Huawei (China)

Category	OSINT / WEBINT	Forensic extraction	Video-surveillance and biometrics
Access type	Digital content / automated processing of data	Physical access to device	Capture of images and biometric data in physical environments
Location of the attack	Web platforms, social media / public or semi-private databases	Physical device, digital platforms associated with the device	Public spaces, borders, buildings
Techniques	*Scraping, public APIs, automated crawlers, Natural Language Processing (NLP), text mining and social media analysis, biometrics on pictures, object and place identification*	Physical access, memory cloning, password cracking, RAM analysis, JTAG exploits for hardware and software	Facial recognition, body-temperature detection, automatic matching with databases
Interaction with target	Indirect and automated, could be targeted or mass	Direct, physical	Concealed from view, automated
Required infrastructure	Crawlers, cloud platforms, scrapers, APIs, and servers for analysis, storage, and processing.	Physical workstations, proprietary software such as UFED or Magnet AXIOM, controlled physical access, expert personnel, and forensic analysis hardware and software.	Cameras, biometric sensors, and facial and biometric databases
Purpose	Obtaining publicly available information to profile individuals, groups, and behaviors.	Extracting data from seized devices	Physically tracking and monitoring individuals through their biometric traits.
Type of collected data	Opinions, profiles, posts, risk scores, predictive indicators, social segments, affiliations.	Files, application messages, passwords, call histories, cloud data	Faces, fingerprints, license plates, trajectories, biometrics
Companies with products deployed in South America	D-SINT (Cy4gate), i2 Limited (IBM), Huawei, Babel X, Voyager Labs, Maltego, Palantir Gotham	UFED (Cellebrite), GrayKey, Oxygen, among others	Clearview AI, Hikvision, Dahua, Visionlabs, AnyVision
Argentina	As a minimum: Cy4gate (Italy) I2 Technologies / IBM (US) Minerva IA (Spain) Rafael - Verint / Cognyte (Israel) IPS Intelligence S.p.A. (Italy)	Cellebrite (Israel) Digital Intelligence (US) EnCase Forensic (US) MOBILedit Forensic (Czech Republic) MSAB (Sweden) Oxygen Forensics (US) Silicon Forensics (US)	3M Electronics Monitoring Inc. (US), AnyVision / Oosto (Israel), BGH Tech, Partner (Argentina), Clearview AI (US) Haivision (Canada), Hikvision and Dahua (China), Huawei and ZTE (China) IDEMIA (former Morpho) (France), Incode (US), Jumio (US), NEC (Japan), NtechLab (Russia), Veridas (Spain), Speech Technology Center (STC Group) / Speech Pro (Russia)
Chile	As a minimum: Cognyte (Israel) ELT Group / Cy4gate (Italy) Cellebrite	Cellebrite (Israel) Toka Group (Mexico) Oxygen (US)	Clearview AI (US) Verint / Cognyte / Intellicene (Israel) NEC (Japan), Dahua Technology (China) Luxriot / VisionLabs (Russia), AnyVision / Oosto (Israel), Hikvision (China), Dahua (China), Huawei (China), ZTE (China), Veridas (Spain), Jumio (US), IDEMIA / Morpho (France).
Uruguay	Innova S.p.A. (Italy) Digitro Tecnologia Ltda (Brazil) Analytic Technologies (US) Social Links (Ukraine)	Cellebrite (Israel) Magnet AXIOM (Canada) Belkasoft Evidence Center X (US)	Hikvision (China), Dahua (China) Huawei (China), ZTE (China), IDEMIA(France), NEC (Japan), Clearview AI (US), M Electronics Monitoring Inc. (US).

1.3. Regional context: Mexico, Brazil and Colombia in the spotlight

The Southern Cone countries do not usually appear among those with the highest levels of information control. Those countries are not listed in any of various annual reports as having internet shutdowns, systematic content censorship, or banned applications[83]. That being said, the situation is complicated.

Within a global context in which the United States protects its own citizens through specific laws and the European Union has managed to establish the General Data Protection Regulation (GDPR), citizens of South America often lack strong legal safeguards against large, medium, and small companies that collect and sell data.

It is also the case that, in those countries, compliance with international standards governing communications and lawful interception technical standards—such as those developed by the European Telecommunications Standards Institute (ETSI) or the American National Standards Institute (ANSI) in the United States—is not always mandatory. Although surveillance products often claim adherence to such standards based on their country of origin, these certifications do not necessarily apply when the technologies are deployed outside their jurisdictions of origin.

A general feature observed across the region is that surveillance technologies are often procured in the absence of specific legislation. As a result, it becomes necessary to refer to international treaties or broader legal frameworks in order to begin determining what the legal limits might be. Many recent reports therefore have attempted to identify which regulations would apply depending on the country in question[84]. This situation is compounded by the existence of special provisions that allow the purchase of intelligence technology through discretionary funds or under import agreements that bypass public procurement processes and import records. There are even reports of purchases made in cash in order to avoid leaving any trail of the transaction[85].

In general, law enforcement and security agencies operate within a largely unregulated procurement environment. Abuses go undocumented. This prevents political, social, and legal debates about them from receiving adequate attention.

The regional landscape is indeed complex. Beyond the Southern Cone, there is a troubling trend toward the expansion of surveillance technologies and the adoption of increasingly repressive security measures. The most notable examples in the region are Mexico, Colombia, and Brazil.

---

83 For example, see indexes by Freedom House for Argentina, Uruguay and Chile in 2024 and 2025. Freedom House. "Country Profile." 2025 URL // Internet Society, "Internet Society - Pulse". URL // Access Now. "Access Now." URL

84 García Muñoz, Luis Fernando, Ana Gaitán Uribe, José Flores Sosa, Santiago Narváez Herrasti and Milán Trnka Osorio. El Estado de la vigilancia Red de Defensa de los Derechos Digitales (R3D), 2025. URL

85 Garay, Vladimir, and Zack Rogoff. *Tecnología y Vigilancia En La Operación Huracán: Una Revisión Del Trabajo Periodístico Realizado En Torno al Caso* (2018). Derechos Digitales, 2018. URL

Through public procurement records across various municipal governments in Mexico, it has been possible to trace the staggering sums of public funds that different Mexican states have allocated to the acquisition of these technologies. Reports continue to accumulate[86]. In addition to high-profile spyware, such as Pegasus, confirmed purchases include FinFisher (United Kingdom–Germany), Hacking Team (Italy), and Quadream (Israel / Cyprus). There are also documented acquisitions of interception and geolocation equipment exploiting the SS7/ Diameter protocol, supplied by Israeli companies, such as Ability, Rayzone, and Circles, as well as web traffic monitoring systems such as Citadel Group (Russia) and Innova's EGO system (Italy). Reports further show the purchase of IMSI catchers from companies including Elaman (Germany), L3Harris (United States), and Kavit (Israel). Regarding OSINT systems, a recent report documents network monitoring carried out through a preventive "Multi-Source System"[87].

Colombia is an equally compelling case[88]. The country has become one of the leading purchasers of intrusive software, including products from Cytrox / Intellexa, Hacking Team (Italy), NSO Group (Israel), and Mollitiam (Spain)[89]. It has also acquired interception and geolocation tools from Ability (Israel); signal jammers from Allen Vanguard; and IMSI catchers from Comstrac (United Kingdom), Phantom Technologies (Israel), and L3Harris Technologies (United States). Monitoring systems from Network Critical Limited (United Kingdom), PKI Electronic Intelligence (Germany), Rohde & Schwarz (Germany), and NICE Systems (Israel/ United States) have also been acquired, along with web and open-source intelligence tools from US company Palantir[90]. Furthermore, Colombia—alongside Ecuador and Paraguay—has been listed among the countries that acquired advanced surveillance suites from Septier Communication, Verint, and VASTech including IMSI catchers and OSINT profiling capabilities[91]. In fact, the National Police (DIPOL) opened a procurement procedure to acquire an AI-powered cyber-intelligence system to monitor social media and messaging platforms[92].

Similarly, in Brazil, the use of a wide array of spyware has been documented. Tools developed by Hacking Team, NSO Group, Candiru, Cytrox, FinFisher, and Cognyte, alongside less sophisticated forms of spyware such as Packrat and

---

86 Rodríguez, Aitana, Mariana Recamier, Dalia Souza, and Darwin Franco. "Vigilad@s: Jalisco invierte millones en tecnologías para espiar y monitorear." *Zona Docs*, 2024. URL

87 Article 19. *Informe sobre prácticas OSINT en México*. 2023. URL

88 Fundación Karisma and TEDIC. *Uso de herramientas digitales y amenazas de seguridad digital en personas defensoras de derechos humanos en Paraguay y Colombia. Karisma- TEDIC,* 2024. URL

89 Suárez, Astrid. "EEUU admite que financió la compra del software espía Pegasus en Colombia." World News. *AP News*, November 8, 2024. URL

90 Privacy International. *The Global Surveillance Industry.* 2016. URL

91 Fundación Karisma and TEDIC. *Uso de herramientas digitales y amenazas de seguridad digital en personas defensoras de derechos humanos en Paraguay y Colombia. Karisma- TEDIC,* 2024. URL

92 Fajardo, Carolina Pardo, Daniel. "Colombia: Police Plans to Procure Cyber Intelligence System to Monitor Social Media and Instant Messaging Platforms." *Global Compliance News*, September 19, 2020. URL

FoxSpy, have been deployed in various documented instances.[93] The presence of IMSI catchers from Kavit (Israel), Russian monitoring systems from Citadel Group, and—much like in the case of Colombia—a diverse set of interception tools supplied by Comstrac (United Kingdom) has also been identified.[94]

In this context, it is worth asking how many of the above tools have been documented for the Southern Cone countries.

93 InterSecLabm Unveiling Celular 007: *An In-Depth Analysis of Brazilian Stalkerware and Strategies for Collective Protection*. 2025. URL

94 Ramiro, André, Amaral, Pedro, Canto, Mariana, and Pereira, Marcos César. *Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil*. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), 2022. URL

2. Argentina

2.1. Context

In 2011, Argentina launched an ambitious biometric database known as SIBIOS (short for "Federal Security Biometric Identification System", in Spanish). That same year, the Office of the Chief of Cabinet of Ministers signed a framework agreement with US company Crossmatch Technologies, which specializes in biometric systems for law enforcement and security agencies[95]. Among other things, the agreement enabled the Argentine state to procure fingerprint readers—scanners to capture and verify identities—for law enforcement, border control, and identity document processing services.

Six years later, WikiLeaks revealed that the CIA's Office of Technical Services (OTS) was operating a global biometric collection system provided to liaison services around the world, and the CIA expected the voluntary sharing of captured data. The system's core components were based on products made by Crossmatch. When the voluntary sharing was deemed insufficient, the CIA used a covert tool known as ExpressLane, installed under the cover of a software update, enabling the clandestine extraction of biometric databases from those systems[96]. The existence of a framework agreement between Crossmatch and the Argentine state allowed direct procurement of biometric equipment through a pre-approved catalogue, reducing timelines and administrative steps involved in ordinary bidding processes.[97] Despite the controversy surrounding the company in countries such as India, there is no record that the Argentine agreement may have been reviewed or subjected to a specific public investigation in light of these revelations.[98]

Since then, Argentina has been at the forefront of biometric identification. A series of legal actions brought by civil society organizations—such as Fundación Vía Libre, Asociación por los Derechos Civiles (ADC), CELS (which is part of the Centro de Estudios en Libertad de Expresión y Acceso a la Información, CELE), and Observatorio de Derecho Informático Argentino (ODIA)—have succeeded in suspending some of these systems in Buenos Aires. Their investigations have also made it possible to identify many of the companies involved in government surveillance contracts. From global technology firms to specialized surveillance vendors, this mix of actors points to a supplier network in which transparency

---

95 "Acuerdo Macro de Cooperación y colaboración entre la jefatura de gabinete y Crossmatch Technologies Inc." 2011. URL

96 Rachel Chitra, "WikiLeaks Hints at CIA Access to Aadhaar Data, Officials Deny It", *The Times of India*, August 26, 2017. URL

97 This adds to the fact that, the following year, Crossmatch was acquired by Francisco Partners fund, which later also acquired NSO Group and Blue Coatinto the fold—the latter being one of the companies behind deep packet inspection (DPI) systems used in Argentina as well as in many other countries—.

98 Kasli, Shelley. "How CIA Spies Access India's Biometric Aadhaar Database," *Voltaire Network*, August 25, 2017. URL

requirements remain contested and deployments often fall into a gray area between the public and private spheres.[99]

In 2014, in Germany, a parliamentary request for information revealed that the country had sold surveillance technologies to several countries in the region, including Argentina.[100] There was no mention in the official documents of the suppliers or the types of licenses approved for "interception systems" and "surveillance monitoring centers."[101] That was the full extent of the information. It has not been possible to determine which technologies were involved, nor which German companies had supplied them.

It is worth noting that, in 2014, Paraguay had recently acquired the German-made spyware FinFisher, while Argentina was seeking to legalize the use of such intrusion technologies and was also negotiating with NSO Group from Israel and Hacking Team from Italy.

In general, there are no indications that would support speculation regarding the acquisition of spyware, nor is it possible to determine with certainty what, specifically, may have been acquired from Germany. It is, however, possible to outline some hypotheses based on product availability and procurement patterns observed in other countries. At least three candidates stand out. ATIS and Utimaco produce Lawful Interception Management System platforms and have documented sales in Colombia, Mexico, Ecuador, and Paraguay. Another possibility is the German company Rohde & Schwarz (R&S). This company maintains a subsidiary in Buenos Aires and markets a wide range of products within the government security sector. Historically, R&S has been one of the leading global suppliers of lawful interception platforms and mobile telephony interception devices. It also offers signal interception tools ranging from IMSI catchers and direction finders (DF), to other frequency-scanning products and advanced packet-inspection network monitoring systems.[102]

In any case, a legal basis for using intrusion software in Argentina has gained a firm foothold since 2014 through the legal category of "remote surveillance of computer equipment"—first at a federal level and later in provincial codes replicating the formula. Argentina's Federal Criminal Procedural Code—enacted by Law 27,063 in 2014 and entered into force in 2019—includes a chapter on "Surveillance measures concerning communications and computer equipment".

---

99 These include 3M Electronic Monitoring (US/Israel), AnyVision/Oosto (Israel), BGH (with operations in several countries of Latin America), Clearview AI (US.), Haivision (US), Hikvision and Dahua (China), Huawei and ZTE (China), Incode (US), Jumio (US), NEC (Japan), NtechLab (Russia/Cyprus), Veridas (Spain) and IDEMIA/Morpho (Netherlands/France). Kiguel, Alejo. *Tecnologías de Vigilancia En Argentina.* ADC, 2021. URL // Pisanu, Gaspar, and Verónica Arroyo. *Surveillance Tech in Latin America: Made Abroad, Deployed at Home.* 2021. URL

100 TEDIC. "La adquisición y el abuso de tecnologías de vigilancia en América Latina - Al Sur." *TEDIC,* March 28, 2019. URL

101 *Jahrbuch Netzpolitik 2014: Von der Überwachungsgesamtrechnung bis zur Netzneutralität* (Berlin: Netzpolitik.org, 2014). URL

102 Currently, Rohde & Schwarz ipoque develops traffic analytical technologies that allow identifying and sorting out network communications, even encrypted ones, through automatic learning techniques. Its engines, such as R&S®PACE 2 and R&S®vPACE, provide real-time visualization of applications and users. This facilitates network management. "Ipoque | Encrypted Traffic Intelligence for Network Traffic Analysis.", 2025. URL, URL , URL

It specifically categorizes "inconspicuous use of software that enables or facilitates remote access to the contents of computers and electronic devices". This is subject to court authorization and is governed by the regime of "special investigative techniques". This provision creates a legal basis for the use of state malware in criminal investigations.[103]

In at least two cases, provincial jurisdictions sought to replicate these legal powers, presumably in order to acquire such software directly and use it in judicial proceedings. In the Autonomous City of Buenos Aires, a 2018 bill to reform the Criminal Procedural Code introduced a new article that reproduced the above wording almost to the letter. Through a public message and a series of technical positioning reports, Fundación Vía Libre, together with other civil society organizations, succeeded in halting the explicit incorporation of "remote surveillance of computer equipment" powers in the City of Buenos Aires. The coordinated pressure led the Legislature to remove the article from the final approved text.[104] On the other hand, the Criminal Procedure Code of Corrientes (Law 6518), enacted in 2019, constitutes another clear example, authorizing judges to approve remote access to the contents of computers, electronic devices, and information systems through software.[105]

Although there is an overall clear trend, an analysis by *Centro de Estudios Legales y Sociales* (CELS) identifies a turning point with the change of government in December 2015. First, Executive Decree 683/2018 amended the regulations of the National Defense Law expanding the role of the Armed Forces. This was followed by another executive order that formalized a new configuration for the intelligence agency. In response to freedom-of-information requests filed by CELS, both the executive branch of government and *Agencia Federal de Inteligencia* (AFI) stated that everything related to the national intelligence system had been reclassified as secret on security grounds.[106] Furthermore, the Argentine Federal Police also acquired new powers: Security Minister Patricia Bullrich formalized new "cyber-patrolling" tools to be used preemptively by the federal police in digital environments.[107]

---

103 Congreso de la Nación, Ley 27.063. *Código Procesal Penal Federal* (Official Gazette of the Republic of Argentina, December 10, 2014).

104 Access Now, *Amnistía Internacional Argentina, Asociación Civil por la Igualdad y la Justicia (ACIJ), Asociación por los Derechos Civiles (ADC), Asociación Pensamiento Penal Buenos Aires chapter (APP), Centro de Estudios Legales y Sociales (CELS), Centro de Estudios en Libertad de Expresión y Acceso a la información (CELE), Colectivo para la Diversidad (COPADI), Fundación Vía Libre, Instituto de Estudios Comparados en Ciencias Penales y Sociales (INECIP), Poder Ciudadano,* "La Legislatura porteña debate una reforma penal que habilita la vigilancia y vulnera la intimidad personal," joint press release of organizations, September 28, 2018. URL

105 Province of Corrientes, Código Procesal Penal de la Provincia de Corrientes (Law 6518/2019), art. 217, "Vigilancia remota sobre equipos informáticos", text available in the Argentine System of Legal Information—*Sistema Argentino de Información Jurídica (SAIJ)*—.

106 Litvachky, Paula, Margarita Trovato, Tomás Griffa, et al. "El secreto. La seguridad nacional como coartada para un Estado sin controles." In *Derechos humanos en la Argentina: Informe 2019,* CELS. 2019. URL

107 "Se relanzó la Policía Federal con su nueva función de 'ciberpatrullaje'." *Clarín*, April 18, 2017. URL

Against this backdrop, in November 2018, the Ministry of Defense signed a US$5.2 million agreement with Israel for the provision of defense and cybersecurity services, on the eve of the G20 summit in Buenos Aires. The contract included the acquisition of equipment from Rafael Advanced Defense Systems Ltd., a military technology company that also sells solutions to the private sector and that frequently operates as an intermediary for other Israeli companies supplying SIGINT, COMINT, and OSINT capabilities, such as Verint or Elbit. [108]

The most plausible acquisition scenarios point to: (i) A SOC (Security Operations Center) and CSIRT/CERT (Computer Security Incident Response Team) platform—i.e., centers where critical networks are monitored, attacks are detected, and incidents are handled in real time. Rafael markets this suite as a platform intended for defense ministries, armed forces, and national cybersecurity agencies.[109] These are standard (and officially unconfirmed) information-security capabilities that, in principle, are not directly related to the core subject of this report. (ii) Open-source (OSINT) analytics and fusion tools integrated into the above-mentioned SOC. Investigative reporting referred to "cyberdefense and cybersecurity software capable of collecting and analyzing social media and accessing public/private databases." This is consistent with Rafael modules as well as with typical Verint/Cognyte suites.[110] (iii) In parallel with the G20—though under different budget lines and agencies—counter-drone (C-UAS) physical protection through Rafael's Drone Dome. It was reportedly deployed in Buenos Aires during the G20 and during the 2018 Youth Olympic Games.[111]

By late 2023, the new government of Javier Milei reappointed Patricia Bullrich as Minister of Security, a position she had previously held from December 2015 to December 2019. Shortly after taking office, the administration introduced a new security protocol. It did so through an executive decree rather than by legislation. Alongside the above, a warning was issued that individuals would be identified through their transit card SUBE—the mandatory public transportation system—and state subsidies would be removed from those found to have participated in

---

108 Through Administrative Resolution 1658/2018 (04/10/2018) Argentina approved expenses for US $5,245,000 for a "CORE iSOC & CSIRT/CERT Cyber-defense" project signed, G2G, with Israel. Rafael was awarded with the purchase contract including installation and setting up of CSIRT/ISOC by mid-November 2018 (within days of G20) in the building known as Edificio Cóndor and in other sites (work included retrofitting, optic fiber, datacenter and deployment of hardware/software). "InfoLEG - Ministerio de Justicia y Derechos Humanos - Argentina." URL

109 Rafael Advanced Defense Systems, RAFAEL Cyber Defense Center (RCDC), 2021. URL, URL // Rafael Advanced Defense Systems, "National SOC – Security Operation Center". URL

110 "El Gobierno le pagará US$ 5 millones a Israel por un programa de ciberseguridad," *Convergencia*, Octubre 5, 2018. URL // Sergio G. Eissa and Ana Albarracín Keticoglu, "La Ciberdefensa en su laberinto. Cambio de rumbo en la concepción de ciberdefensa durante la gestión de Mauricio Macri (2015–2019)," *Revista Defensa Nacional Nº 5* (Universidad de la Defensa Nacional, 2020), 26–28 (detail of bidders Rafael, Verint, IAI/ELTA and Elbit; awarding to Rafael; installation timeline).

111 Rafael Advanced Defense Systems Ltd., *Drone Dome Counter-Unmanned Aerial System (C-UAS) Solution* – Technical Data Sheet (Haifa: Rafael Advanced Defense Systems, 2018).

social demonstrations.[112] In addition, the minister announced further regulatory measures and announced that data from the official "Mi Argentina" app would also be used to monitor participation in strikes and protests. Regardless of the above warnings, there is concrete evidence that SUBE travel records have been used to monitor individuals outside any ordinary course of judicial processes as would ordinarily be expected. To date, it remains unclear what specific technologies or data-processing capabilities would enable such practices, or whether these measures are technically or legally feasible.[113]

Six months later, *Secretaría de Inteligencia del Estado* (SIDE) started reporting directly to the executive branch of the national government and was granted a record allocation of discretionary funds. Through a presidential executive order, the *Agencia Federal de Ciberseguridad* (AFC) was also created within the institutional orbit of SIDE.[114] Assigning cybersecurity to the sphere of state intelligence constitutes a significant political decision with far-reaching institutional implications. At its most basic level, this decision places a veil of secrecy over the capabilities, procurement processes, and regulatory practices of an agency that could otherwise perform a range of functions. At the same time, it restricts public oversight and civil participation, transferring the design and implementation of cybersecurity policy to intelligence services—an institutional setting typically subject to secrecy regimes and one that remains unusual in the region to date.

This forms part of a broader reconfiguration of security and intelligence policy set in motion in December 2023, characterized by an explicit geopolitical alignment with the governments of the United States and Israel in international arenas, and by significant increases in discretionary funds earmarked for the technological modernization of the intelligence services through direct procurement. This alignment is also reflected in an intense schedule of international travel by the President and the Minister of Security. The central aim of those visits has reportedly been the negotiation of cooperation agreements and the acquisition of more sophisticated digital intelligence capabilities. Within this network of relationships, particular attention should be paid to intermediary firms such as OCP Tech and Tactic Global—IT and cybersecurity solutions companies associated with former intelligence officer Leonardo Scatturice. Under the current administration, Scatturice has not only provided services to the State; as reported in the press, he has also emerged as an intermediary linking Argentine authorities with U.S. security-sector actors and political networks. In the relationship with Israel, a central figure appears to be Mario Montoto, president of the Argentine–Israeli Chamber of

---

112 "El Gobierno argentino quitará ayudas sociales a quienes asistan a protestas." *SWI swissinfo.ch*, December 18, 2023. URL // Débora Rey, "Argentina: gobierno de Milei advierte con retirar ayudas sociales a los que salgan a manifestarse." –*Los Angeles Times en Español*, December 18, 2023. URL // Centenera, Mar. "Milei amenaza con quitar las ayudas sociales a quienes corten la calle para protestar." *El País*, December 19, 2023. URL

113 For a glimpse on Argentina's privacy laws, see: Rodríguez, Katitza, Verdiana Alimonti, Leandro Ucciferri, and Luiza Reheder. *Necessary & Proportionate*. EFF, 2020. URL

114 "Boletín Oficial República Argentina- Sistema de Inteligencia Nacional - Decreto 656/2024." URL

Commerce, a shareholder in Global View—a firm specializing in urban video-surveillance systems—and publisher of DEF magazine and DEF TV, outlets focused on defense, security, and intelligence.[115]

For this reason, in August 2024, Members of Congress Juan Manuel López and Victoria Borrego submitted a formal request for information to the Chief of the Cabinet of Ministers, expressing concern over the unusually sharp increase in discretionary funds allocated to SIDE. In that document, they warned that "recently enacted Emergency Executive Order (DNU) 656/2024, which increased SIDE's reserved funds by one hundred billion pesos, raises concerns regarding the ultimate destination of these resources, which may be used discretionarily, in secrecy, and without any form of public oversight or supervision."[116]

Box 11: Some resellers worth looking into

- **Global Interactive Group** (sometimes registered as Digital Global Interactive Ltd.) appears as a company incorporated in Tel Aviv–Jaffa, Israel. In trade-fair catalogues and programs such as ISS World Latin America, it is listed as a commercial partner of Verint, Elbit, and Rayzone Group—three Israeli companies that develop SIGINT/COMINT/OSINT tools.[117] In the 2015 the Hacking Team email leaks, their CEO, Alejandro "Alex" Lawson, appeared as the person who signed non-disclosure agreements with the Italian firm. Later, on January 19, 2018, another meeting was held in the auditorium of the Ministry of Security. On that occasion, Global Interactive Group (as Enforce One S.A.) presented Hacking Team's Galileo products, as well as another product called Iron Man from the "Spanish" company In nova (the latter is likely an error; it most probably refers to the well-known Italian company Innova S.p.A.). Attendees included representatives from Argentina's security and intelligence sectors, from Argentine Naval Prefecture (coast guard), and from Secretaría de Fronteras (international borders).[118] In Argentina and Mexico, Global Interactive Group markets tracking equipment, counterintelligence equipment, SIGINT tools, and the Spanish OSINT tool Minerva IA.

---

115 "Milei announced that the Memorandum with Israel will entail improvements in Defense. "After decades of looting the state and the hollowing-out of the Armed Forces, Argentina is plainly behind in military, weapons, and intelligence capabilities. Any country that commands respect needs these resources," Russo, Emiliano. "Netanyahu praised Milei as an 'example for the world,' and the President demanded the 'immediate' release of Hamas's hostages." Clarín, June 12, 2025 .URL

116 Juan Manuel López and Victoria Borrego, "Pedido de información sobre Pegasus - 4609-D-2024", 23/08/2024. *Trámite Parlamentario Nº 123*. URL

117 "ISS World Latin America Brochures / Program: Presentaciones de interceptación judicial y productos de vigilancia electrónica," ISS World Latin America, trade-fair catalogue, URL

118 Amongst the most prominent attendees were Martín Siracusa (Head of *Subsecretaría de Gestión Administrativa*), Alejandro Lawson (CEO of Global Interactive Group / Enforce One S.A.), Luis Antonio Barreto (PFA—federal police—), Luis Fernando Gallardo (*Secretaría de Fronteras*—borders—), Gonzalo Javier Alvarez (Global Interactive Group / Enforce One S.A.), Mario Gabriel Babijezuk (Intelligence Division of *Prefectura*—Coast Guard—), Rubén Sassone (*Secretaría de Fronteras)*, Jorge Nicolás Occhionero (Global Interactive Group), and Crispín Ezequiel Ortigoza (Intelligence Division of *Prefectura*). "Registro Único de Audiencias." URL

- **Assine S.A.**, an Argentine-owned company, operates as a regional representative and integrator for several European firms specializing in intelligence and defense technologies, with a focus on SIGINT, COMINT, and OSINT solutions for security organizations. On its corporate website, the company states that it represents Elettronica S.p.A. (ELT Group), an Italian leader in Electronic Warfare (EW) systems, with product lines including COMINT sensors and electromagnetic defense platforms for air, sea, and land forces.[119] It also acts as a representative of CY4GATE S.p.A., a company spun off from the same industrial group, dedicated to the development of lawful interception, network intelligence, and cyber-intelligence tools, including the QUIPO platform, designed for the analytical exploitation of open sources and communication networks.[120] In addition, Assine incorporates products from Divitech S.r.l., an Italian firm specializing in command-and-control centers and telematics solutions for public security and operations management.[121] In this way, the company positions itself as a commercial and logistical hub importing and distributing intelligence and defense software and equipment—primarily from Italy—to state forces and agencies in the Southern Cone, serving as a local interface for European technology providers in the field of national security.
- **TAMCE** (formerly High Security) is a company organized in Buenos Aires in 1998 by Nicolás Ruggiero and renamed in 2012. It has offices in Argentina and Mexico, and commercial presence in several Latin American countries and in the United States (Miami). The company imports and markets—primarily to law enforcement agencies—certain weapons, tactical surveillance equipment, and countermeasure systems. It offers restricted-sale SIGINT/COMINT solutions—for example, "PHOENIX Tactical Interceptor" designed for IMSI/IMEI capture—as well as jamming systems (including anti-drone and prison security applications) and forensic analysis tools (UFED and Oxygen). In the OSINT field, it provides cyber-intelligence platforms such as Medusa and Social Links (for monitoring social media, the open, deep and dark web, as well as CDR analysis), intended for criminal investigations. In 2014, the company reportedly attempted to act as an intermediary for spyware produced by both NSO Group and Hacking Team.
- **VEC SRL** is an Argentine company that currently operates as an importer, distributor, and integrator of communications equipment, radiofrequency systems, satellite links, and surveillance technologies for security and defense forces. In its "Digital Investigations" catalogue, it offers products from brands such as Cellebrite, Inseyets Ltd., Chainalysis, Smart Search, Pathfinder, Clearview AI, and Mollitiam Industries for digital forensics, online monitoring, and OSINT. The company also represents Mollitiam, with a suite of OSINT, COMINT, and electronic interception tools marketed exclusively for security agencies and law enforcement. In addition, it distributes Clearview AI, which specializes in facial recognition based on publicly available images, and Chainalysis, focused on blockchain analytics for tracing cryptocurrency

---

119 Elettronica S.p.A. (ELT Group), "Company Profile," accessed October 16, 2025, URL

120 CY4GATE S.p.A., "Law Enforcement & Security Agency Solutions," accessed October 16, 2025, URL

121 Divitech S.r.l., "Solutions," accessed October 16, 2025. URL

transactions. Presenting itself as the official distributor of Cellebrite in Argentina, VEC SRL has thus assembled a portfolio oriented toward providing technological support for digital investigations and intelligence activities in the public and judicial spheres.

- **HK Systems SRL** is an Argentine company organized in 2016 by Hugo Issel and Erik Kanter Snaider. It serves as the local representative of the Israeli firm PICSIX Ltd., which specializes in SIGINT technology. Its catalogue and public presentations indicate that it offers multiband IMSI catchers and SS7/Diameter-based geolocation systems, as well as mobile forensics and analysis solutions. In 2018, the company participated in a national public tender involving the above type of equipment. According to open sources from the security sector, it has reportedly supplied or showcased SIGINT systems for *Policía de Seguridad Aeroportuaria* (airport security police), *Policía Federal Argentina* (federal police), and Gendarmería Nacional Argentina (national borders), as well as for other provincial forces. Connections have been documented in catalogues and technical trade fairs, even though specific contracts are not publicly available due to their sensitive nature. Taken together, HK Systems operates as an Argentine integrator of Israeli-origin mobile phone interception and geolocation technology, with a client portfolio centered on federal security forces.

2.2. Demand / Solutions

2.2.1. *Spyware*

In 2015, the leak of internal emails from Italian spyware developer Hacking Team revealed that Argentina had been holding simultaneous negotiations with that firm and with NSO Group. Both the press and several civil society organizations began to voice concern about the implications of these reports.[122]

The emails suggested that three members of Hacking Team organized a visit to Buenos Aires in March 2012 in order to present its Remote Control System (RCS) to various law enforcement and security agencies. The meetings took place between March 19 and 23 at the Hilton Buenos Aires in Puerto Madero, with the attendance of representatives from the National Ministry of Security (specifically, *Dirección Nacional de Inteligencia Criminal*—national intelligence directorate—), the National Prosecution Office (specifically, *Unidad de Investigaciones Complejas* —complex investigations—), the Ministry of Justice and Security of the Province of Buenos Aires, and the national head of the Argentine Naval Prefecture.

The emails make clear that several local companies sought to act as intermediaries in the deal. While they do not indicate that any purchase was ultimately secured, they do mention the signing of two non-disclosure agreements intended to continue negotiations: one with the company Nullcode Team and another with Global Interactive Group. Nicolás Ruggiero, a representative of the Argentine–Mexican company Tamce, also sought to connect the firm with the intelligence agency that, during the

122 Ucciferri, Leandro. "Hacking Team, Software de Interceptación y Vulneración a Derechos Humanos." *ADC Digital*, August 2015.

presidency of Cristina Fernández, was headed first by Héctor Icazuriaga and later by Oscar Parrilli. "I am sure they will make a purchase in the short term (hopefully from us)," Nicolás Ruggiero wrote to his Hacking Team counterpart on July 8, 2015." [123]

The optimism expressed in Ruggiero's message is notable. However, the existence of any actual purchases could not be confirmed.[124] This raises a crucial question: could the software have been acquired and used for some time without the public knowing?

Two years later, in 2017, Patricia Bullrich—who, as noted, is the current Minister of Security, having held the same office between December 2015 and December 2019—expressed interest in acquiring spyware for mobile phones. In fact, during the process of reforming the Criminal Code, the executive branch attempted to introduce legal authorization for the use of such programs to monitor citizens' activities through their phones, computers, and other devices, including proposals that would have extended their use outside traditional judicial authorization frameworks. [125]

It was in this context that, in January 2018, a new meeting reportedly took place with Global Interactive Group—one of the resellers that had signed a non-disclosure agreement with Hacking Team—to present additional surveillance software solutions to senior officials from the country's main security forces.[126]

On that occasion, the company also took the opportunity to promote another product. Its code name was "Iron Man" and, according to the official record, it belonged to a "Spanish" company called "In Nova". Two possibilities emerge at this point. The most likely scenario is that the reference in the meeting record is a mistake and that, as discussed below, the company in question was in fact the Italian firm Innova S.p.A., which specializes in network intelligence products. If, alternatively, it did refer to a Spanish company, the most plausible candidate would be IN-NOVA, based in Toledo, which participates in a drone interception development program. However, this does not seem likely. [127]

---

123 "WikiLeaks - The Hackingteam Archives." 2015. URL

124 While Mobile Surveillance Monitor Network platform showed four cases of Pegasus, from NSO Group, in 2024, the results turned out to be false positives. URL

125 *Asociación por los Derechos Civiles* (ADC), *Asociación Civil por la Igualdad y la Justicia* (ACIJ), *Asociación Pensamiento Penal* (APP), and *Instituto de Estudios Comparados en Ciencias Penales y Sociales* (Inecip). "La reforma del Código Procesal amplía las facultades del Estado para vigilar." Políticas de Seguridad. CELS, April 17, 2018. URL

126 Registro Único de Audiencias de Gestión de Intereses, Ministerio del Interior (Argentina), "Audiencia ID 9763," URL

127 The less likely option. If it in fact referred to a Spanish company, the leading candidate would be IN-NOVA Programa de Innovación Internacional S.L.U., registered in Toledo, which develops R&D&i projects and provides technology consulting services—including in the field of cybersecurity—through its subsidiary and the In-Nova Castilla–La Mancha Foundation, related to the National Cybersecurity Institute (INCIBE). Documents from Spain's Public Sector Procurement Platform confirm its participation in a contract with the *Instituto Nacional de Técnica Aeroespacial* (INTA—aerospace technology—) for the development of an interceptor RPA prototype, an indication of its involvement in security and defense solutions. *Boletín Oficial del Registro Mercantil,* "IN-NOVA Programa de Innovación Internacional, S.L.U.," September 27, 2024 URL // Plataforma de Contratación del Sector Público (Spain), *Adquisición de prototipo RPA interceptador* – INTA, October 16, 2019, URL

In 2021, two journalists gained access to the financial records of Italian company Cy-4gate, discovering the existence of contracts with Argentine entities.[128] To demonstrate that its client portfolio extended beyond the domestic market, the company itself highlighted that it held export licenses for dual-use products destined for Argentina—most likely through local intermediary Assine S.A. Based on the products marketed by Assine, two possibilities emerge: that the contracts concerned the spyware known as Epeius, conceived as a competitor to NSO Group's Pegasus, or alternatively, other company developments such as D-SINT (an OSINT-type passive analysis tool) or Hydra (designed for the active interception of IP traffic).

Another source of suspicion concerns spyware developed by the Spanish company Mollitiam Industries, with its best-known products Invisible Man and Night Crawler, used in surveillance operations in Colombia. Various sources describe Mollitiam as a supplier of cyber-espionage tools to armed forces and security organizations in Latin America. More specifically, in Argentina, its solutions are offered through VEC S.R.L., which presents itself as a specialist in digital intelligence, critical communications, and defense. Technologies for law enforcement and security agencies are marketed under COMINT and OSINT labels, with unusually ambiguous wording. Its COMINT line is described as follows:

> **"Exploitation and post-exploitation platform. Mollitiam's modular COMINT solutions cover the entire interception process, improving operational results and optimizing resources. (for Law Enforcement Agencies ONLY)."** [129]

It is further stated that it is capable of covering the entire interception process, including encrypted communications. This wording resembles spyware marketing language more than that of traditional communications intelligence.

This is reinforced by the Spanish Government's Annual Report on Exports of Defence Material and Dual-Use Products and Technologies. The report records exports to Argentina in 2020 under Category 5 of the dual-use annex—"Telecommunications and information security"—a category typically encompassing digital intrusion and surveillance tools. Publicly available data do not allow for the identification of the specific suppliers or the products exported; however, Mollitiam appears in Spanish defense-industry catalogues and applies for export licenses for parts of its cyber-espionage suite. This supports the hypothesis that these technologies may be marketed domestically through local intermediaries such as VEC, even in the absence of open evidence of specific contracts with federal or provincial agencies.[130]

Consequently, suspicions persist to varying degrees. The companies mentioned—VEC S.R.L. (a distributor of Mollitiam), Assine S.A. (a channel partner for Cy4gate), Global Interactive Group (which signed a non-disclosure agreement with Hacking Team in 2015 alongside other regional intermediaries), and High

---

128 Bagnoli, Lorenzo, and Ricardo Coluccini. "Sorveglianza: l'azienda italiana che vuole sfidare i colossi NSO e Palantir." *IrpiMedia*, November 17, 2021. URL

129 "Mollitiam Industries soluciones de inteligencia | VEC." Accessed June 25, 2025. URL

130 Secretaría de Estado de Comercio. *Informe Estadístico de Exportaciones de Material de Defensa, Otro Material y Productos y Tecnologías de Doble Uso 2020.* Madrid: Ministerio de Industria, Comercio y Turismo, 2021, 55–56. URL

Security / TAMCE (which appears to have acted as an intermediary in contacts with Hacking Team)—are among those that offered surveillance and interception solutions to Argentine state institutions and, in several cases, also to provincial authorities.

Although no specific spyware purchases have been proven, it would be premature to dismiss this possibility. This is not only because the scenario is legally enabled, with substantial discretionary funds and multiple supply channels. As we emphasize in the report's conclusion, other detection methods remain to be explored, such as consensual forensic analysis or the mapping of malicious infrastructure.[131]

2.2.2. SIGINT

Argentina carried out several public bidding processes for IMSI-catcher equipment and other frequency interception technologies, such as direction-finder.[132] Examining these processes makes it possible to identify both the companies and the equipment involved.[133]

HK Systems S.R.L. offered two products manufactured by Israeli firm PICSIX: the P6 IMSI Catcher and a direction-finding (DF) system (often included with IMSI-catcher equipment). The latter provides a simple Android application used to geolocate a target device at relatively close range, since it must operate within the target device's reception range. Once the IMSI catcher detects a phone in the general area, the system operates by intercepting and analyzing the radio-frequency signals emitted by that mobile phone in order to obtain a more precise location.[134]

For its part, the Argentine company Global Interactive Group markets two products in the region under the TITAN brand. The system is described as a long-range cell phone tracker. Technically, however, it operates as a high-power portable tactical cellular base station emulator to which nearby cell phones connect automatically, enabling IMSI capture and accurate geolocation of a target

---

131 Only one isolated case was registered related to Hermit, Italian RCS Lab's spyware, identified by the Monitor Network Research Workbook in 2022. Mobile Surveillance Monitor. "Surveillance Dashboard." URL

132 In Argentina, its use requires a court order (Law 25520 and amendments).

133 Licitación Pública Nº 0006/2018, a public bidding process carried out in 2018. Resolution awarding Teclab LLC and dismissing HK Systems SRL Policía Federal Argentina, "Adquisición de 2 sistemas de localización IMSI Catcher y 1 sistema de consultas de geolocalización (LPU 30-0006-LPU18) — Acto de apertura," *Boletín Oficial,* Sept 14, 2018. URL. Policía Federal Argentina, "LPU 30-0006-LPU18 — Dictamen de Evaluación (adjudicación a Teclab LLC; desestimación de HK Systems SRL y Tecoar SA)," *Boletín Oficial*, December 18, 2018. URL // Ministerio de Seguridad, UAI, "Informe de Auditoría N.º 15/2024 (formulación PFA) — menciones a 'IMSI Catcher' y paquete de 2.000 consultas," October 15, 2024. URL

134 PICSIX, "P6-Catcher," Products, consulted October 16, 2025; "P6-MITM," Products, consulted October 16, 2025; "P6-Fi5," *Products*, consulted October 16, 2025. URL Picsix's geolocation platform deploys an encrypted application that passively queries mobile networks (GSM, UMTS, LTE) to identify base transceiver station (BTS) to which the target device is connected. When determining location of those BTSs and the device's signal direction, the system can infer the device's location.

device.[135] TITAN is likely to be a commercial brand name of the product. In the absence of any legal name associated with a specific manufacturer, TITAN could refer to a company with no publicly documented presence or equipment developed by a governmental or industrial entity without an open commercial profile. A similar situation arises with the Argentine-Mexican firm TAMCE, which markets an IMSI catcher known as Phoenix with Direction Finder capabilities.[136]

Regarding these devices, two detection initiatives are worth noting: the University of Washington's FADE (Fake Antenna Detection) project, and the Electronic Frontier Foundation (EFF)'s Crocodile Hunter project. Both projects propose simple, do-it-yourself hardware setups designed to detect potential IMSI-catcher activity using a standardized methodology. However, the data collected by these projects do not demonstrate the presence of IMSI catchers; instead, they record network anomalies consistent with their possible use and explicitly warns about the risk of false positives (for example, misconfigured or outdated cell sites). In addition, measurements conducted in the region using these methodologies covered only a limited time window—from April to November 2020—and were not carried out during specific periods, such as protests or strikes, when such equipment is often deployed. That being said, in central Buenos Aires, 2G measurements reported 17 total cases (15 "network parameter outliers" and 2 "unknown towers"), while no anomalies were detected on 4G.[137]

With regard to geolocation technologies based on the exploitation of SS7/Diameter signaling systems, Israeli company Kavit lists Argentina on its website as a client for these types of tools. Beyond identifying who is supplying such technology, there is other relevant evidence. According to Mobile Surveillance Monitor, Argentina appears among the countries with the highest recorded exposure levels in terms of surveillance enabled through signaling exploitation. This is due to the significant presence of vulnerable infrastructure in its mobile networks. In fact, within the region, Argentina has the largest amount of infrastructure prone to sustaining and enabling this type of attack. The same source indicates that, since 2022, Argentina has recorded more than 60,000 instances of significant surveillance-related activity linked to signaling attacks, primarily affecting 3G networks, with some incidents also observed on 4G.[138]

In addition, there are records in Argentina documenting official RFPs and public bidding processes regarding geolocation "queries". For example, a publicly available internal audit from Argentina's Federal Police refers to the intent to acquire IMSI catchers, a Russian voice biometrics system, and "2,000 queries" of a SS7-based geolocation platform.[139]

---

135 "Localizador de Celulares a Gran Distancia – Global Interactive Group." June 15, 2025. URL

136 TAMCE, "Interceptor Táctico PHOENIX (IMSI/IMEI; BTS falsa; 2G/3G/4G/LTE)," consulted October 16, 2025. URL

137 South Lighthouse, *FADe (Fake Antenna Detection Project),* "Buenos Aires (2G)," URL; "Buenos Aires (4G)," accessed November 5, 2025, URL; "FAQs," accessed November 5, 2025, URL

138 Mobile Surveillance Monitor. "Mobile Surveillance Monitor: surveillance dashboard." Accessed December 12, 2025. URL

139 Ministerio de Seguridad, UAI, "Informe de Auditoría N.º 15/2024 (formulación PFA)", October 15, 2024. URL

2.2.3. IP traffic intelligence

Since 2003, Argentina's regulatory framework has required telecommunications operators to implement lawful interception (LI) capabilities in line with ETSI and 3GPP standards.[140] In practice, this entails deploying mandatory LI modules within core networks. As a result, it is now possible to access official figures on the number of interception requests of the above type, submitted in recent years.[141] It is also possible to find public records documenting the transfer of "interception" equipment to *Dirección de Delitos Complejos* (complex crime division) from the *Agencia Federal de Inteligencia* (AFI).[142]

Ericsson and Nokia manufacture the infrastructure used by Argentina's largest mobile operators: Claro, Movistar, and Personal. Because it is up to these operators to provide lawful interception (LI) capabilities, it is reasonable to expect that Ericsson and Nokia supplied the LI modules integrated into their infrastructure.[143]

There are also records referencing products marketed by US company Pat Systems.[144] Its Vortex AIT-Stack suite combines IMSI catchers and an IP communications interception system designed to integrate directly into telecommunications networks to capture metadata and communications content in compliance with ETSI standards. Through nodes deployed within a provider's network, the system can intercept calls, messages, and IP traffic, transmitting the collected data in encrypted form to a monitoring center where it is processed, analyzed, and stored. Depending on the protocol involved, the system may access unencrypted content or intercept content before or after encryption is applied. According to an older promotional brochure, the platform also includes advanced capabilities such as search and geolocation tools, ensuring operational traceability and security.[145]

---

140 Executive Order 357/2002 and resolutions from Secretaría de Comunicaciones. Corte Suprema de Justicia de la Nación, "Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado (DAJuDeCO)," *Poder Judicial de la Nación*, URL

141 Between 2016 and 2025, *Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado* (DAJuDeCO—legal assistance division in complex and organized crime—) recorded a marked increase in requests for assistance related to the interception and processing of communications data. Of all assistance requests, 79.4 percent originated from public prosecutors' offices, compared with 20.6 percent from courts. During the same period, 5,327 urgent communication handover assistance cases and 1,875 communication assistance cases were documented, while requests for associated information totaled 206,818, most of them addressed to the Public Prosecutor's Office. Between 2019 and 2024, 160,232 requests for processed data were handled, resulting in 426,349 responses, pointing to a sharp intensification in the use of investigative tools based on traffic data and related metadata. "Crece la actividad de la Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado con el sistema acusatorio." URL / URL

142 Argentina.gob.ar. "La AFI entregó equipos a la DAJUDECO." July 17, 2020. URL

143 Nokia Corporation, "Lawful Intercept (LI) describes a process to intercept telecommunications ... Nokia's implementation satisfies most national standards' requirements," *Nokia Infocenter*, URL // Ericsson AB, "Regulatory Products," URL

144 "PAT Systems | Surveillance Watch." Consulted December 12, 2025. URL

145 PAT Systems, *VORTEX AIR-STACK V4 — IMSI CATCHER* (brochure/PDF), consulted October 16, 2025. URL // "Pat Systems - Centros de Monitoreo." October 6, 2024.URL // "Pat Systems | Vortex-Stack." URL

Equipment developed by Italian firm Cy4gate is also available on the local market. Based on the available offers, this could refer to its Hydra product. Hydra is deployed within an internet service provider's infrastructure—for example, connected to an aggregation point, core router, or backbone switch—allowing it to integrate passively into network traffic flows. Hydra collects metadata—such as website visits, application usage, and communication frequencies— thereby generating digital profiles. The system cannot decipher content or access private messages; its stated focus is metadata analysis and digital behavior. Even so, it can profile content categories, identify users and usage patterns, map connections, inspect packets, and extract visible metadata from network traffic. It is also worth noting that Cy4gate currently markets an integrated product known as CEWIS (Cyber Electronic Warfare Integrated System), which combines multiple modules, including IMSI catcher technology, SS7/Diameter protocol exploitation, communications interception, direction finding, and OSINT capabilities.[146]

It is likely that Global Interactive Group acted as an intermediary in offering products from Italian company Innova S.p.A. in 2018. Innova's technologies have previously been marketed alongside those of Hacking Team in other countries across the region, including Chile in that same year. Innova typically specializes in IP-based lawful interception systems, such as EGO. The name "Iron Man," which appears in records of a hearing with the firm, may have functioned as a commercial alias or localized branding for Argentine agencies.[147]

To this list of tools that Argentina likely acquired, one could add Cognyte (formerly Verint), given that Argentina appears as a "regional government client" in the company's 2021 marketing materials.

As noted in Section 1.2.3, if a security agency were to connect on its own initiative any commercial platforms such as Vortex (Pat Systems), Hydra/CEWIS (Cy4gate), or EGO (Innova) to access points within the network infrastructure, an important question arises: to what extent could these tools provide meaningful and sustained visibility into traffic flows without the cooperation of service providers—that is, beyond established legal frameworks.

Several considerations are relevant here. (i) The above-mentioned 2014 technical report "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping" had explained that end-to-end encryption became more widespread and, as a result, interception capabilities increasingly had to be paired with techniques that directly targeted users' devices to obtain data before encryption was applied[148]; (ii) more recently, Amnesty Tech documented how the

---

146 "HOMELAND SECURITY MOBILE ASSETS | CY4GATE S.p.A." URL

147 One possibility is that we are dealing with EGO (also marketed in Chile during the same span of years) or some other centralized platform for IP traffic interception developed by Innova S.p.A. "Innova_Product List, Specifications_MicroIP, EGO, Internet Interception and Probes, Gps Innova, RB800." 2011. URL

148 In 2014, this paper explained "the viability and implications of an alternative method for addressing law enforcement's need to access communications: legalized hacking of target devices through existing vulnerabilities in end-user software and platforms. The FBI already uses this approach on a small scale; we expect that its use will increase, especially as centralized wiretapping capabilities become less viable". Bellovin, Steven M., Matt Blaze, Sandy Clark, and Susan Landau. "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet." *Northwestern Journal of Technology and Intellectual Property* 12, no. 1 (2014): 66. URL

Intellexa suite integrates network intelligence tools with additional techniques of questionable legality. In that case, the Predator spyware is designed to operate in cooperation with internet service providers to inject infection links while a target is browsing the web[149]; (iii) in the previously cited investigation, CIPER documented the operational capacity of lawful interception modules outside the formal circuit. [150]

Based on these investigations, it is plausible to believe that, in principle, duplication of traffic and metadata for storage and analysis is feasible. However, its practical extent would depend critically on factors such as the exact connection point and the scale of deployment. Platforms such as Hydra, Vortex, or EGO can operate lawfully as LI systems within standardized channels. However, they could also be used alongside other technologies to intercept outside the legal framework if they are fed copies of traffic or if they are combined with additional tools, in ways that fundamentally alter the legal basis, traceability, and risk of abuse.

2.2.4 Network monitoring

At least since 2010, this category has included Blue Coat, a supplier to the NSA and developer of PacketShaper—equipment that can be used both to secure and manage networks and to restrict access to information and monitor communications and Internet traffic.[151]

Also of regional reach, Sandvine has reported deploying its traffic management solutions in multiple Latin American countries, without specifically referring to Argentina, Chile, or Uruguay.[152] A similar case is Allot. The latter markets a network intelligence and traffic management platform for telecommunications operators that incorporates deep packet inspection (DPI), application and user visibility, policy control, and high-capacity service gateway capabilities. The company advertises that a "Tier 1 fixed-line operator in Latin America, with millions of subscribers, has chosen Allot HomeSecure to deliver cyber protection services," which points to a regional commercial contract.[153]

---

149 Amnesty International Security Lab, "To Catch a Predator: Leak Exposes the Internal Operations of Intellexa's Mercenary Spyware" URL

150 Peña, Cristóbal and Sebastián Minay. "Así se hacen los cuestionados 'pinchazos' telefónicos legales." Investigación. *CIPER Chile*, October 29, 2008. URL

151 Marquis-Boire, Morgan, Collin Anderson, Jakub Dalek, Sarah McKune, and John Scott-Railton. *Some Devices Wander by Mistake: Planet Blue Coat Redux.* Citizen Lab and Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, 2013. URL

152 *"Sandvine Expands Multi-Country Deployments Across Latin America,"* Sandvine Press Release, 2023, URL // BNamericas, "Sandvine Seals US$3 mn Contract with Tier 1 LatAm Telco," BNamericas, July 15, 2022, URL

153 Allot, *Allot Solutions for Service Providers* (ca. 2021), technical brochure, URL // Allot, "Tier-1 Fixed Broadband Operator, with Millions of Subscribers in Latin America, Selects Allot HomeSecure to Provide Cyber Protection Services," Press Release, May 11, 2023, URL

In 2021, Telecom Argentina rolled out an Open Caching platform with Cisco and Qwilt integrated into its infrastructure. This was to improve video content delivery through advanced traffic analytics.[154] While this technology is not deep packet inspection (DPI) in a strict sense, it relies on related mechanisms for network-level data analysis and flow optimization, and it provides significant visibility into the operator's data flows.[155]

As this report has stressed from the outset, given the monitoring and intrusion capabilities of tools like these, it becomes clear why their scope and real-world uses must be openly debated.

2.2.5. OSINT/WEBINT

Argentina has also emerged as a significant purchaser of web content analysis tools.[156] Shortly after the Ministry of Security's announcement in 2018, the civil society organization *Asociación por los Derechos Civiles* (ADC) warned about the human rights risks associated with state monitoring of social media posts.[157] That same year, likely through Israeli company Rafael, OSINT solutions from Verint and Cognyte were reportedly acquired that were compatible with their IP monitoring capabilities.[158]

D-SINT, developed by Italian firm Cy4gate, is also marketed locally. Cy4gate holds export authorizations for dual-use technologies in the country. Designed to compete with Palantir, it collects, processes, and analyzes data from digital platforms—social networks, online forums, and public or semi-public databases—using techniques such as web scraping, text mining, and communication pattern analysis. The system is designed to operate in conjunction with Phoenix or Hydra—also developed by the same company—functioning as a data-fusion platform that integrates multiple sources. According to available information, it includes facial and object-recognition functions, enabling searches for information about individuals and items across text repositories, image databases, and social media. [159]

In addition to the products offered and available, another clue is a bidding process issued by Argentina's Airport Security Police (PSA) in 2024. The official bidding

---

154 Qwilt, *"Open Caching and Edge Delivery for Telecom Operators"*, URL // Cisco Systems, "Telecom Argentina Launching New Cisco, Qwilt and Digital Alpha CDN Solution to Improve Streaming Experience for Its Customers in Argentina," Cisco Newsroom, February 5, 2021, URL

155 *"Telecom Argentina Adopts Open Caching CDN Solution from Cisco and Qwilt,"* Cisco Newsroom, 2021, URL // Telecom Argentina, "Plataforma Open Caching CDN 'as-a-service'", press release, 2021.

156 Ucciferri, Leandro. Seguidores que no vemos – *Una primera aproximación al uso estatal del Open-source intelligence (OSINT) y Social media intelligence (SOCMINT)*. ADC, 2018. URL

157 Asociación por los Derechos Civiles (ADC), *Seguidores que no vemos: prácticas estatales de monitoreo en redes sociales y sus impactos en los derechos humanos*, Buenos Aires, 2018, URL

158 "InfoLEG - Ministerio de Justicia y Derechos Humanos - Argentina." URL

159 Bagnoli, Lorenzo, and Ricardo Coluccini. "Sorveglianza: l'azienda italiana che vuole sfidare i colossi NSO e Palantir." I*rpiMedia*, November 17, 2021. URL

documents for the purchase of an "integrated data-fusion, geolocation and WEBINT platform" set out requirements that appear specifically consistent with the above tool: real-time fusion, analysis and visualization of heterogeneous data, including case-management functions, cellular geolocation, OSINT/social-media profiling, graphs/AI analysis, report exporting, and predictive analysis.[160] None of the other OSINT platforms discussed later simultaneously combines AI-enabled WEBINT analysis with the specific geolocation functions required by the bidding specifications (MSISDN/IMSI 2G/3G/4G). By contrast, Cy4gate's full suite —(D-SINT/QUIPO) with lawful-interception components—would be one of the few offerings that could plausibly cover the entire set of specifications.[161] It is therefore reasonable to infer that the bidding process was structured with this particular acquisition in mind.

This category may also include the i2 Limited system, acquired by Argentina's Ministry of Security, as well as by the City of Buenos Aires and the province of Río Negro in 2019. The platform serves primarily as an analytical engine designed to interoperate with other data-analysis tools referenced in public procurement records.[162] According to available information, i2 Limited—acquired by IBM in 2011—offers advanced network and link-analysis and visualization capabilities aimed at identifying patterns and relationships across large datasets in support of investigative and intelligence analysis.[163]

It is also likely that some of the country's law enforcement and security agencies use Medusa, the OSINT platform by Italian company IPS Intelligence (Intelligence Positioning Solutions S.p.A.), which also markets IP network analysis, intelligence, and interception capabilities.[164] Medusa collects and analyzes large volumes of data from social media, as well as from the web, deep web, and dark web, with the aim of transforming open-source information into actionable intelligence. According to the company's prospectus, the platform—marketed primarily for national security and defense contexts—uses advanced analytics and artificial-intelligence techniques to detect real-time trends, monitor senti-

---

160 *"Plataforma integral de fusión de datos, geolocalización y WEBINT"* (official bidding specs), Gobierno de la República Argentina, 2023, URL

161 "Products | CY4GATE S.p.A." Accessed December 12, 2025. URL

162 "I2 Analyst's Notebook - Discover and Deliver Actionable Intelligence | I2." Accessed August 1, 2025. URL // IBM. "IBM -Integrated Law Enforcement: A Holistic Approach to Solving Crime." IBM, 2014. URL

163 There was a case of direct procurement from the Ministry of Security (2016) with the description "Software avanzado para el análisis criminal con la firma Unitech S.A."—advanced software for criminal analysis with firm Unitech S.A.—(Proc. 347-0066-CDI16), designed for criminal analytics and intelligence (link analysis, data mining, and network visualization). Organizations that audited the process cite the same case file and link it to the IBM i2 suite (Analyst's Notebook / Enterprise Insight Analysis), a family of tools used by ministries of security and prosecutors' offices to uncover patterns, connections among individuals, calls, and cases, as well as timelines and network graphs. In addition, in 2018 the Public Prosecutor's Office of the City of Buenos Aires (MPF CABA) awarded a contract for an "i2 criminal analysis package". In those proceedings, IBM stated that Unitech S.A. was its authorized reseller; this is consistent with its role as an integrator and distributor of analytical software. URL

164 In addition to TAMCE's offer, IPS S.p.A. is also known to operate as a global provider of open-source intelligence, with activities in several regions, including Latin America, and subsegments that include Argentina. URL

ment and public opinion, and analyze the circulation of messages across digital platforms. In addition, it supports automated target profiling based on publicly available data and enables proactive engagement through managed social-media identities, such as amplifying counter-narratives or responding to selected posts. These features are presented as improving reaction and prevention capabilities in digital-threat monitoring environments. The platform also claims the capability to collect information from forums and ".onion" sources within dark-web ecosystems through dedicated crawling components.[165]

Minerva IA is another Spanish OSINT/WEBINT tool that TAMCE markets in Latin America. It is advertised as more than a basic scraping-and-analysis product. The company presents it as a broader suite of cybersecurity, cyber intelligence, and cyber defense solutions, building on proprietary AI, machine learning, deep learning, and big-data models to detect, analyze, and anticipate complex threats—particularly in high-volume data environments. Independently of marketing claims, its products range from infrastructure and system cybersecurity services to analysis of digital information and online narrative, supported by the work of human analysts, consultancy, and digital forensics for civilian, military, and governmental organizations.

TAMCE also markets another OSINT solution in the region aimed at both law enforcement and security agencies, and the private sector: Social Links CrimeWall. This one is designed to support investigations with object recognition, facial biometrics, and sentiment analysis across social media and open sources.[166]

It is clear that in recent years Argentina has steadily expanded the deployment of intelligence systems based on data analytics and digital monitoring, via WEBINT tools, geolocation, and AI-driven automated analysis. In 2024, Argentina gained a new framework. The Ministry of Security's Artificial Intelligence Unit was formally structured through Resolution 710/2024, authorizing the use of software to analyze social media activity, anticipate riots, and track crime-related movements.[167] It is worth noting, however, that this "unit" was created through ministerial resolution, within a division itself established through ministerial resolution, and reporting directly to the head of the advisory cabinet of Security Minister Patricia Bullrich. In other words, it operates outside any formal organizational chart and beyond the scope of the Intelligence Law, which explicitly prohibits intelligence activities being conducted by entities not expressly listed in it.

---

165 "MEDUSA - Plataforma de Inteligencia Activa | TAMCE. URL

166 "CrimeWall." *TAMCE*. Consulted October 19, 2025. URL

167 *Resolución 710/2024*, Boletín Oficial de la República Argentina, July 29, 2024, URL

Table 2: Summary — Argentina

ARGENTINA				
Tool	Company	Distributor	Technology / Product	Acquisition
Spyware	**Hacking Team (Italy)**	Global Interactive Group / Nullcode Team / TAMCE	Remote Control System (RCS) marketed under various names, such as Galileo	Likely. The company has given presentations in Argentina at least in 2012 and 2018.
	NSO Group (Israel)		Pegasus	Likely. The company held negotiations at least during 2014.
	Mollitiam (Spain)	VEC S.A.	*Invisible Man / Night Crawler*	Likely. VEC offers products such as "exploitation platform" and holds export licenses for dual-use products in cybersecurity to Argentina.
	Cy4gate (Italy)	Assine S.A.	Epeius	Likely. The company has a local reseller and export licenses for dual-use cybersecurity products to Argentina.

ARGENTINA				
Tool	Company	Distributor	Technology / Product	Acquisition
SIGINT	**PICSIX (Israel)**	HK Systems SRL	*IMSI catcher / Direction Finder* / SS7 exploitation	Very likely. Offered in national and provincial tenders.
	TITAN (US)	Global Interactive Group	*IMSI catcher*	Very likely.
	Kavit (Israel)		SS7-Diameter exploitation	Very likely. Confirmed by the company itself.
	Pat Systems (US)		*IMSI catcher* / SS7 exploitation	Very likely. Advertised by the company.
	Phoenix	TAMCE	*IMSI catcher / Direction Finder*	Confirmed.
	Cy4gate (Italy)	Assine S.A.	*IMSI catcher* / SS7-Diameter exploitation	Very likely. The company has local reseller and export license of dual-use products in cybersecurity to Argentina.
	Rohde & Schwarz (Germany)	Rohde & Schwarz Argentina SRL	*IMSI catcher / Direction Finder*	Very likely. The company has local subsidiary, and numerous national and provincial agreements.

ARGENTINA				
Tool	Company	Distributor	Technology / Product	Acquisition
Network intelligence/ Lawful interception	**Pat Systems (US)**			Likely
	Cy4gate (Italy)	Assine S.A.	Hydra / CEWIS	Likely
	Rohde & Schwarz (Germany)	Rohde & Schwarz Argentina SRL		Very likely. The company has local subsidiary, and numerous national and provincial agreements.
	Ericsson (Sweden)	Movistar, Personal, Claro	Ericsson *Lawful Interception* (LI-IMS/LMISF)	Confirmed.
	Nokia (Finland)	Movistar, Personal, Claro	Nokia LI	Confirmed.
	Innova S.p.A. (Italy)	Global Interactive Group	Some Lawful Interception system	Likely
Network monitoring	**Blue Coat (US)**		PacketShaper	Confirmed
	Sandvine / Procera (Canada)	Ingram Micro / Datco / Cablevisión– Fibertel	Active Network Intelligence, PacketLogic	Very likely
	Allot (Israel)	Telefónica	Service Gateway Tera (SG-Tera) (DPI for CSP and ISP)	Confirmed

ARGENTINA				
Tool	Company	Distributor	Technology / Product	Acquisition
OSINT / WEBINT	**Cy4gate (Italy)**	Assine S.A.	D-SINT / QUIPO	Likely
	I2 Technologies / IBM (US)	Unitech S.A.	i2 Analyst's Notebook – search and visualization engine with integration capability with other data-mining technologies/	Confirmed
	Minerva IA (Spain)	Global Interactive Group		Likely
	Rafael - Verint / Cognyte (Israel)		SOC (Security Operations Center) + OSINT tools	Confirmed
	IPS Intelligence Spa (Italy)	TAMCE	Medusa	Likely

ARGENTINA				
Tool	Company	Distributor	Technology / Product	Acquisition
Forensic extraction	**Cellebrite (Israel)**	Security Team Network S.A. / IAFIS Argentina S.A., ARSEC	UFED	Confirmed
	Digital Intelligence (US)	Estudio de Informática Forense	Forensic Recovery of Evidence Device (FRED)	Confirmed
	EnCase Forensic (US)			Confirmed
	MOBILedit Forensic (Czech Republic)			Confirmed
	MSAB (Sweden)	VEC S.A.		Confirmed
	Oxygen Forensics (US)			Confirmed
	Silicon Forensics (US)	HOZ S.A		Confirmed

ARGENTINA				
Tool	Company	Distributor	Technology / Product	Acquisition
Video-surveillance / Biometrics / Facial recognition	**3M Electronics Monitoring Inc. (US)**		Biometrics	Confirmed
	AnyVision / Oosto (Israel)		Better Tomorrow	Confirmed
	BGH Tech Partner (Argentina)		Video-surveillance – facial recognition	Confirmed
	Clearview AI (US)		Facial recognition (open-source images)	Confirmed
	Haivision (Canada)	Danaide SA		Confirmed
	Hikvision and Dahua (China)		Cameras and biometric video analysis	Confirmed
	Huawei and ZTE (China)			Confirmed

ARGENTINA				
Tool	Company	Distributor	Technology / Product	Acquisition
	IDEMIA (former Morpho) (France)			Confirmed
Video-surveillance / Biometrics / Facial recognition	**Incode (US)**		Digital identity and biometrics	Confirmed
	Jumio (US)		Identity verification	Confirmed
	NEC (Japan)		Biometrics and facial recognition	Confirmed
	NtechLab (Russia)		Find Face, UltralP	Confirmed
	Veridas (Spain)		Voice and facial biometrics	Confirmed
	Speech Technology Center (STC Group) / Speech Pro (Russia)		Voice biometrics (acoustic analysis tools)	Confirmed

3. Chile
3.1. Context

Chile also became part of the regional list to which Germany was revealed to have exported dual-use tools for cybersurveillance.[168] This marked a regional milestone in 2014. In that context, the hypotheses outlined in the previous section also apply here. Furthermore, the following year, Chile was explicitly referenced in the Hacking Team email leak, which named the Investigations Police of Chile (PDI — *Policía de Investigaciones*—) as a client.[169]

Two further episodes drew widespread media attention in 2017. First, Global Systems Chile—an affiliate of Israeli company Rebrisa Ltd.—sold aerostatic surveillance balloons to the municipality of Las Condes, triggering a series of investigations concerning video surveillance and biometric technologies. Along similar lines, news outlet *América Transparente* later uncovered a multimillion-dollar investment in a facial recognition system supplied by French company IDEMIA. The system reportedly operated without prior public disclosure in Santiago.

That same year, the so-called *"Operation Huracán"* became publicly known. In the context of social conflict in the country's south, a police fabrication of evidence was used to implicate Mapuche activists in acts of violence. The false information in the police *(Carabineros)* investigation stemmed from allegedly "intercepted" encrypted WhatsApp messages. To justify the police's purported access to those messages, it was claimed that *Carabineros* had a locally developed spyware tool known as "Antorcha." Later reports concluded that the evidence was fabricated and also cast doubt on whether the tool itself ever existed as described.[170]

On October 18, 2019, a wave of social mobilization broke out, lasting through March 2020. During those months, digital rights civil society organization *Derechos Digitales* received numerous reports of police investigations and intimidation based on information obtained through social-media monitoring.[171] In that context of unrest, leaks of internal *Carabineros* documents, known as "Pacoleaks", exposed cases of police intelligence activities targeting activists, unions, and student groups.[172]

In the wake of these high-profile episodes, the Inter-American Commission on Human Rights (IACHR) condemned that same year surveillance targeting journalists investigating corruption cases, as well as the fabrication of police evidence

---

168 TEDIC. "La adquisición y el abuso de tecnologías de vigilancia en América Latina - Al Sur." *TEDIC*, March 28, 2019. URL

169 "WikiLeaks - The Hackingteam Archives." 2015. URL

170 Garay, Vladimir, and Zack Rogoff. *Tecnología y Vigilancia En La Operación Huracán: Una Revisión Del Trabajo Periodístico Realizado En Torno al Caso*. Derechos Digitales, 2018. URL

171 Derechos Digitales, "Situación de derechos humanos y el uso de tecnología en el contexto de la protesta social en Chile 2019", Santiago de Chile, November 2019; URL ; Datos Protegidos. "Informe 2020 - Libertad de expresión en Chile." *Fundación Datos Protegidos*, June 30, 2021. URL

172 Fossa, Lissette. "PacoLeaks: Estos son los nombres y organizaciones que han sido vigiladas por Carabineros en los últimos meses." *Interferencia,* November 1, 2019. URL

and the monitoring of unions and social organizations. Investigations conducted by organizations such as Amnesty International, the Inter-American Commission on Human Rights, Human Rights Watch, and the Office of the United Nations High Commissioner for Human Rights determined that serious violations had been committed by officials of the Chilean state.[173]

In subsequent years, the debate over state surveillance capabilities went from the headlines to the regulatory sphere. Starting in 2018, a series of technical resolutions increasingly introduced a framework that enabled retention and cross-analysis of traffic data. This process culminated in 2025 with a broader reform of the regulation governing interception and recording of communications (Decree No. 142/2005), updating procedures regarding court orders and the handling of traffic data.[174] The same year, a supplemental law introduced the power of network intervention using "technologies that simulate telecommunications transmission systems", i.e., cell-site simulators or IMSI catchers. The new wording expressly references identifiers such as IMSI, IMEI, MSISDN, and IP, expanding the scope of tracking and authentication-related data. Chile thus moved from specific episodes of irregular surveillance toward a more formalized regulatory environment—one that remains contested by civil society groups for lack of transparency in the deployment of such technologies and of effective democratic control mechanisms.

Box 12: Some resellers worth looking into

- **Tecnodata**. A long-standing supplier within the technological circuit of Chilean police, *Carabineros*, particularly in relation to interception infrastructure and technical support. Investigative reporting indicates that the Danish ETI system—operational for interceptions since 2001—was acquired through Tecnodata, a company publicly associated with Alfredo Giacoman. This positioned Tecnodata as a recurrent actor in the procurement and support of sensitive technologies for the institution.
- **Mipoltec.** Mipoltec was established in 2013 by Jorge Patricio Lorca Rivera, a former Tecnodata employee, who subsequently operated as a supplier and integrator of equipment for use by law enforcement with a focus on interception capabilities. The supply of Innova S.p.A.'s EGO interception system was awarded to Mipoltec through a private tender process, to be used by *Carabineros* (awarded in late 2013 and contracted in 2014). Simultaneously, Mipoltec secured additional contracts linked to monitoring and wire-tapping for other agencies. Lorca and Mipoltec also acted as the local intermediary for Hacking Team in the sale of its RCS Galileo system, rebranded "Phantom" for the Investigations Police. Emails published by WikiLeaks show direct exchanges between Hacking Team executives and Lorca under the subject line "Proposal to DEMTEL" (Telephone Monitoring Department), along with references to commercial presentations held with *Carabineros* as a prospective client.

---

173 Montes, Rocío. "La ONU denuncia 'violaciones graves de los derechos humanos' durante el estallido social en Chile." *El País* (Madrid), December 13, 2019. URL

174 *Diario oficial de la República de Chile* - Number 42.096, Saturday June 30, 2018 - Number 44.063, Friday January 31, 2025 - Number 44.073, Wednesday February 12, 2025. URL // URL /// URL

- **SAT Internacional S.A.** is a Chilean company incorporated in 1990 and founded by former Colonel Jaime Vicencio Serre. His son, Jaime Vicencio Silva, is the legal representative, lobbyist, and shareholder of the company. In the intelligence/OSINT field, SAT Internacional appears in official records under Chile's Lobby Act, as a representative of an interest group, introducing Israeli company Prelysis and its Tucán platform in Chile. Tucán is described in those records as an OSINT tool designed to monitor instant messaging and social media, including capabilities for "de-anonymizing" users and messages, as well as conducting searches across leaked data. In their capacity as intermediaries and representatives for foreign vendors (not only in surveillance), SAT Internacional is listed in Chile's institutional registry of "special foreign suppliers with representation in Chile." It is registered as the local representative of Israel Weapon Industries (IWI). Within the same context of hearings under the Lobby Act, SAT Internacional also appears to manage presentations linked to Israel Aerospace Industries (IAI), identified in those records as their principal.
- **DYMEQ Ltda.** (DYM Equipos e Ingeniería Limitada) appears as a Chilean integrator/vendor focused on security and telecommunications. It states that it delivers solutions to the armed forces and government entities for the monitoring of terrestrial and satellite signals. Within its defense portfolio, the company includes "radio intelligence systems." Administrative records show DYMEQ features capabilities typically associated with radio-spectrum monitoring to hand over data to the monitoring center of Chile's Under-secretariat of Telecommunications (SUBTEL), including components and licenses from Rohde & Schwarz. This reinforces DYMEQ's profile as a recurring supplier of signal infrastructure. In addition, at hearings under the Lobby Act, DYMEQ appears to present "communications and electronic warfare equipment". In those instances, the company identifies itself as the Chilean representative of Rohde & Schwarz, consistent with a broader pattern of local intermediation and representation for sensitive technologies.
- **DTS** (Desarrollo de Tecnologías y Sistemas SpA) is positioned as an actor within the defense electronics sector operating in the SIGINT domain and adjoining areas. Its origins are formally associated with the Chilean state. Chile's Empresa Nacional de Aeronáutica (ENAER) states that, in 1991, DTS was created as a subsidiary in partnership with ELTA Systems Limited, as part of a diversification strategy into aeronautical electronics. In specialized media, DTS appears associated with defense capabilities, including electronic warfare, support and modernization, and industrial integration—positioning it as a recurring technological supplier within Chile's military ecosystem. In its own publicity materials, the company explicitly references electronic warfare activities "using the electromagnetic spectrum" with a catalog of related products and solutions. Supplementing this profile, DTS and third-party sources have made public technical alliances with international vendors in the sector—such as EMC testing training and equipment provided by Rohde & Schwarz under military standards—. This typically points to integrators operating within sensitive technology supply chains. DTS's capacity as a regional importer for Italian ELT Group / Cy4gate Spa is also noteworthy.

- **Grupo Zeuz / RightCom** (Verint/Intelligence/Cognyte ecosystem). Group Zeus identifies itself as the official representative of Verint in Chile, and Chilean Lobby Act records include entries in which the company appears as a representative for the Southern Cone on behalf of Verint and Cognyte before defense and security institutions.
- **Innova Chile SpA** is the only regional subsidiary of Italian lawful-interception firm Innova S.p.A.. It was incorporated in 2019 with Innova S.p.A. as its sole shareholder, represented by Daniele Traunero. Its stated line of business explicitly includes the "supply of products and services in the field of security and interception," alongside the marketing of electronic equipment, the design and maintenance of networks, video-surveillance systems, and related training. For instance, Mercado Público (the state procurement platform) registered a purchase order from the Chilean Gendarmerie for "maintenance, support and updating of the EGO monitoring service". In parallel, specialized press disclosed that Chilean Investigations Police awarded Innova Chile the lease of the EGO system as an interception, recording, and monitoring platform—detailing technical and implementation features—further underscoring its position as a local supplier and support provider for lawful-interception technology.

3.2. Demand / Solutions

3.2.1. *Spyware*

In July 2015, the aforementioned Hacking Team's email leak revealed that *Policía de Investigaciones* (PDI) had acquired the company's spyware under the name "Phantom."[175] To this day, the terms under which this technology was used remain unknown, as do the identities of those infected and placed under surveillance with this spyware. As elsewhere in the region, there have been no published forensic analyses of specific devices in Chile. In one of the leaked emails, the head of the *Departamento de Monitoreo Telefónico* (DEMTEL—telephone monitoring department) stated that the software's actual purpose was "to use it as a support tool to obtain targets IP data and access information that could not be obtained through a court order."[176] That statement about its intended use is particularly revealing.

A central figure in Hacking Team's email exchanges was Jorge Lorca Rivera, who at the time was operating through Mipoltec, identified as a key supplier of this kind of technology in Chile.[177] The emails also make clear that Rivera served as an intermediary for another Italian firm, Innova S.p.A., better specialized in ne-

---

175 "WikiLeaks - The Hackingteam Archives." 2015. URL

176 Partarrieu, Bárbara, and Matías Jara. "Los correos que alertaron sobre la compra del poderoso programa espía de la PDI." Actualidad. CIPER Chile, July 11, 2015. URL

177 Pérez de Acha, Gisela. *Hacking Team: malware para la vigilancia en América Latina*. Derechos Digitales, 2016. URL

twork intelligence solutions.[178] As in the Argentine case, it appears to have been common practice for these two Italian companies to pitch their tools as a combined offering.

The second spyware case uncovered in Chile involved NSO Group's Pegasus. According to the dataset cited by the CyberPeace Institute in its reporting, three cases of alleged Pegasus use attributed to the Chilean Investigations Police against journalists were documented in 2023.[179] The following year, another suspected infection was identified through Mobile Surveillance Monitor.[180] These findings add a new chapter to the history between that institution and the company: two years earlier, reports had already surfaced about the use of Circles—an NSO tool—for SS7/Diameter signaling exploitation.[181]

3.2.2. SIGINT

After the 2014 report submitted to the German Parliament, public procurement records in Chile confirm the presence of Rohde & Schwarz equipment, integrated locally by DYMEQ Ltda. Such equipment was intended for technical monitoring of the radio spectrum, rather than for the interception of communications content. Contracts of the Undersecretariat of Telecommunications (SUBTEL), along with *Mercado Público* datasheets, reference monitoring and radiolocation stations installed at facilities in Santiago and La Reina. The equipment is designed for the inspection and geolocation of radio emissions, typically used for radiomonitoring, interference detection, and enforcement of spectrum allocation. In principle, it does not include intrusive lawful interception capabilities, IMSI capture, or SS7/Diameter exploitation. [182]

Similarly, in the case of German lawful interception company Utimaco, municipal bidding specifications reference the Utimaco HSM product line for encryption and advanced electronic signature. This confirms the company's presence in the local procurement ecosystem. It does not confirm, however, any deployment of interception platforms.

---

178 Other people referenced in Hacking Team's emails, for the Chilean case, include Eduardo Pardo Carvajal, on account of his technical-commercial role within Hacking Team, appearing as "Field Application Engineer" for the region; also, Sergio Rodríguez-Solís, who acts in Chile as technical staff of Italian Hacking Team vendor. "WikiLeaks - The Hacking Team Archives." 2015. URL

179 Kreke, Aditi, Maira Cardillo, and Sina Fisher. *Targeting, Infecting, Surveilling, Harming. A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People.* CyberPeace Institute, 2023. URL

180 Monitor, Mobile Surveillance, 2025 Workbook, URL

181 Fossa, Lissette. "Prensa internacional revela espionaje con software Pegasus a dirigentes sociales, políticos y periodistas." *Interferencia,* July 20, 2021. URL

182 Rohde & Schwarz's ARGUS line falls into the category of spectrum monitoring systems used by telecom regulators in a range of countries. It belongs to a broader technical frame for monitoring the radioelectric space, distinct from spying on mobile or Internet networks. Chile's Subsecretaría de Telecomunicaciones, *Resolución Exenta N° 470/2024,* Transparencia Activa (Santiago: SUBTEL, 2024), URL // URL

According to a report by Privacy International, IMSI-catcher equipment used in Chile may have been supplied by U.S.-based company Almenta.[183] If this is the case, it should be noted that Almenta markets the CAPTUR product line. According to company documentation, CAPTUR C operates as an IMSI/IMEI catcher with relatively limited functionality, whereas CAPTUR A includes expanded capabilities. As an active interception system functioning as a false base station, it can capture IMSI and IMEI identifiers and force nearby devices to connect to the system. Depending on configuration and network conditions, such systems may also enable interception of unencrypted traffic and support traffic-analysis functions. This places them within the category of active cell-site simulators capable, in some scenarios, of man-in-the-middle operations.[184] Testimony gathered through investigative reporting by CIPER Chile on the use of similar devices appears broadly consistent with the technical characteristics described above.[185]

According to the results of the aforementioned fake-antenna detection project conducted in Santiago de Chile, and subject to the same methodological caveats—namely, that anomalies do not constitute conclusive proof and that the study covered only a limited observation period between April and November 2020—FADe documented signals consistent with the possible operation of cell-site simulators. The report identified 21 anomalous cases in 2G networks and 11 in 4G networks. It should be stressed once again that measurements were not conducted during specific periods of social unrest, when such mobile fake-cell-site deployments are more likely to occur.[186]

With regard to geolocation equipment based on SS7 protocol exploitation, as previously noted, the Canadian research group the Citizen Lab published a report in 2020 stating that *Policía de Investigaciones de Chile* (PDI) appeared as a client of Circles, a company related to NSO Group.[187] Although that police force denied having acquired anything, the episode underscored that law enforcement and security agencies do have access to tools of this kind. Separately, the Mobile Surveillance Monitor Network has recorded more than 37,000 compatible events on Chilean telecommunications networks since November 2022.[188]

In 2024, local firm DTS (Desarrollo de Tecnologías y Sistemas) announced a partnership with Italy's ELT Group—a partner company to Cy4gate. One of DTS's announced business lines is "electronic warfare." The above agreement refers to "improving interoperability among defense systems, strengthening detection

---

183 Privacy International, and Derechos Digitales. *State of Privacy Chile*. Privacy International, 2019. URL

184 Almenta Group, "CAPTUR — Tactical Interceptions," Almenta Group, archived on August 20, 2016, URL

185 Peña, Cristóbal and Sebastián Minay,. "Así se hacen los cuestionados 'pinchazos' telefónicos legales.". *CIPER Chile,* October 29, 2008. URL

186 South Lighthouse, *FADe (Fake Antenna Detection Project)*, "Santiago de Chile (2G)," accessed November 5, 2025, URL; "Santiago de Chile (4G)," accessed November 5, 2025, URL; "FAQs," accessed November 5, 2025, URL

187 Marczak, Bill, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert. *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*. Citizen Lab Research Report No. 133. University of Toronto, 2020. URL

188 Mobile Surveillance Monitor. "Mobile Surveillance Monitor: Research Workbook." URL

and response capabilities, and providing high-level technical and operational support." The announcement adds that both firms are "pooling expertise" to deliver "innovative solutions tailored to the Chilean and broader Latin American markets" in the field of electronic defense.[189] For its part, ELT Group lists "Homeland Security & Law Enforcement" capabilities, with a general description that points to a range of SIGINT-related solutions.[190] In addition, its sister company Cy4gate SpA explicitly markets itself as a provider of "Lawful Interception & Network Intelligence" for security forces, including tools for the lawful interception of mobile and fixed networks, IMSI catchers, and OSINT.[191] Therefore, there is a medium-to-high likelihood that the partnership includes interception solutions for mobile or network communications. As the announcement indicates, the cooperative agreement may be ELT's entry point in South American markets. This is especially plausible given that DTS describes itself as "a Chilean company founded in 1991 and a leader in service provision and in the development of technology integration and defense systems", with an established track record of contracts with the Chilean state and security agencies.[192]

3.2.3. Network intelligence

Article 222 of the Criminal Procedure Code requires telecommunications providers to keep, for at least one year, a record of the IP addresses of the connections made by their subscribers and make it available at the request of the Prosecutor's Office. Investigative reporting by CIPER has also established that Chile has maintained lawful interception mechanisms in place since at least 2008.[193]

Since 2017, the organization *Derechos Digitales* has periodically assessed how transparent internet service providers in Chile are about user data practices and how they respond to government information requests. Its most recent report

---

189 *ELT Group y DTS firmaron un acuerdo de cooperación en el sector de defensa electrónica en Chile y Sudamérica. - DTS® | Desarrollo de Tecnologías y Sistemas SpA.* Noticias DTS. December 20, 2024. URL

190 *ELT Group*, "Company Profile", URL

191 ELT Group (formerly Elettronica S.p.A.) maintains a close corporate relationship with CY-4GATE S.p.A.. It holds 38.38% of CY4GATE's stock capital and publicly identifies itself as the company's principal shareholder, positioning CY4GATE as part of the group focused on cyber intelligence and lawful interception. In ELT Group's institutional materials, CY4GATE is described as "part of the ELT Group, specialized in cybersecurity and cybernetic intelligence." The two companies also maintain internal collaboration agreements, including a joint R&D contract for more than €6.5 million, in which CY4GATE refers to ELT Group as its majority shareholder "Shareholding Structure and Share Capital," *CY4GATE S.p.A.*, consulted October 22, 2025, URL

192 One of those, pertaining to the "Chilean defense industry", states that DTS "develops, manufactures, and supports systems for the Armed Forces and law enforcement agencies in the areas of Command and Control, Electronic Warfare, and Communications." Zona Militar. "Industria de la Defensa de Chile - Empresas Autónomas del Estado, Filiales y Privados." January 21, 2019. URL

193 Peña, Cristóbal and Sebastian Minay. "Así se hacen los cuestionados 'pinchazos' telefónicos legales." Investigación. *CIPER Chile*, October 29, 2008. URL

was published in 2022. Overall, gradual improvements have been observed in privacy and transparency policies among Chilean telecom companies—Claro, Entel, Movistar, VTR, WOM, and GTD Manquehue—although none fully meets international data-protection standards or demonstrates a consistent, active defense of their users' digital rights. The report also underscores that, even in 2022, Chile's legal framework remains inadequate, particularly due to delays in updating Law 19,628 on personal data protection, leaving wide discretionary powers both to companies and to authorities requesting information. Some providers, including Claro and Movistar, have improved the structure and quality of their transparency reporting, adding more detail on information requests and denials. Others, however, continue with ambiguous or partial formats. This adds to the fact that most companies do not notify affected individuals when authorities request their data—except in rare cases. This lack of user notification is still one of the report's most persistent weaknesses.[194]

In 2014, Chile's *Carabineros* acquired the EGO communications interception system, developed by Italian firm Innova S.p.A., through Tecnodata–Mipoltec. The purchase coincided with the acquisition of spyware from Hacking Team. However, due to apparent issues related to contract design, and the distributor Mipoltec's procurement process, the system reportedly did not become operational at the time.[195]

Perhaps reflecting limitations in the distributor's role, the Italian company later established its own subsidiary in Chile—suggesting a more permanent commercial presence in the country. Innova Chile began operating around 2019 and has since participated directly in procurement processes related to interception platforms. In a tender process held the following year, Innova again competed for the contract—this time against another Italian firm, RCS Labs.[196] This suggests that the system may have remained operational in subsequent years. In 2021, the news outlet InfoDefensa reported that the Chilean Investigations Police (PDI) awarded Innova Chile a new lease for the EGO platform, covering maintenance, support, and system upgrades for the monitoring service over a 36-month period. A similar contract was later awarded to the Chilean Gendarmerie in 2023.[197]

According to an old promotional brochure dating back to 2011, EGO, by Innova S.p.A., was already an advanced lawful interception system of communications designed to capture, decode, reconstruct, and analyze a broad range of IP communications—including video calls, MMS messages, and emails—in compliance with standards set by the European Telecommunications Standards Institute (ETSI) for lawful interception. The system is deployed at strategic points within telecommunications networks—such as switches, routers, access nodes, or gateways—and receives copies of traffic selected by the operators (for example, traffic associated with a specific phone number or IP address). The system wor-

---

194 Michelle Bordachar, *¿Quién defiende tus datos?,* Santiago: Derechos Digitales - EFF, 2022. URL

195 Miranda, Ida, and Bárbara Partarrieu. "Carabineros pagó US$3,3 millones por equipo para 'pinchar' teléfonos: lo instaló y no funcionó." Investigación. *CIPER Chile*, February 12, 2015. URL

196 García, Nicolás. "Innova arrendará a la PDI de Chile el sistema de interceptación y monitoreo telefónico Ego." *Infodefensa - Noticias de defensa, industria, seguridad, armamento, ejércitos y tecnología de la defensa*, January 26, 2020. URL

197 Purchase Order N°634-748-SE23 "Mantenimiento soporte actualización Monitoreo EGO", URL

ks as an enhanced packet analyzer: rather than displaying individual packets in isolation, it reconstructs full sessions; it automatically categorizes data, such as incoming and outgoing calls, location, or sent emails; and it enables interpretative analysis. The system incorporates proprietary algorithms that digitally sign acquired data to ensure integrity, combining software, hardware, and architectural solutions. Finally, the brochure describes EGO as a tool supporting advanced data analytics, target location and tracking, directory management and mapping associations among users, and optimized investigative tools tailored for law enforcement operators. [198]

In 2018, the Public Prosecutor's Office purchased a version known as Vigía Elite or Vigía Elite Advanced for roughly US$1 million, as part of an effort to modernize its interception capabilities. [199] Implementation thereof, however, failed: it never became fully operational and later triggered investigations into fraud and irregularities. [200] The Vigía software is an interception, analysis, and geolocation platform acquired in Chile by the Investigations Police and the Public Prosecutor's Office for criminal investigations. [201] It is developed and supplied by Cognyte (previously part of the Israeli-U.S. conglomerate Verint Systems), a company specializing in surveillance and data analysis. [202] According to several sources, the system captures phone calls and SMS/MMS, analyzes data traffic linked to a target's identifier, and geolocates devices using information derived from mobile telephony antennas. [203] It also records and organizes metadata such as time, location, and participants of the communications. [204]

Given the concern surrounding the uses of lawful interception systems, this case is particularly significant. It points to the concrete deployment of equipment installed through formal legal channels, yet used in excessive ways stemming both from its own configuration and its technical possibilities. Even though its installation would likely have required cooperation from the specific internet service provider under established legal procedures, investigative reporting by Nicolás

---

198 "Innova_Product List, Specifications_MicroIP, EGO, Internet Interception and Probes, Gps Innova, RB800", 2011 URL

199 *La Tercera Sábado*, "Vigía Elite: El software del millón de dólares que complica a la Fiscalía," 2023, URL

200 *BioBioChile,* "La trama del Vigía: Cómo la Fiscalía tiró 1 000 millones a la basura en el proyecto estrella de Abbott," July 3, 2025. URL

201 *Interferencia*, "Vigía: El software con que la PDI trató de situar a Llaitul en atentados durante dos años," 2022. URL

202 Vigía is the local code-name for some of the LI products of Cognyte. Cognyte Software Ltd., *"Cognyte Software Ltd."* (Oslo: The Council on Ethics for the Norwegian Government Pension Fund Global, December 2022), URL

203 Verint describes its products RELIANT / VANTAGE as interception products. In corporate material, Verint describes its RELIANT /VANTAGE lines as suites for "intelligent recording and analysis solutions for communications interception activities for law enforcement" offered to law enforcement and security agencies. URL The corporate compendium also establishes that Reliant and Vantage are marketed to police forces and governmental agencies, including South America. URL

204 Fiscalía de Chile, "Fiscalía se capacita en software que analiza información derivada de interceptaciones telefónicas," 2020, URL

Sepúlveda documents testimony that vouches for its discretionary use. [205]

In addition, products marketed by US firm Pat Systems—particularly its Vortex AIT-Stack suite—combine IMSI catchers with an IP-network communications interception capability. The latter, the judicial monitoring system by PatSystems, is an interception platform that connects directly to telecommunications networks to capture both communications metadata and content, in line with ETSI and CALEA standards. [206]

In closing this section, two probable, yet unconfirmed, cases of acquisition and deployment are worth mentioning.

It appears that RCS Labs—another Italian firm that at one point acted as a reseller for Hacking Team—may also have played an intermediary role. The company, which specializes in lawful interception of communications and digital forensic analysis, has been referenced in international reports as being associated with, or conducting, commercial activity in Chile. However, there is no public evidence confirming operational deployments in the country. [207] RCS Lab's portfolio includes lawful interception platforms, mobile and fixed network monitoring systems, and data extraction from electronic devices, marketed for law enforcement and security agencies, and for telecommunication operators. Its presence in Chile should be regarded as plausible but unverified, and limited, according to the information available, to commercial outreach and negotiations. [208]

Lastly, while there are no public records confirming deployment in Chile of interception or surveillance systems developed by SearchInform Ltd., the Russian company does maintain commercial presence in the country through its local partner Techlaw, based in Santiago. More than interception of communications, its offering is oriented towards corporate data loss prevention (DLP), internal user monitoring, and cyber risk management. As a result, the likelihood that SearchInform may have deployed SORM-type state surveillance technologies in Chile seems remote. Still, the existence of commercial outreach and local representation points to at least a potential connection with the Russian security and data analytics market. [209]

---

205 The investigation of Nicolás Sepúlveda claims that Carabineros might have had access to Vigia, software used to organize and analyze interception-related data and communication records, including numbers, incoming calls, outgoing calls, their duration, and in some cases, data of the antennas used. While access to the above information is legal and regulated, in the case at hand, there would not have been the relevant authorization and such information would have circulated along informal channels. "Members of Intelligence admitted to CIPER that much of the wiretapping was illegal." Sepúlveda, Nicolás. "'Operación Huracán': la secreta casa donde se hacían centenares de escuchas telefónicas ilegales." Investigación. *CIPER Chile,* April 5, 2018. URL

206 Surveillance Watch, "PAT Systems." Accessed December 12, 2025.2025 URL

207 Feldstein, Steven, and Brian Kot. *Global Inventory of Commercial Spyware & Digital Forensics.* 2023. DOI

208 Lookout Threat Intelligence, *"Hermit Spyware Discovery,"* Lookout Inc., 2022, URL

209 SearchInform, "Partners – Latin America," consulted October 23, 2025, URL // International Coalition Against Illicit Economies (ICAIE), "How Russian Surveillance Tech Is Reshaping Latin America," September 12, 2024, URL

3.2.4. Network monitoring

In the telecommunications operators sector, Canadian company Sandvine reported contracts, as early as 2008, with Internet Service Providers (ISPs) in Brazil, Chile, and Colombia for its Policy Traffic Switch platform, designed for deep packet inspection (DPI), congestion management, and application analytics at the backbone level. [210]

VTR Chile S.A., one of the country's leading Internet and cable television providers, introduced a next-generation IP infrastructure (IP NGN) in the mid-2000s, with Cisco CRS-1 equipment at the core of its network. This operator-level architecture enables operators to measure, analyze, and manage network traffic through control systems that regulate network usage and enhance quality of service. [211]

More recently, in 2022, the firm VAS Experts reported that a major Chilean internet provider had incorporated the firm's carrier-grade NAT (CGNAT) system. This type of software allows many clients to share a single public address while simultaneously recording how traffic travels through the network, giving operators detailed visibility into connection usage and performance. [212]

For its part, Entel—one of the country's largest providers—has consolidated part of its cybersecurity infrastructure around Palo Alto Networks, integrating next-generation firewalls (NGFW), intrusion detection (IDS/IPS), and coordination at its corporate Network Operations Center/Security Operations Center (NOC/SOC). Despite having been designed as security solutions, these tools enable continuous traffic monitoring and comprise the technical core of network observability and control for large-scale Chilean providers. [213]

As noted, the deployment of network monitoring and management technologies by Chilean ISPs—such as deep packet inspection (DPI), filtering policy controls, carrier-grade NAT (CGNAT), and next-generation firewalls (NGFW) integrated into operators' networks—is justified on the grounds of necessary traffic management, IP range efficiency, and network security. At the same time, these tools also enable granular observability of user behavior. This capability allows distinguishing applications, prioritizing flows, or identifying consumption patterns and, in the absence of adequate safeguards, could be repurposed for commercial or state surveillance. This raises significant questions about privacy and transparency.

For example, in Chile, Law No. 20,453 consecrates the principle of network neutrality for Internet users. That means providers cannot "arbitrarily block, interfere with, discriminate against, hinder, or restrict" the lawful use of content,

---

210 Light Reading, "Sandvine Touts LatAm Success," 2008. URL

211 Cisco Newsroom, "Chile's VTR First in Latin America to Deploy IP NGN with Cisco CRS-1," July 17, 2006.

212 VAS Experts, "CG-NAT Solution for Saving IPv4 Address Space — A Case Study," April 6, 2022.

213 Palo Alto Networks, "Modern Managed Cybersecurity Services in Chile: Entel Case Study," 2024; *ANDA Chile,* "Palo Alto Networks eleva a Entel Ocean a su máxima categoría de partner," November 8, 2022.

services, or applications. This establishes a regulatory framework intended to protect users' equal access and privacy against arbitrary provider decisions.[214] However, the framework—in its current wording and as it has been implemented to date—does not impose any general public obligation that requires Internet service providers (ISPs) to disclose, in technical detail, which management mechanisms they use; how they configure any traffic inspection or prioritization systems; what kinds of metadata they keep; or for how long traffic records are stored. This regulatory gap opens up a gray area regarding actual network management practices. Thus, even if network neutrality sets boundaries—by prohibiting arbitrary blocking and discrimination—there remain structural risks that traffic-management technologies designed for quality maintenance may be used extensively or improperly for monitoring, prioritizing, or filtering, without users having reliable means of knowing it. This regulatory control deficit warrants concerns about potential violations of privacy rights, freedom of communications, and transparency within the telecommunications ecosystem.[215]

Likewise, institutional controls are still weak. Although Chile's personal data protection regime (Law No. 19,628) grants users certain rights, there is still no fully operational specialized authority with strong supervisory and sanctioning powers over how ISPs process personal data. This means that, even when corporate network monitoring tools have been acquired, there is not always public evidence of independent audits, operators' transparency reports, or accessible user grievance mechanisms on the uses of these systems.

3.2.5. OSINT

An investigation conducted by newspaper Haaretz reported that Israeli company Cognyte reportedly supplied the Chilean Army with active open-source intelligence (OSINT) equipment. Cognyte was also cited in Meta's report on the surveillance industry published in December 2021. The company reportedly used fake avatars as part of an active, offensive, targeted OSINT phase. According to the company, the avatars were used to monitor and collect information about journalists in several countries, including Chile. The reporting suggests the system works by building profiles that pull social media data associated with any given phone number. Once assembled, that information can be used to craft highly tailored phishing campaigns. In other words, this would not amount to passive OSINT collection. It would be rather an active operation to obtain data.[216]

---

214 Law 20.453, "Consagra el principio de neutralidad en la red para los consumidores y usuarios de Internet", amending the General Telecommunications Law, sections 24 H, 24 I and 24 J. See: Biblioteca del Congreso Nacional de Chile, text of the law. URL

215 "Chile's ISPs have over the last five years improved transparency about how they protect their users' data, thanks in large part to Derechos Digitales ..." Informe "¿Quién defiende tus datos?", quoted in EFF, 2022. URL // Veridiana Alimonti, *Who Defends Your Data in Latin America & Spain? A Comparative View of Telecom Companies' Commitments to User Privacy* (San Francisco: EFF, March 2023), URL

216 Benjakob, Omer, and Phineas Rueckert. "Fake Friends: Leak Reveals Israeli Firms Turning Social Media into Spy Tech." National Security & Cyber. *Haaretz,* February 28, 2023. URL

In 2024, Chilean Investigations Police (PDI) awarded the acquisition of an "OSINT-type software with image-based search" to Servicios Profesionales UP SpA, for an estimate of Chilean Pesos 252,000,000 (about USD 267,000). The contract is about the acquisition of licenses of the Clearview AI type, intended to strengthen the agency's operational capabilities of reverse image search and facial recognition through open-source analysis. This purchase stands out as one of the earliest documented instances of explicit adoption of OSINT technologies by any Chilean security force for criminal investigation and cyber-intelligence.[217]

Furthermore, the newspaper La Tercera reports that Chile's *Carabineros* maintains within OS-9 a team specialized in "cyber-patrolling" to detect threats on social media platforms. A spokesperson for OS-9, Lt. Javiera García, told the newspaper that the unit "constantly carries out online monitoring or virtual patrols, reviewing multiple social networks. When a comment directly signals the intent to seriously harm someone—for example, 'I'm going to kill you'—an alert is triggered," categorizing the message as a threat to be assessed and investigated together with the Public Prosecutor's Office. According to the same reporting, analysis of social-media interactions may also help investigators identify contacts and associations linked to the monitored individual; this information can then be cross-referenced with additional data sources, such as criminal-record databases, to determine whether the scope of the investigation should be expanded. OS-9 representatives also acknowledged monitoring online activity associated with groups and collectives—including soccer fan clubs, anarchist groups, and feminist organizations—in connection with potential public-order or criminal investigations.[218]

More recently, official minutes of the hearings on the Lobby Act Platform show that Chilean company SAT Internacional presented Tucán, a product developed by Israeli firm Prelysis, as an OSINT platform designed to centralize all monitoring of social media and instant messaging in a single environment, with capabilities to "de-anonymize" users and messages—explicitly referencing platforms such as Telegram, Threema, WhatsApp, Zalo, and Imo—. Alongside these there are modules for digital footprint detection, AI-powered image analysis and facial recognition, online forums and dark net monitoring, link analysis, and big data operations. At a subsequent hearing, the company explicitly incorporated the ability to conduct targeted searches within "data leaks".[219]

Also, Chilean company Black Up SpA markets Babel Street in the country—a risk intelligence platform aimed at public sector and private clients. It combines collection and analysis of digital information for threat detection, risk assessment, and identity resolution. The suite includes OSINT/SOCMINT-like

---

217 "Adquisición de software tipo OSINT con búsqueda a través de imágenes (5890-36-LQ24)," *todolicitaciones.cl*, consulted October 30, 2025, URL

218 Rivera, Victor. "El Desconocido 'Ciberpatrullaje' de Carabineros En Las Redes Sociales." *La Tercera* (Santiago de Chile), August 28, 2018. URL

219 Lobby Law platform (Chile), Chile's Navy, "Audiencias - Año 2024 - Marco Villegas Zanón," Identifier AD007AW1685110 (October 22, 2024), URL / Lobby Law platform (Chile), Chile's Air Force, "Audiencias - Año 2025 - César Pineda," Identifier AD008AW1742130 (March 12, 2025), URL / Buitrago, Leonardo. "Empresa israelí ofreció 'Tucán' a Armada y FACh: actas consignan promesa de 'eliminar el anonimato' en WhatsApp y Telegram." *El Ciudadano,* August 27, 2025. URL

capabilities, plus text analysis, alongside modules for mapping entities and relationships and investigative tools.[220]

Beyond the intelligence, security, and defense sector, other public bodies have also adopted open-source monitoring capabilities. Chile's Electoral Service (SERVEL) issued an invitation to tender for a social media management and monitoring platform aimed at improving the public perception of its performance and strengthening institutional communications. According to its own website, the agency uses consumer intelligence and social media analytics software to collect and systematize publicly available information, with the goal of detecting election-related disinformation.[221] Adding to this, the Commission for the Financial Market (CMF) has likewise issued an invitation to tender services to monitor social media, websites, and online news outlets. In a separate process, the same agency sought specialized cybersecurity services that include cyber surveillance, cyber intelligence, and threat hunting. The foregoing points to a risk-management and incident-response approach that draws on threat-intelligence inputs. In CMF's case, the stated objective is to use AI- and natural language processing–based social listening tools to track public conversations across social networks and digital media, in order to identify trends, perception, and potential communications risks that could affect either the financial system or the institution itself.[222]

220 Babel Street, "Text Analytics and Identity Intelligence Solutions (Modules)," in URL

221 Chile's Electoral Service, "Servicio de plataforma de administración y monitoreo de redes sociales del Servicio Electoral," bidding cover sheet (Santiago, 2025), ID 5155-14-LE25. URL

222 Commission for the Financial Market (CMF), "Servicio de monitoreo de redes sociales, sitios web y medios online," bidding cover sheet (Santiago, 2023/2025). URL // CMF, "Contratación de herramientas y servicios especializados de ciberseguridad (incluye monitoreo de ciberseguridad, threat hunting, cibervigilancia y ciberinteligencia)," bidding cover sheet ID 1005498-21-LR25 (Santiago, 2025).URL

Table 3: Summary — Chile

CHILE				
Tool	Company	Distributor	Product / Technology	Acquisition
Spyware	**Hacking Team (Italy)**	Tecnodata - Mipoltec / RCS Lab	Remote Control System (Phantom / Galileo)	Confirmed by the 2015 leaks.
	NSO Group (Israel)		Pegasus	Documented in CyberPeace Institute dataset (alleged use)
SIGINT	**Almenta Group (US)**		Dominator - Captur (*IMSI catcher*) / Observer (SS7-Diameter Signaling Interception)	Likely. Reported in Privacy International documentation
	NSO / Circles (Israel)		SS7/Diameter exploitation	Confirmed (Citizen Lab 2020)
	ELT Group / Cy4gate (Italy)	DTS	*IMSI catcher*	Medium to high probability
	RCS Labs (Italy)		IMSI Catcher / SS7 exploitation	Low probability
	Pat Systems (US)		IMSI Catcher / SS7 exploitation	Very likely
	Rohde & Schwarz (Germany)	DYMEQ Ltda.	*IMSI catcher* / *Direction Finder*	Likely

CHILE				
Tool	Company	Distributor	Product / Technology	Acquisition
Network intelligence	**Innova S.p.A. (Italy)**	Mipoltec / Innova Chile	EGO	Confirmed
	Verint / Cognyte (Israel)	Grupo Zeuz / RightCom	Vigía	Very likely. Documented procurement (implementation disputed / partially failed)
	Pat Systems (US)		IP network interception	Very likely
	ELT Group / Cy4gate (Italy)	DTS	Cy4gate LI	Medium to high probability
Network monitoring	**Blue Coat (US)**		PacketShaper	Confirmed
	Sandvine / Procera (Canada)		Policy Traffic Switch, PacketLogic	Confirmed
	CISCO (US)		IP NGN architecture	Confirmed
	Allot (Israel)	ENTEL	ContentSecure, MailSecure, WebFilter, Service Gateway, Deep Packet Inspection (DPI)	Confirmed. Mentioned in Annual Report 2014 by Allot Communications.
	VAS Experts (Netherlands)		Stingray Service Gateway (DPI / CGNAT service-gateway platform)	Confirmed. In 2022, the company claims to have premises in Chile.
	Palo Alto Networks (US)		NGFW / SOC orchestration	Confirmed

CHILE				
Tool	**Company**	**Distributor**	**Product / Technology**	**Acquisition**
OSINT	**Prelysis (Israel)**	SAT Internacional S.A	Tucán	Very likely
	Verint / Cognyte (Israel)	Grupo Zeuz / RightCom	Active OSINT surveillance / Analytics/ data fusion for investigation	Confirmed
	ELT group / Cy4gate (Italy)	DTS	Cy4gate OSINT	Probable
	BabelStreet (US)	Black-up SpA	Risk intelligence / SOCMINT	Very likely
	IBM (US)	Xmartlab	i2 Analyst's Notebook and also i2 iBridge	Confirmed
	Clearview	Black-up SpA / Servicios Profesionales UP SpA	Facial recognition OSINT	Confirmed

CHILE				
Tool	Company	Distributor	Product / Technology	Acquisition
Forensic extraction and analysis	**Cellebrite (Israel)**	IAFIS group (IAFIS Chile) / Black-up SpA	UFED	Confirmed
	Toka Group (Israel / Mexico)		Forensic extraction	Likely
	Oxygen (US)	Xmartlab / Digitoforense SpA.	Oxygen Forensic Rugged Kit	Confirmed
	MSAB (Sweden)	Digitoforense SpA.	Mobile device extraction	Confirmed

CHILE				
Tool	Company	Distributor	Product / Technology	Acquisition
Video-surveillance / Biometrics/Facial recognition	**Clearview AI (US)**	Black-up SpA / Servicios Profesionales UP SpA	Facial recognition	Confirmed
	Verint / Cognyte / Intellicene (Israel)	Grupo Zeuz and RightCom	Facial recognition ("FaceDetect" / Nextiva Video management / VMS (CCTV IP)	Confirmed
	NEC (Japan)	NEC Chile S.A.	Facial biometrics	Confirmed
	Dahua Technology (China)	SSTT SpA (Chile) / Dahua Technology Chile SpA		Confirmed
	Luxriot / VisionLabs (Russia)	Rustec (Chile)		Confirmed
	AnyVision / Oosto (Israel)		Better Tomorrow	Confirmed
	Hikvision (China)			Confirmed
	Huawei / ZTE (China)		Videosurveillance infrastructure	Confirmed
	Veridas (Spain)		Digital identity	Confirmed
	Jumio (US)		Identity verification	Confirmed
	IDEMIA / Morpho (France)		Identification systems	Confirmed

4. Uruguay
4.1. Context

Turning to Uruguay, the country initially appears to present a less contentious surveillance landscape than Argentina or Chile—largely removed from major procurement scandals involving international vendors, with governments less inclined to publicly dramatize security policy and a stronger tradition of civil society participation in public policymaking. Patterns of social protest also appear comparatively less intense. Uruguay is, moreover, a country of fewer than three and a half million residents, compared to nearly twenty million in Chile and roughly forty-five million in Argentina. This requires adjusting the analytical scale of comparison. There are substantial differences in size and in the origin of the technological packages adopted; however, day-to-day operational practices do not appear substantially different from those of its neighbors.

Uruguay enters today's surveillance conversation with comparatively strong institutions and constitutional protections regarding privacy and freedom of expression, underpinned by Law No. 18,331 on Personal Data Protection and Law No. 18,381 on Access to Public Information.[223] From 2016 onward, however, several assessments were already warning that—even where this legal framework enables oversight and transparency—real-world operation of that framework could be less than uniform and transparent. An initial report published that year highlights that there is no legal obligation for mass retention of data; however, some operators retain it voluntarily, without rules requiring notification to users.[224]

The new Code of Criminal Procedure (Law 19.293) and, above all, Law 19,696—regulating the National State Intelligence System—redefined the institutional landscape.[225] Critical analyses, such as those by Datysoc, note that the definition of "police intelligence" remains legally ambiguous and that the boundaries between prevention, criminal investigation, and intelligence activities are blurred. This ambiguity facilitates the extension of surveillance techniques into domains where stronger safeguards would normally apply. They also warn that the legal framework does not clearly distinguish between "open sources" and social-media intelligence (SOCMINT), with important implications for expectations of privacy in digital environments.

The assessments produced by Datysoc—a pioneering civil society organization in the country on these issues—are worth following. Since 2020, the so-called 'cyber-patrolling'—preventive monitoring of digital spaces—has gained prominence as a policing practice. In its report, Datysoc documents that there is no

---

223 República Oriental del Uruguay, *Ley Nº 18.331, Protección de Datos Personales y Acción de Habeas Data* (published D.O. August 18, 2008), IMPO. URL // República Oriental del Uruguay, *Ley Nº 18.381, Derecho de Acceso a la Información Pública* (published D.O. November 7, 2008), IMPO/URCDP. URL

224 Scrollini, Fabrizio, Ana Tuduri, and Katitza Rodríguez. *State Communications Surveillance and the Protection of Fundamental Rights in Uruguay* (2016). 2016. URL

225 República Oriental del Uruguay, Ley Nº 19.293, Código del Proceso Penal (enacted 2014), IMPO. // República Oriental del Uruguay, Ley Nº 19.696, *Aprobación y regulación del Sistema Nacional de Inteligencia de Estado* (enacted October 29, 2018), IMPO/SIEE. URL

specific regulation or publicly available protocols governing OSINT/SOCMINT activities; that the Prosecutor's Office admits to using it occasionally (including for the possible creation of undercover profiles); and that clear rules are lacking regarding necessity, proportionality, chain of custody, and judicial accountability.[226]

Opacity further aggravates the situation. The Ministry of the Interior has been criticized for withholding information requested under Law 18,381. The *Unidad de Acceso a la Información Pública* (UAIP, Access to Public Information Unit) has recently issued rulings recognizing that the Ministry failed to comply with deadlines. Meanwhile, Datysoc obtained a favorable court ruling to obtain information on cyber-patrolling practices that the Ministry had withheld.[227] Even when the Ministry's own 2020 Annual Report admits having incorporated network analysis software—UCINET—for the National Observatory on Violence and Criminality, the Ministry declared the secrecy of purposes and usage protocols.[228] In parallel, the Ministry moved forward with a reorganization of its data unit. In July 2025, an *Área de Estadística y Criminología Aplicada* (AECA, Statistics and Applied Criminology Area) was introduced, alongside its Advisory Council, with the promise to professionalize production and use of evidence in public security.[229] As a result, it has not been possible to determine the scope of cyber-patrolling or which tools are being used with certainty.

The Ministry of the Interior stands out among the agencies with the highest levels of noncompliance with the Public Access to Information Law. It records one of the lowest scores in Uruguay's transparency ranking and is the object of the largest number of lawsuits from civil society on this matter. Two recent lawsuits resulted from the Ministry's refusal to respond to requests concerning records of various police procedures, as well as its refusal to provide information about facial recognition software acquired. Likewise, implementation of a facial recognition system for police use reportedly is already underway, even though no specific regulations or public protocols exist to provide safeguards for its use.

These developments have received comparatively less media attention, but they are far from trivial: adoption of data protection and access-to-information laws; incorporation and operation of an interception system with OSINT-related capabilities; legal reforms to the criminal procedure; expansion of cyber-patrolling practices without specific rules; and the creation of internal analytical units.

Nevertheless, the country's participatory institutional tradition, together with a less pronounced pattern of political fluctuation than that observed in neighboring countries, creates conditions conducive to the development of institutional safeguards. Within the framework of the Sixth Open Government Action Plan (2025–2029), the Ministry of the Interior convened civil-society organizations

---

226 Díaz Charquero, Patricia, and Jorge Gemetto. *Ciberpatrullaje: Los Límites Borrosos de La Vigilancia Policial En Uruguay.* Montevideo. Datysoc, 2022. URL

227 Díaz Charquero, Patricia, and Jorge Gemetto. *Ciberpatrullaje: Los Límites Borrosos de La Vigilancia Policial En Uruguay.* Montevideo. Datysoc, 2022. URL // Unidad de Acceso a la Información Pública (UAIP), Resolution 2521/2025. URL

228 Ministerio del Interior, *Memoria 2020* (quoted in Datysoc): UCINET acquisition for the Observatory; purposes/protocols declared secret.

229 Ministerio del Interior, "Ministerio del Interior presenta el Área de Estadística y Criminología Aplicada (AECA)", July 1, 2025. URL // Presidencia – Uruguay, "Ministerio del Interior diseñará política pública en seguridad basada en evidencia" , July 1, 2025. URL

to advance the creation of a "Multisector Roundtable on the Regulation of Police Surveillance Technologies and Digital Evidence." This initiative—currently under development—aims to establish clearer regulatory criteria, including standards of necessity and proportionality, as well as mechanisms of democratic oversight over OSINT/SOCMINT practices, facial-recognition systems, and communications-interception technologies. As of November 4, 2025, the commitment remained at the draft stage and formalized a multi-stakeholder working group tasked with producing guidelines and public protocols.

BOX 13: Some firms worth looking into

- **Teleimpresores S.A.** (Uruguay) is a Uruguayan technology and security firm that markets products and services ranging from CCTV systems, alarms, access control, and telephony to security systems services. Between 2010 and 2011, the company also supplied telephone interception equipment acquired through Uruguay's State Procurement Portal. Also for the early acquisitions, the firm acted as an intermediary in the purchase of the Brazilian system Intellotum - El Guardián.
- **Aeromarine S.A.** appears in official regulations (URSEC) as the exclusive representative in Uruguay for equipment manufactured by Rohde & Schwarz, a brand covering radiomonitoring and radiolocation instrumentation and solutions.

4.2. Demand / Solutions

4.2.1. *Spyware*

As elsewhere in the region, in May 2014, executives from Italian firm Hacking Team—Alex Velazco and Sergio Solis—traveled to Montevideo to pitch their Remote Control System (RCS)—also marketed under names Da Vinci, Galileo, and Phantom—to Uruguayan security officials. The internal emails leaked in 2015 showed they held separate meetings with the then National Police Director Julio Guarteche and State Intelligence Coordinator Ramón Bonilla.[230] In their own records, the executives mention presentations using "infected devices," a highly favorable reception, and assurances from local counterparts that they would apply political pressure in favor of the acquisition. The same documents depict RCS as a tool capable of stealthily infecting target devices, extracting content, and remotely activating microphone and camera.[231]

In parallel, a 2016 report prepared for Electronic Frontier Foundation (EFF) documented that the intermediary company involved in the negotiations appears to have been the Paraguay-based firm Radar S.A. and highlighted the absence of specific legal rules governing device-infection tools. That regulatory gap, the

---

230 "WikiLeaks - The Hacking Team Archives." 2015. URL // Solis, Sergio, "Paraguay-Uruguay Report". July 8, 2015. Wikileaks. URL

231 Gonzalo Terra, "Gobierno de Mujica sondeó compra de más equipos de espionaje," *El País* (Montevideo), July 10, 2015. URL

report argued, makes it difficult to assess the legality, necessity, and proportionality of such capabilities against international standards. [232]

After the leak, the then Minister of the Interior, Eduardo Bonomi, confirmed that the ministry had reviewed Galileo spyware, but said it was ultimately rejected as "too invasive." In the same remarks, he defended the newly acquired network interception platform, El Guardián, as a surveillance tool "with safeguards," drawing a distinction from the use of intrusive malware. The official position further maintained that, following Hacking Team's presentation, no negotiations were pursued over Galileo.[233]

Years later, the weekly publication Búsqueda reported that the Ministry of the Interior had reportedly received a proposal to acquire Pegasus, developed by NSO Group, as part of a broader set of international offers intended to "replace" or "upgrade" existing interception capabilities.[234] The article noted that, at the time of publication, no final decision had been made and the evaluation process was still ongoing. Soon afterwards, Uruguay's Unidad Reguladora y de Control de Datos Personales (URCDP—the data protection authority—) issued Resolution No. 30/021 (12 August 2021) in response to an access-to-information request seeking any documents mentioning NSO Group, Pegasus, or a potential spyware purchase. The authority replied that no such information existed.[235] From the standpoint of public traceability, the above points to negotiation over, and evaluation of, state-grade "mercenary" spyware, without any open evidence of purchase or operational deployment.[236] It is worth noting that one of NSO Group's regional representatives, Martín Berenstein, is Uruguayan. He has participated in regional product presentations. In this regard, it is worth mentioning as well that public statements by some security officials have expressed interest in acquiring such tools.

---

232 Fabrizio Scrollini, Ana Tudurí and Katitza Rodríguez, *Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Uruguay*, Electronic Frontier Foundation, 2016. URL

233 "Bonomi: 'Descartamos la compra de El Galileo porque es invasivo'," *El País* (Montevideo), July 16, 2015. URL

234 "Ministerio del Interior recibió oferta para adquirir software espía Pegasus," *Caras y Caretas,* July 23, 2021. URL

235 Unidad Reguladora y de Control de Datos Personales, Resolution Nº 30/021 (August 2, 2021). URL

236 Juan Francisco Pittaluga, "El Ministerio del Interior recibió propuesta para obtener Pegasus, el software israelí usado en presunto espionaje ilegal," *Búsqueda*, July 21, 2021, consulted November 3, 2025, URL

4.2.2. SIGINT

There is no publicly available evidence—whether in legislation, procurement records, court rulings, press reporting, or technical disclosures—confirming the acquisition or operational deployment of IMSI catchers by Uruguayan agencies. Local media references describe IMSI catchers as "possible" technologies, without proving acquisition.[237]

Companies reported to be operating across the region—Pat Systems, Almenta Group, Titan/Titan-Geo, among others—advertise IMSI catchers and offer their products to governments throughout Latin America. However, no contracts or deliveries have been identified in Uruguay.

Regarding documented geolocation requests through exploitation of the SS7 signaling, Mobile Surveillance Monitor platform reports more than 8,000 incidents categorized as "IMSI Identity Disclosure / sendRoutingInfoForSM (SRI-SM) / 3G" attributed to CTI/AM Wireless Uruguay, the corporate name of Claro Uruguay. This indicates SS7 activity aimed at obtaining the IMSI of Uruguayan subscribers via SRI-SM requests. This is a legitimate signaling procedure in 2G/3G core networks, but when misused, it allows retrieval of the target's IMSI and associated MSC information. Even without confirmation, a credible risk of SS7/Diameter exploitation can be inferred from the volume of anomalous SRI-SM activity targeting the Claro network attributed to private or state actors in other countries in the region.[238]

The system available in Uruguay with these capabilities is EGO by Innova S.p.A., which is also operational in Chile. This suite was acquired in 2024 and is reportedly used by the *Dirección General de Represión al Tráfico Ilícito de Drogas* (General Directorate for the Suppression of Illicit Drug Trafficking). Innova's EGO tools enable monitoring of telephony communications and integrate multiple real-time surveillance capabilities. Its geolocation capabilities through the use of the SS7/Diameter protocol were described by the officials involved in the acquisition as follows: "Among its main functions are the geolocation of mobile devices—including map-based visualization—the sending of silent SMS messages to track targets without their knowledge, and the generation of audible alerts triggered by predefined events." This description is drawn from a document of the Italian Public Prosecutor's Office to which the newspaper *Búsqueda* had access.[239]

---

237 Marina González, "Secretos a la luz", *La Diara*, 2025, URL

238 M. Cappellari, *Detecting SS7 Attacks in the Telecommunication Networks*, Aalborg University, 2025. URL

239 Pittaluga, Juan Francisco. "Carlos Negro sobre la necesidad de comprar nueva tecnología de interceptación: 'El Guardián pasó de moda.'" *Búsqueda,* July 10, 2025. URL

4.2.3. Network Intelligence

Following a legislative information request, the Supreme Court of Justice reported that between 2009 and March 2014 criminal court judges had ordered more than 6,000 telephone interceptions—an average of nearly three per day—without uniform transparency standards governing their use.[240] Records from the public procurement bidding system indicate that one of the companies providing this type of service was Teleimpresores S.A.

At least initially, this company also acted as an intermediary in the acquisition of Brazilian system Intellotum – El Guardián, from Dígitro Tecnologia Ltda. In 2014, the purchase was presented as a solution to unify interception activities that, in practice, operated in a disorganized manner. The Ministry of the Interior in fact argued in favor of the tool for its oversight capabilities, and in December of that year the Supreme Court authorized its operation.[241]

In parallel, multiple tender processes were launched for developing and maintaining the *Sistema Automatizado de Interceptaciones Legales* (SAIL—interface for the management of lawful interceptions—). Public procurement bidding specs and technical annexes describe SAIL as a system that automatizes generation, signature, and transmission of court orders to telecommunications operators, and centralizes the flow of approvals, denials, and types of measures (wiretapping, information, historical data, traffic, etc.).

In this way, the operation of El Guardián in conjunction with SAIL is governed by a memorandum signed by the Prosecutor's Office, the Judiciary, and the Ministry of the Interior: the police forces request a measure, the Prosecutor's Office reviews it, and the judge authorizes or denies it; the order is then transmitted through SAIL to the telecommunications operator, which validates the judge's digital signature and feeds the traffic to El Guardián, where it remains stored and made available for the investigation.[242]

According to media coverage at the time, Intellotum – El Guardián was capable of intercepting up to 800 mobile phones and 200 fixed lines simultaneously, besides creating up to 100 email mirror accounts, and monitoring social networks.[243] These capabilities expanded over time.

The Ministry of the Interior, in fact, maintained and expanded the platform. In 2019, it allocated around $65,000 to extend its capabilities. It also emphasized that development had been carried out by Dígitro Tecnologia Ltda. 'tailor-made'

---

240 Fabrizio Scrollini, Ana Tuduri, and Katitza Rodríguez, "Vigilancia de las Comunicaciones del Estado y la Protección de los Derechos Fundamentales en el Uruguay (2016)", *Necessary and Proportionate, March 2016.*

241 "El Guardián: el nuevo vigilante que compró el gobierno", *El Observador,* March 4, 2015. URL / "El sistema 'El Guardián' quedó habilitado; protocolo firmado por Fiscalía, Interior y SCJ", En Perspectiva, December 2, 2015, URL

242 "'El Guardián': así funciona el sistema de escuchas telefónicas del Ministerio del Interior", *Subrayado,* November 21, 2022. URL

243 "Justicia avaló cerrojo en torno a 'El Guardián'; apelarán el fallo", El País, March 14, 2015; "Gobierno compró 'El Guardián' para espiar llamadas y redes sociales", *Subrayado,* July 26, 2013.

for the Ministry of the Interior.[244] In 2022, Tribunal de Cuentas (the state's supervisory agency) authorized the use of more than one million dollars—through a direct acquisition process classified as 'secret'—for new functionalities of El Guardián. In November 2024, the Presidency also recorded an official mission to visit Dígitro, identified there as the "supplier of the Guardián On-line System", confirming the platform's technological continuity.[245]

El Guardián was, above all, a centralized lawful interception (LI) system operating under judicial authorization that connects the police, the Prosecutor's Office, the courts, and the operators to intercept communications (fixed telephony, mobile telephony, and messaging) within criminal proceedings. This was how the government itself presented it, specifying that "only the competent judge holds the digital key" to enable its use.[246]

That said, over time the various capabilities of El Guardián turned it into a more encompassing system with expanded functions (e.g., the creation of email mirror accounts and the monitoring of posts on social networks). Even when used within the framework of court orders in court proceedings, these functions push the limits of lawful interception and enter the domain of OSINT and digital surveillance of open information. Its functional core is seemingly lawful interception, but it incorporates modules that enable tasks akin to OSINT when it comes to observing and analyzing online public content.[247]

---

244 "Compra por Excepción 17/2019. Proveedor Digitro Tecnología Ltda. para 12 unidades". URL

245 "Tribunal de Cuentas autorizó compra secreta de nuevas funcionalidades de El Guardián", *Montevideo Portal,* November 14, 2022. // Presidencia — Gub.uy, "Resolución S/N/024: participación de Hugo Darío Imas Charlin en la visita a la empresa DIGITRO TECNOLOGÍA (TELEIMPRESORES S.A.), proveedora del Sistema Guardián On-line", November 1, 2024.

246 Presidencia de la República (Uruguay), "Solo el juez competente tiene la llave digital para autorizar uso del sistema Guardián," March 13, 2015.

247 *El Observador,* "Ministerio del Interior afirma que pondrá en marcha los controles de El Guardián," July 9, 2019. URL // *Necessary & Proportionate,* "Vigilancia de las comunicaciones del Estado y la protección de los derechos fundamentales en el Uruguay," March 2016. URL // *UyPress,* "¿Qué es el Guardián?," March 9, 2015. URL

Indeed, according to the diagram of the Guardião platform (Dígitro), the system involves more than telephone interception and voice recognition/transcription. The manufacturer presents it as a modular intelligence and investigation ecosystem that integrates operations management and capture from multiple data sources, data analysis and fusion, monitoring of public information, financial intelligence, facial-recognition and biometric databases, georeferencing, and secure collaboration. While actual deployments may correspond to only a subset of modules depending on the client, the vendor's advertising makes it clear that the Guardião is a broad suite under continuous development.[248]

The timeline thus reflects a shift from a fragmented interception regime to a centralized one, followed by sustained expansions in capabilities—yet marked by a significant degree of opacity regarding disclosure of usage and control data.

Journalistic investigations have documented some abuse risks, ranging from the political use of information obtained through interceptions, to the selling of sensitive data, to internal control issues—such as the shared use of user ID and passwords between the Intelligence Directorate and the Counterterrorism Department.[249]

In this regard, the two private mobile operators are integrated into the same lawful-interception ecosystem as Antel. Movistar Uruguay publishes a "Protocol for Data Handover to Competent Authorities" explaining that most judicial requests reach the company through the SAIL interface (Sistema Automatizado de Interceptaciones Legales), which interoperates with the El Guardián platform. According to the document, both systems are provided by the Ministry of the Interior and are interconnected with the infrastructures of Uruguay's

---

248 "Plataforma Guardião: Solução para Segurança Pública | Dígitro." *Dígitro Tecnologia,* consulted October 1, 2025. URL

249 Garat, Guillermo. "Escándalo Uruguay: de pasaportes rusos a espiar opositores." *AP News,* November 30, 2022. URL

three telecommunications operators.[250]

In addition, in 2024, Uruguay reportedly acquired the EGO system from the Italian company Innova S.p.A., through its distributor in Chile.[251] The reported cost was €250,000. As a modular and scalable platform, however, it is difficult to determine which specific capabilities were included in the acquisition. EGO is designed as a lawful-interception and monitoring platform supporting multiple communication channels—including fixed and mobile telephony, IP traffic, email, MMS, and video communications—as well as conversation recording, metadata processing, and geolocation functions. The system also incorporates repositories with timestamping and digital-signature mechanisms to ensure evidentiary integrity, along with case-management, user-management, and centralized audit features. According to vendor descriptions, the platform can further integrate with external systems through APIs, including formats associated with OSINT workflows.[252] Available information does not allow us to determine whether EGO also operates through SAIL.

4.2.4. Network monitoring

Uruguay is the only case analyzed in which public documents refer relatively directly to the existence of deep packet inspection (DPI) within the state-owned operator.[253] A policy document explicitly mentions the need to "legislate on the proper use of the devices that Antel already possesses for inspection of communications among citizens". The same document highlights "deep packet inspection (DPI) technology" as a risk to the protection of personal data. At a minimum, the issue appears in the political platform of a senator and a provincial candidate in 2015: "To strengthen the personal data protection act, guarding data against deep packet inspection (DPI) technology. To legislate on the proper use of the devices that Antel already possesses for inspection of communications among citizens."[254]

---

250 According to an investigation of journal *Sudestada* on SAIL, the system was designed to digitally process interceptions, and under the 2015 protocol, the Ministry of the Interior and the three telephone operators (Antel, Movistar and Claro) had to report, on a quarterly basis, any interceptions conducted because such interceptions are deployed within their own networks. *Sudestada.* "Sudes Ministerio Del Interior Omitió Informar a SCJ Por Casi Cuatro Años Sobre Intervenciones Telefónicas Tada." August 31, 2019. URL

251 Pittaluga, Juan Francisco. "Carlos Negro sobre la necesidad de comprar nueva tecnología de interceptación: 'El Guardián pasó de moda.'" *Búsqueda,* July 10, 2025. URL

252 This according to Innova's technical manual (2011) and based on secondary sources describing EGO as a tool that "enables to intercept, decode and restore on the same interface all types of IP communication, such as Video-communications, MMS..."URL

253 There is in fact long-standing, yet clear-cut, evidence of DPI-type traffic management in an ISP. By the mid-2000s, users of Dedicado (wireless/fixed ISP) reported strong filtering of P2P traffic. A technical analysis published in 2006 described that P2P traffic was being filtered through Packeteer equipment (the "Packeteers") installed on the network central router, identifying and limiting P2P traffic following a time schedule so as to avoid saturating international connection. Packeteer was precisely one of the most popular DPI/traffic shaping commercial solutions of those days, later taken over by Blue Coat. URL

254 "Tecnología de la Información y las Comunicaciones - Senador Dr. Pedro Bordaberry", URL

Official documents from Antel as early as 2010 suggest that DPI capabilities were already present in its mobile core network, thereby avoiding the need for "additional probes".[255] The information does not identify the manufacturer, but it makes it clear that deep packet inspection is located within the core network, where traffic policies, application classification, and traffic management are applied.

Planning documents from Uruguay's mobile sector, together with the technological evolution of Antel itself, suggest a technological continuity with Alcatel-Lucent (now Nokia). In 2011, Antel launched the region's first commercial 4G network using a complete Alcatel-Lucent suite. In 2019, Nokia and Antel announced the first 5G connection on a commercial network in Latin America. Given this track record, it is reasonable to infer that Nokia is likely a central supplier of Antel's current equipment. In addition, Nokia's public documentation describes "Application Assurance" modules that identify applications and enforce policies on network traffic—functions equivalent to DPI—within its network platforms. This makes it plausible that the same provider responsible for setting up the network also provides inspection capabilities.[256]

Huawei also has a strong presence in Antel's 5G infrastructure, which means its equipment can support modules for deep packet inspection (DPI) and lawful interception, depending on operator configuration and regulatory requirements.

4.2.5. OSINT / WEBINT

As noted, the use of OSINT by law enforcement exists in Uruguay, but the Ministry of the Interior provides no information on protocols, responsible units, or specific "cyber-patrolling" tools.[257]

Based on the analysis conducted, the two platforms acquired by Uruguayan security agencies—El Guardián and EGO—include modules with OSINT capabilities. However, although this appears likely, it is unknown whether those modules were acquired as part of the suites hired.

In 2022, the state upgraded the platform to "Guardian On-line" (from Brazilian provider Dígitro) through an acquisition authorized under a classified regime. Official documentation confirms Dígitro/Teleimpresores as supplier of the "Guardián On-line System," while the company's commercial literature describes modules for "social media and open-source data," featuring a "catalog of more than 200 OSINT sources"—that is, WEBINT/OSINT-type functionalities integrated into the investigative ecosystem.[258] Similarly, EGO could include OSINT capabilities, but it is unclear whether those modules were acquired.

---

255 Administración Nacional de Telecomunicaciones (ANTEL), "Archivo adjunto de la aclaración N° 4," State Procurement Website (Uruguay), July 3, 2024., URL

256 Alcatel-Lucent. "Antel and Alcatel-Lucent Launch 4G/LTE Services in Uruguay and Establish the First Commercial 4G/LTE Wireless Network in a Latin American Country.", URL

257 Díaz Charquero, Patricia, and Jorge Gemetto. *Ciberpatrullaje: Los Límites Borrosos de La Vigilancia Policial En Uruguay*. Montevideo. Datysoc, 2022. URL

258 Prosecretaría de la Presidencia de la República, Expte. N° 2024-4-1-0006320, November 1, 2024. URL

Meanwhile, Uruguay's National Secretariat for the Fight against Money Laundering and Terrorist Financing (SENACLAFT) has received international training that includes methods to transform intelligence into admissible evidence. This suggests the use of open-source or publicly available data analysis tools.[259]

The National Observatory on Violence and Crime also reported incorporating "software for social network analysis (UCINET)" to examine "relational aspects of criminal activity." In security settings, UCINET can be used to analyze criminal networks, associations of individuals, support structures, actor maps, and flows of communication or collaboration—making it a relevant tool for network-based intelligence.[260]

Independently of security agencies, Uruguayan public bodies have also procured services related to digital monitoring and media-environment tracking, including tools designed to generate alerts about institutional mentions and reputational risks in online spaces. For example, procurement records show that public entities have contracted monitoring services covering network environments and digital communications infrastructures, while other government offices have issued tenders for media and online-content monitoring in support of crisis-management and institutional-communications functions. Although these tools are not operated by police forces, they indicate that state institutions maintain capabilities for tracking and generating alerts based on open online content.

---

259 "First joint training on Intelligence into Evidence to Paraguay, Uruguay" URL

260 Nicolás Zara, "Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay," Buenos Aires, CELE, 2023. URL

Table 4: Summary — Uruguay

URUGUAY				
Tool	Company	Distributor	Product / Technology	Acquisition
Spyware	**Hacking Team (Italy)**	OMNI S.A.–RADAR (Paraguay)	Remote Control System (RCS)	Evaluated but not acquired
	NSO Group (Israel)		Pegasus	Reportedly proposed; no evidence of acquisition
SIGINT	**Innova S.p.A. (Italy)**	Tecnodata / Mipoltec (Chile) / Innova S.p.A. (Chile)	EGO (SS7/ Diameter exploitation capabilities)	Confirmed (2024 acquisition reported)
Network intelligence	**Teleimpresores SA (Uruguay)**	Teleimpresores SA (Uruguay)	Telephone-interception equipment	Confirmed
	Digitro Tecnologia Ltda (Brazil)	Teleimpresores SA (Uruguay)	Intellotum - El Guardián	Confirmed
	Innova S.p.A. (Italy)	Innova S.p.A. (Chile)	EGO	Confirmed
	Nokia (Finland)	Antel	LI modules	Very likely
	Ericsson (Sweden)	Antel	*Lawful Interception* System	Confirmed
	Huawei (China)	Antel	LI modules	Very likely
Network monitoring	**Nokia (Finland)**	Antel	DPI modules	Very likely
	Huawei (China)	Antel	DPI modules	Very likely

URUGUAY				
Tool	Company	Distributor	Product / Technology	Acquisition
OSINT	**Innova S.p.A. (Italy)**	Innova S.p.A. (Chile)	EGO	Possible (module availability confirmed; deployment unknown)
	Digitro Tecnologia Ltda (Brazil)	Teleimpresores SA (Uruguay)	Intellotum - El Guardián	Confirmed (platform includes OSINT-type modules)
	Analytic Technologies (US)		UCINET	Confirmed
	Social Links (Ukraine)	TAMCE (Argentina-Mexico)	Crimewall	Reported marketing presence; no confirmed acquisition.
Forensic extraction and analysis	**Cellebrite (Israel)**	Softron Uruguay S.A. (SoftronIT) / IAFIS Uruguay	UFED	Confirmed
	Magnet AXIOM (Canada)	Softron Uruguay S.A. (SoftronIT)	Axiom / Axiom Cloud add-on	Confirmed
	Oxygen Forensics		Oxygen Forensic Detective / Oxygen Forensic Extractor	Confirmed
	Belkasoft Evidence Center X (US)			Confirmed

URUGUAY				
Tool	Company	Distributor	Product / Tech-nology	Acquisition
Video-surveillance / Biometrics / Facial recognition	Hikvision (China)			Confirmed
	Dahua (China)			Confirmed
	Huawei (China)			Confirmed
	ZTE (China)			Confirmed
	IDEMIA (France)			Confirmed
	NEC (Japan)			Confirmed
	Clearview AI (US)			Reported use / licensing discussions (not publicly confirmed)
	M Electronics Monitoring Inc. (US)			Confirmed

5. Some conclusions

5.1. A common context

As noted at the outset, PRISM and Pegasus illustrate two distinct narrative scenarios—two opposite ends that are seemingly unacceptable at first sight. Both reveal different limits of what can be considered legitimate, while also sharing similar conditions for their acceptability. The general characteristics of PRISM did not disappear; rather, they consolidated. NSO Group and other similar companies continue to exist. The narratives on the issue shape the debate itself, defining the variables under discussion and either legitimizing or challenging interception and monitoring tools.

In this context, Argentina, Uruguay, and Chile do not typically rank among countries with strong controls over information flows. According to parameters of Freedom House, the Internet Society, and Access Now, these countries do not exhibit systematic web traffic blocking, internet shutdowns, banned applications, or systematic barriers to accessing content.[261] Nor have they made front-page headlines in the news about the marketing of the most high-profile surveillance technologies. They can therefore be considered settings that remain within a certain average range.

However, such a conclusion warrants caution. This remains a largely underexplored domain. State procurement in the security sector is often veiled. No consensual forensic analyses of devices to rule out indicators of compromise, or sustained investigations into malicious infrastructure have been carried out either. If anything, the opposite conclusion is more appropriate: there has been insufficient scrutiny of the issue. There has been a consistent interest in acquiring these types of tools. And, in effect, it is likely only a matter of time until further acquisitions are confirmed, or they may already be underway. For this reason, what is already known about this landscape underscores the importance of further investigation.

The solutions implemented show that there are not enough avenues for visibility and debate around processes that unfold continuously and at an accelerating pace. Based on the review conducted, the regional landscape shows shared characteristics that should be taken into account in ongoing debates.

Convergence towards integrated surveillance architectures. The compiled tables show that all three countries have incorporated, to varying degrees, virtually the full spectrum of surveillance technologies. This points to a broader regional trend toward integrated architectures, where capabilities are not acquired in isolation; rather they are acquired as complementary systems or with modular integration.

However, the tables also reveal relevant differences in the adoption modes. Apparently, Uruguay stands out as a distinct profile within the region. There appears to be a low likelihood of commercial spyware adoption, as opposed to sustained development of capabilities integrated directly into state infrastructure, particularly through the state telecommunications operator. The emphasis is

---

261 Freedom House. "Countries and Territories." 2025. URL // Internet Society. "Internet Society Pulse." URL // Access Now. "Access Now." URL

on lawful interception, network monitoring via DPI, the use of OSINT, and forensic analysis. This shapes a model that is more centralized, structural, and regulated, rather than one based on specific covert operations. By contrast, Argentina shows a more fragmented ecosystem, with multiple local intermediaries, probable or partial acquisitions, and a gradual accumulation of capabilities across different state agencies and administrative levels. This results in a model that is fluid, opaque, and difficult to audit. In Chile, a broader and more sustained pattern of adoption is observed: several highly intrusive technologies—including commercial spyware—appear to be confirmed acquisitions by more prominent actors in the field.

Political shifts and technological capabilities. Despite significant—and at times radical—political changes across countries in the region, a common pattern persists. From Piñera and Bachelet to Boric, from Cristina Fernández and Macri to Alberto Fernández and Milei, and from Mujica and Vázquez to Lacalle Pou and Orsi, interest in the same categories of surveillance technologies has remained broadly constant. This continuity appears with varying intensity, under different degrees of public visibility, through shifting narratives used to justify acquisition, and with important differences in the institutional safeguards surrounding their deployment.

This last point is central: the political and institutional framework on which these tools rest is crucial, as it determines the mechanisms of oversight. This, however, represents an even greater risk. These tools may be accepted under certain political conditions, but those conditions can change while the technologies remain in place. The capabilities described will never cease to pose a latent political and social risk.

Implementation within a specific institutional framework introduces structural risks. Many classic formulations have already outlined this type of political challenge in the field of security. It is worth recalling that the issue is not the technologies themselves, but their documented use against journalists, activists, and political actors. Conditional acceptance nevertheless entails structural risks. In the case of technologies like these, power granted under certain conditions does not vanish when those conditions change. The deployment of these technologies embodies political decisions that continue to operate even as the political context shifts. Moreover, their adoption is, in all likelihood, difficult to reverse. Put plainly: whether it is Milei–Bullrich, Cristina Fernández–Parrilli, Piñera, Maduro, or Bolsonaro, political rivals would be unlikely to want each other to have discretionary access to these technologies. Almost certainly, we would not want autonomous intelligence agencies wielding them.

Nonetheless, at a macro level, regardless of the political orientation of any given government, the number of acquisitions continues to rise steadily.

Security forces and intelligence agencies. In parallel with the deployment of digital surveillance capabilities, “old school” espionage practices persist in Argentina, Chile, and Uruguay. This includes tailing targets, going under cover, wiretapping, and political intelligence carried out by intelligence services and security forces that operate with significant degrees of autonomy and weak civilian oversight. Cases of illegal espionage attributed to the AFI in Argentina, the irregularities and fabrications exposed in Chile’s Operation Huracán, and parliamentary investigations into military and police spying in democratic Uruguay all point in the same direction. State resources and technologies can be used

in a discretionary—or even self-directed—manner, blurring boundaries between intelligence functions and policing tasks, and without effective oversight over the actual use of the tools at hand. At present, these activities are carried out by intelligence services with limited legal assurances, without proper political authorization, and with blurred boundaries vis-à-vis law enforcement agencies. As a result, we may have to assume that security forces have discretionary powers of use of these tools, beyond their potential lawful uses.

Geopolitical shifts and international alignments shape a landscape that, while at times opaque or fragmentary, suggests that the countries producing interception tools are few and that acquisitions follow clear international alliances. It is important to understand which governments have promoted certain offerings and which have rejected them. Spyware and interception capabilities have become geopolitical instruments. States not only seek to develop or acquire these capabilities for their own use, but also to regulate them for their own benefit, or against the interest of rival states. In this context, human-rights concerns and digital-rights commitments often function more as ethical bargaining chips within a debate driven primarily by geopolitical competition.

While Israel, Italy, and India are at the forefront when it comes to spyware, Latin America appears to consume primarily those produced by Israel and Italy.

In the realm of SIGINT tools, Israel, the United States, and Germany lead the field. Of these, Israel and the United States are, in particular, our main suppliers of IMSI catchers and location-tracking technologies based on SS7/Diameter protocols.

"Lawful interception" through network data intelligence appears to be largely in the hands of European producers, with Italy and Germany at the forefront. But it is Italy in particular where the companies that have successfully captured our market are based.

This provides a fairly clear picture: while most South American countries acquire these technologies from Western suppliers, tools from other major global producers—such as Russia and China—have primarily been confirmed in Cuba, Venezuela, and Nicaragua.[262]

Research by Insikt Group raises questions about the possible acquisition of products from the Russian conglomerate Citadel—which brings together companies such as MFI Soft, Vas Experts, and Protei. Together, these firms develop both information security solutions—including packet inspection, database protection, and internet traffic filtering—as well as lawful interception systems (SORM). Various Russian media outlets reported that purchases of MFI Soft products may have begun in the region as early as 2017. To this, one can add Argentina's approach to Russia and the BRICS between 2019 and 2023, with Brazil playing a central role in the region.

In sum, some governments are deepening their security ties with the United States and Israel, while others are also opening up to contracts with China and Russia.

---

262 Insikt Group. *Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America.* Recorded Future, 2025. URL

Experts. Argentina, Uruguay, and Chile form a regional cybersecurity hub with highly skilled technical professionals who are competitive in terms of expertise relative to cost. This has driven the establishment of regional offices, remote teams, and advanced operations by multiple companies in the sector. For example, Core Security—established in Argentina in the 1990s—and the local web of firms that includes Onapsis, demonstrate the capacity to produce research, tools, and services with global reach. This ecosystem is further strengthened by specialized conferences—such as EkoParty in Buenos Aires and 8.8 Matrix in Chile—which attract international actors, serve as intensive training spaces, and act as recruitment platforms.[263] For this reason, foreign companies—including Swiss firm Dreamlab, linked to the early operational structure of FinFisher—have established teams in the Southern Cone countries, capitalizing on the availability of specialized talent. This adds to the systematic incorporation of technical professionals from the region into research teams at multinational companies (antivirus vendors, consultant firms, and digital security providers), favored by their high level of expertise, English proficiency, time zone alignment with Europe and the United States, and relatively low labor costs. As a result, countries in the Latin American Southern Cone supply skilled specialists to companies operating at different points along the chain. Rather than acting as direct producers of digital surveillance tools, they act as developers of infrastructure, vulnerabilities, and exploits.

Legislations, gaps. This is not the report's main focus, but it clearly constitutes a central issue. As in the rest of the region, outdated security laws remain in force and create a legislative gap in much of what concerns digital surveillance tools. From a regulatory standpoint, Argentina (Law 25,520 on National Intelligence and the general data protection framework), Chile (Law 19,974 on the State Intelligence System and Law 19,628), and Uruguay (Law 19,696 on the National State Intelligence System and Law 18,331 on personal data protection) all retain frameworks designed for traditional interception of communications and the generic processing of personal data. They lack specific, detailed, and transparent rules governing the acquisition, use, democratic oversight, and accountability of spyware, vulnerability exploitation, online mass monitoring, and other advanced digital surveillance tools. This results in a regulatory vacuum, across all three countries, that enables broad discretionary use by security and intelligence forces and leaves significant gray areas in the effective protection of fundamental rights in light of contemporary digital surveillance. As noted, in a global context where the United States has enacted specific protections for its own citizens and Europe has imposed its General Data Protection Regulation (GDPR), citizens in South America remain comparatively less protected vis-à-vis companies of different sizes that collect and market data.

Structural reliance on foreign providers. This last point is particularly relevant. In all three cases, a consistent pattern emerges: critical technologies come mostly from companies based in Israel, Italy, and the United States. Local actors appear almost exclusively as distributors, integrators, or commercial partners. This reinforces a form of technological dependence that limits transparency and auditing of tools with high impact upon fundamental rights. In turn, this dependence introduces structural risks: loss of technological sovereignty, obstacles

---

263 For more on the latter, see: Perlroth, Nicole. *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. Bloomsbury Publishing, 2020.

to auditing, and an asymmetric relationship in which states acquire advanced surveillance capabilities without effective control over their scope and limits.

Intermediary importers. There is, therefore, a dense network of intermediary companies and local representatives marketing advanced surveillance technologies in a discreet manner, often with limited transparency and, in some cases, uneven levels of technical capacity. Leaked emails from Hacking Team revealed negotiations with resellers and agencies in the region marked by improvisation, weak technical support, and costly licenses that were sometimes rendered obsolete or unusable, as well as indications of room for discretionary uses of these tools. Many of these firms simultaneously provide services to the private sector, public institutions, and security forces, combining open commercial catalogs with more opaque portfolios. They often adopt generic, difficult-to-trace names—Infotech, Teleinformaciones, Automation Systems, Business Solutions Group, and similar—and maintain minimal websites where contact forms are sometimes the only visible channel. This may allow verification of the existence of a commercial relationship, but not the specific type of product acquired or its actual capabilities, further reinforcing gray areas in oversight and accountability.

By contrast, the **ecosystem** of civil society institutions researching available tools and their uses plays a fundamental role. Amnesty International's Security Lab, together with the Citizen Lab at the University of Toronto, are at the forefront of technical research and development of novel methods to detect these technologies. Their technical reports—often published in collaboration with leading journalistic outlets—set key milestones in the field.

At the regional level, Access Now operates across multiple lines of action in the Global South. Among other initiatives, it provides support through its Digital Security Helpline and promotes global campaigns—such as #KeepItOn against internet shutdowns—to counter censorship, mass surveillance, and abuse of state and corporate power. In addition, there are regional organizations focused on fostering public debate, filing freedom-of-information requests, and conducting legal analysis. Notable examples include Argentina's Fundación Vía Libre, Chile's *Derechos Digitales*, Uruguay's Datysoc, Mexico's SocialTIC, Colombia's Fundación Karisma, Brazil's MariaLab, Argentina's ODIA, and the Latin American collective 0xche. Among them, only SocialTIC and 0xche have in-house technical analysis capabilities.

Spyware. The Latin American market is saturated with deprecated Android devices. In many cases, even when security patches for the operating system are publicly released, vendors do not incorporate them into their devices. When users buy these under the providers' own terms and conditions, they let the providers effectively determine how long those devices will receive security updates. In addition, this is a region where consensual forensic analyses have not been systematically conducted. Not only that. Indicators of compromise or reliable information to identify specific spyware infections are largely absent. In this context, tracking offers, purchases, and procurement processes has proven to be one of the most effective methods for establishing the presence of spyware in the region.

SIGINT. In the Southern Cone, SIGINT capabilities associated with mobile surveillance combine at least the use of IMSI catchers with remote geolocation platforms based on vulnerabilities in signaling systems. In the case of interception via SS7/Diameter signaling protocols, services are often procured directly from

abroad, operating over infrastructures with insecure networks. These tools can enable continuous tracking and, in some cases, selective interception of communications, with limited traceability, outdated legal frameworks, and weak oversight mechanisms.

As previously noted, two research projects stand out. The first, aimed at detecting fake antennas or IMSI catchers—known as FADE (Fake Antenna Detection Project)—, was carried out exclusively during 2020 in Buenos Aires and Santiago, Chile.[264] The second project, Mobile Surveillance Monitor, records both the persistence of insecure infrastructure and instances of malfunction and network errors in mobile telephony systems consistent with attacks on SS7/Diameter signaling.[265]

Network intelligence, lawful interception and adjacencies. There is a central issue: the specific capabilities of these tools remain unknown. In the field of network intelligence and lawful interception in Latin America, a structural gap persists in terms of transparency and control regarding the actual capabilities available to states and service providers. All the knowledge we have gained comes primarily from independent technical analyses, academic research, and reports by organizations such as the EFF, ADC, *Derechos Digitales,* and Access Now. These sources point to a mixed landscape: while some telecommunications providers have adopted improved privacy policies, they are yet to systematically publish statistics on government requests, data handover criteria, the use of traffic management tools, or details concerning retention and generation of metadata. Meanwhile, many assessments of data privacy policies conducted by independent organizations tend to yield poor results overall. Companies such as Personal, Telecentro, Arlink, DirectTV, and Claro, in fact, show concerning performance levels.[266] In parallel, the existence of both active and passive monitoring solutions has been documented—including deep packet inspection (DPI) and interception interfaces integrated into network infrastructure—procured under strict confidentiality and with very limited public auditing mechanisms. This makes it difficult to accurately assess the true scope of surveillance capabilities and reinforces existing grey areas in terms of procedural guarantees and democratic checks.[267]

Forensic extraction and analysis, video-surveillance and biometrics. These technologies fall outside the scope of this report and raise their own distinct concerns. Video surveillance systems are generally supplied by Chinese companies such as ZTE, Huawei, Dahua, and Hikvision, while biometric systems are predominantly sourced from the United States. The market for forensic extraction and analysis tools used by law enforcement is regionally dominated by UFED technology from Cellebrite. Although no concrete abuses have been identified in South America to date, the risks associated with these technologies have been extensively discussed. Multiple international reports note that these same com-

---

264 https://fadeproject.org

265 Mobile Surveillance Monitor. "Mobile Surveillance Monitor: dashboard". URL

266 Penas, Victoria. *¿Quién defiende tus datos? Argentina – 3ra. edición. ADC,* 2023. URL

267 Veridiana Alimonti, *Eight Years Holding ISPs to Account in Latin America: A Comparative Outlook of Victories and Challenges for User Privacy.* San Francisco: EFF, 2023, URL

panies market their products in countries where human rights violations have been documented.[268] In practice, such extractions have in some documented cases been conducted without a court warrant in the United States.[269] In Brazil, indiscriminate use has been documented,[270] and in Serbia there are records of these tools being used to unlock devices in order to install spyware—without consent—to achieve persistent monitoring.[271]

For this reason, the debate around these technologies is extensive. Commercial forensic tools are not subject to independent audits and do not allow for the independent establishment of standards of reliability, transparency, and admissibility. Law enforcement and security agencies often place their trust in these products with little evidence to support it. It can also be argued that the use of exploits against unpatched vulnerabilities may produce uncontrolled changes on the device, undermining the chain of custody of information and, consequently, the validity of digital evidence presented in court.[272] Moreover, it must be added that the tools themselves can contain security vulnerabilities that may be exploited through data deliberately stored on the phone—potentially altering the evidence or disrupting the proper functioning of the forensic tools.[273]

Finally, as the Serbian case cited above illustrates, the fact that these tools can operate without leaving traces on the device further increases the risk of illicit use for illegal purposes. And, as documented, in contexts where the state acts against dissidents, journalists, activists, or minorities, these tools can easily become instruments of repression.

---

268 Pisanu, Gaspar, and Verónica Arroyo. *Surveillance Tech in Latin America: Made Abroad, Deployed at Home.* Access Now. 2021. URL

269 Koepke, Logan, Emma Weil, Urmila Janardan, Tinuola Dada, and Harlan Yu. *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones.* Upturn, 2020.URL

270 Ramiro, André, Amaral, Pedro, Canto, Mariana, and Pereira, Marcos César. *Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil –Instituto de Pesquisa em Direito e Tecnologia do Recife* (IP.rec), 2022. URL

271 Amnesty Tech. Serbia: *"A Digital Prison": Surveillance and the Suppression of Civil Society in Serbia.* Amnesty International, 2024. URL

272 P. Dimpe, "Impact of Using Unreliable Digital Forensic Tools," *Proceedings of the World Congress on Engineering and Computer Science* (San Francisco: IAENG, 2017), 118–125, URL

273 There are documented cases of vulnerabilities prone to exploitation in UFED and EnCase. URL

5.2. Problems and Tensions

Each of these tools gives rise to distinct political, social, and legal debates, while also presenting a set of shared challenges. Below, we outline a partial list by way of conclusion.

- **Privatization of and opacity in state security and surveillance capability.** The commercial expansion of these tools causes the privatization of functions traditionally associated with state sovereignty. Decisions about who does the surveillance, and who the targets of that surveillance are, are effectively shifted to corporate boards and opaque contracts. From a theoretical and political standpoint, this amounts to the emergence of an industrial complex capable of shaping public policy without commensurate democratic checks.[274]
- **Deliberate production of structural insecurity**. The business model behind spyware, SS7/Diameter signaling attacks, and other technologies discussed, relies on the persistence of unpatched security holes. Companies look into vulnerabilities, and develop and market exploits and intrusion suites. Economic incentives favor market expansion, technical secrecy, and the continued existence of unpatched vulnerabilities. Each unreported exploit leaves not only purported "legitimate targets" exposed, but entire populations. This subverts a basic principle of digital security: rather than strengthening systems for everyone, weaknesses are preserved for selective use. This creates a broader social problem: the security of millions of people is subordinated to the strategic interests of a few actors seeking access to information that should remain protected.[275]
- **Sovereignty, geopolitics, and surveillance colonialism.** Spyware, attacks exploiting signaling protocols, and many IP intelligence and OSINT tools enable under-the-radar transnational operations. Devices located in virtually any country can be remotely accessed or interfered with. Companies and governments from the so-called Global North supply tools used to monitor opposition figures, journalists, and communities in the so-called Global South. States with more limited technical capabilities become dependent on external providers. This setup reproduces patterns of technological dependency and extractive data models: the capacity to observe, map, and anticipate is concentrated in a few nodes, while exposure is distributed asymmetrically.
- Security / privacy / political control. Very briefly put, the displacement of the line between security and political control is underpinned by the legitimizing narrative surrounding many of these tools, which invokes the fight against terrorism, illegal pornography, and organized crime. However, international research shows their recurrent use against journalists, human rights defenders, opposition figures, and political organizations. This shifting of the line has specific political consequences: the line between national security and political surveillance becomes blurred, the category of "threat" expands to

---

274 Amnesty Tech, *Operating in the Shadows: Investor Risk from the Private Surveillance Industry* London: Amnesty International, 2021. URL

275 Lookout Mobile Security *Technical Analysis of Pegasus Spyware*, 2016. URL

include critical voices, and control over public debate is exercised through tacit means.[276]

- Structural risk. Adopting these tools entails accepting a form of structural political risk never before known or considered. As noted, the political-institutional framework in which these tools are embedded is crucial: it determines the control mechanisms. As a result, any given tool may be deemed acceptable under certain political conditions; now, those conditions may change, and the technologies already in place will remain unchanged. It is worth stressing that the issue is not the technologies themselves; their long-documented use against journalists, activists, and political actors is. The power granted under specific conditions does not disappear when those conditions are no longer there. The capabilities described here will never cease to be a latent political and social risk.
- **Normalization of surveillance.** The risk lies in surveillance coming to be perceived as an accepted fact of life, operating as a mechanism of depoliticization. These tools act in an environment where data extraction by platforms, advertisers, and apps is already considered part of our routine. The distinction becomes blurred between (i) commercial tracking, (ii) acceptance of specific terms and conditions on given platforms, (iii) state surveillance, and (iv) full control of devices. This is not only about individual privacy; it is about a structural erosion of trust as a political and social asset.
- **Impact on journalism and public deliberation.** International bodies and specialized rapporteurships have documented how this highly intrusive surveillance erodes the material conditions for independent journalism, even in the absence of direct reprisals.[277] According to this argument, these tools introduce a chilling effect on freedom of expression and the production of information. Journalists and editors can no longer guarantee confidentiality to their sources. Organizations and newsroom teams begin to operate under the assumption of persistent device compromise. This generalized perception fuels preemptive self-censorship: the cutting-down of topics under investigation, moderation of language, and dismissal of critical sources. And, those who assume that "everything is digitally recorded" lean toward cynicism or constant self-correction. Both dynamics reduce the willingness to engage in open dissent and to organize collectively against the limits imposed by these technologies. In this sense, many of these tools act on political behavior itself, rather than merely as instruments for the collection of criminal evidence.
- **Limits to the notion of surveillance.** For all these reasons, the concept of "surveillance" is not entirely adequate to address the use of these technologies. We use it while recognizing the following problems: (i) it tends to fore-

---

276 Forbidden Stories, "Pegasus: The New Global Weapon for Silencing Journalists," July 18, 2021. URL

277 United Nations, Human Rights Council, *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* (Geneva: OHCHR, 2019), URL ; Council of Europe, Commissioner for Human Rights, "Highly Intrusive Spyware Threatens the Essence of Human Rights," January 27, 2023, URL; Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, *The Impact of Digital Surveillance on Freedom of Expression* (OEA, 2025).URL

ground the analysis of state security agencies, while obscuring the decisive role of private companies and transnational networks operating under their own logics; (ii) it suggests continuity with traditional persecution practices, failing to capture the qualitative and quantitative leap involved; (iii) it assumes that the primary issue lies in its misuse—"seeing too much" or excessive collection of data—when the debate also encompasses the capacity to sustain structural insecurity, shape behavior, and produce political change; (iv) it maintains a focus on the legitimate/illegitimate dichotomy as defined by law, which can hide how these technologies reconfigure power relations even when they operate within formal frameworks.

***

In conclusion, these are technologies that are expanding faster than the mechanisms designed to oversee them. To a significant extent, the full capabilities of these tools—and of their combined use—remain unknown, as do the political and social consequences of their large-scale deployment. We hope this review at least provides a state-of-the-art overview of the main tools and many of the companies that develop and market them.

5.3. Limitations and lines of further research

- **Prospective intelligence.** Various reports by civil society organizations have identified a growing trend toward the development of prospective intelligence activities linked to preventive policing. This involves the acquisition and accumulation of digital data without a defined criminal hypothesis—a type of practice that riskily blurs the line between police intelligence work and crime prevention functions, and entails forms of monitoring and data collection that may lack a clearly defined legal basis.
- **Consensual forensic analyses.** To date, there have been no systematic sampling campaigns involving mobile devices of activists and social leaders in search of indicators of infection to detect traces of spyware in the region, in the way that Amnesty International has done in other parts of the world.
- **Tracking of malicious infrastructure.** Organizations such as Amnesty International's Security Lab and Citizen Lab conduct continuous monitoring of domains and network infrastructure to identify the deployment of attack servers and other components linked to spyware operations. Infrastructure associated with different intrusion-software providers often leaves distinctive "fingerprints" in the configuration of web servers, domain-registration patterns, and the setup of intermediary servers. These methods have enabled organizations such as Amnesty International, for example, to gain visibility into the testing and deployment of spyware systems across multiple countries worldwide. No systematic analyses of this kind appear to have been conducted at the local level.
- **Analysis of historical domain and DNS data.** The systematic examination of domain histories, DNS changes, ownership records, and infrastructure changes of domains already identified as showing indicators of compromise (IOCs), remains an underexplored line of inquiry for uncovering the presence

of spyware campaigns in the region.

- **Granular legal analysis of each tool's scope.** To the best of our knowledge, there is generally no established practice of conducting detailed legal assessments of the specific capabilities of each surveillance solution. In the absence of technical-legal opinions that contrast functionalities (geolocation, interception, intrusion, data retention, etc.) against constitutional and procedural regulations, gray areas become consolidated, allowing highly intrusive technologies to be normalized through generic administrative contracts.
- **Freedom-of-information requests**. Access-to-information mechanisms are a key, yet underused, tool for auditing procurement and use of surveillance technologies. Where requests have been filed, responses are often partial, fragmented, or withheld on national-security grounds, reinforcing the need for more systematic strategies, strategic litigation, and regional coordination to open up this data to democratic scrutiny

Glossary

0-DAY EXPLOIT	An exploit that takes advantage of a vulnerability that is not publicly known and for which no official patch is available.
0-CLICK EXPLOIT	An exploit that does not require any user interaction to run.
1-CLICK EXPLOIT	An exploit that requires a single user interaction to run (e.g. clicking a link).
2 FA (TWO-FACTOR AUTH)	An access control mechanism that requires two independent factors to verify identity, thereby reducing the risk of compromise from stolen credentials.
3G / 4G / 5G	Third-, fourth-, and fifth-generation mobile telecommunications technologies, respectively.
3GPP (3RD GENERATION PARTNERSHIP PROJECT)	A global partnership of telecommunications standards organizations that develops technical specifications for mobile systems, including GSM, UMTS, LTE, and 5G NR.
ANSI (AMERICAN NATIONAL STANDARDS INSTITUTE - ANSI)	Body that oversees the development of standards for products and services in the United States.
APT (ADVANCED PERSISTENT THREAT)	Targeted and persistent digital attacks aimed at collecting data and monitoring communications over extended periods.
ATTACK VECTOR	The path or method through which an attacker gains access to a system (email, web, messaging, etc.).
BACKDOOR	A hidden or undocumented access mechanism that allows persistent or privileged access to a system, sometimes intentionally introduced and sometimes discovered after deployment.
CALEA (COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT)	U.S. law requiring the facilitation of lawful interception on networks.
CSPS (COMMUNICATIONS SERVICE PROVIDERS)	Organizations that offer and operate communication and connectivity services (voice, data, messaging, video) through telecommunications infrastructure and networks, managing their provision, operation, and support for end users or businesses.
DF (DIRECTION FINDING)	Radio direction finding technique that estimates the direction of arrival of a radiofrequency signal using antennas/sensors and signal processing methods, in order to locate or track the emitting source.
DIAMETER	A signaling protocol used in 4G and 5G telecommunications networks for authentication, mobility management, and policy control. Security weaknesses in some implementations can enable location tracking or interception.

DOS/DDOS (DENIAL OF SERVICE / DISTRIBUTED DENIAL OF SERVICE)
An attack that aims to degrade or disrupt the availability of a service or network by exhausting resources (bandwidth, CPU, memory, or connection sessions).

DNS (DOMAIN NAME SYSTEM)
Service that enables human-readable domain names (such as example.com) to function by translating them into IP addresses so that the correct server can be located.

DOWNSTREAM
Data acquisition model in which information is obtained directly from service providers or platforms, rather than intercepted upstream—that is, while it is in transit across the core network infrastructure.

DPI (DEEP PACKET INSPECTION)
Network traffic inspection technique that analyzes packets beyond their headers to identify, classify, filter, or prioritize communications.

DUAL-USE TECHNOLOGIES
Technologies, components, or knowledge that can be used for both civilian-commercial purposes as well as military or security applications, and are therefore often subject to controls and risk assessment.

END-TO-END ENCRYPTION
Encryption scheme in which data is encrypted on the sender's device and can only be decrypted on the recipient's device, preventing intermediaries (e.g., transport servers) from accessing content.

ETSI (EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE)
European body responsible for telecommunications standardization.

EXPLOIT
Code, technique, or sequence of actions that exploits a vulnerability to trigger unintended behavior in a system (e.g., code execution, privilege escalation, or bypassing security controls).

EXPLOIT CHAIN
A sequence of combined exploits used to bypass defenses and achieve unauthorized control of a system.

FADE (FAKE ANTENNA DETECTION PROJECT)
Project/methodology for detecting potential fake base stations (e.g., IMSI catchers) through mobile network anomaly analysis.

FINGERPRINTS
A set of characteristics that enable the unique or probabilistic identification or correlation of a device, user, application, or network flow, even in the absence of explicit identifiers.

GDPR (GENERAL DATA PROTECTION REGULATION)
EU regulation that establishes the legal framework for the processing of personal data, defining core principles, legality bases, data subject rights, and the obligations of controllers and processors.

GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS)
2G digital mobile telephony standard that defines the radio interface, signaling, and network architecture for voice and data services (e.g., SMS).

IMEI (INTERNATIONAL MOBILE EQUIPMENT IDENTITY)
A unique numerical identifier (typically 15 digits) assigned to a mobile device, used by the network to identify the equipment and support functions such as access control, inventory management, and blacklisting.

IMSI (INTERNATIONAL MOBILE SUBSCRIBER IDENTITY)	A unique identifier of a mobile subscriber stored in the SIM card, used by the cellular network to authenticate the user and manage subscription and mobility.
IP (INTERNET PROTOCOL ADDRESS)	Logical numerical identifier assigned to a network interface that enables the routing of packets across networks.
IOC (INDICATOR OF COMPROMISE)	Observable evidence associated with malicious activity or intrusion (e.g., hashes, domains/IPs, paths, signatures, host artifacts, or network patterns) used to detect, investigate, and respond to incidents.
ISP (INTERNET SERVICE PROVIDER)	An entity that offers access to the Internet and associated services.
JAMMERS/ BLOCKERS/ SIGNAL INHIBITORS	Electronic devices that generate interference to disrupt or block mobile telephony, radio communication, or data transmission signals.
KEYLOGGER	Software or hardware device that records keystrokes to capture credentials or messages.
LEA (LAW ENFORCEMENT AGENCY)	Governmental agencies responsible for the enforcement of law and public security.
LAWFUL INTERCEPTION (LI)	The interception of communications and associated data carried out by service providers under legal authorization and in accordance with national regulatory frameworks.
MITM (MAN-IN-THE-MIDDLE)	An attack in which a third party intercepts and/or alters communication between two parties without being detected.
MALWARE	Malicious software designed to harm systems, gain unauthorized access, or steal information.
MVT (MOBILE VERIFICATION TOOL)	Open-source tool for analyzing mobile device logs to detect indicators of compromise (IOCs) resulting from spyware infections.
N-DAY EXPLOIT	*An exploit that leverages a publicly known vulnerability.*
NETWORK INJECTION	Technique that injects packets into a target's Internet traffic to block, intercept, or manipulate traffic.
NETWORK MEASUREMENT METHODS	Techniques used to assess network quality, policies, or controls (e.g., scanning, interference measurement).
NOC (NETWORK OPERATIONS CENTER)	Facility or unit dedicated to the continuous monitoring, management, and maintenance of network infrastructure.
NSA (NATIONAL SECURITY AGENCY)	U.S. intelligence agency focused on signals intelligence and cybersecurity/cryptography for the protection of government systems and infrastructure.
OSINT (OPEN SOURCE INTELLIGENCE)	Intelligence discipline that collects, processes, and analyzes publicly available information (open sources) to produce actionable insights, using verification, correlation, and contextualization techniques.

PHISHING
A social engineering technique that induces users to reveal credentials, sensitive data, or perform malicious actions through impersonation (e.g., fraudulent emails, websites, or messages).

PRISM
Codename for an NSA intelligence collection program through which communications and associated data were obtained directly from U.S.-based electronic communications service providers.

RANSOMWARE
Malware that encrypts or locks systems and demands a ransom payment to restore access.

RCE (REMOTE CODE EXECUTION)
An exploit that allows code to be executed on a system from a remote location.

RCS (REMOTE CONTROL SYSTEM)
Commercial spyware developed by Italian company Hacking Team.

SOC (SECURITY OPERATIONS CENTER)
A specialized unit or facility dedicated to the monitoring, detection, analysis, and response to cybersecurity incidents. A SOC continuously monitors events and alerts from networks, systems, applications, and devices in order to identify malicious activity, vulnerabilities, or unauthorized access, and to coordinate containment and mitigation actions.

SIGINT (SIGNALS INTELLIGENCE)
Intelligence derived from the interception and analysis of electronic signals and communications (e.g., radio, telephony, data links), including both content and metadata, for intelligence and security purposes.

SOCMINT (SOCIAL MEDIA INTELLIGENCE)
An intelligence discipline that collects and analyzes data from social media and social platforms (content, metadata, and interactions) to obtain information on actors, events, patterns, and relational networks.

SORM (SYSTEM FOR OPERATIVE INVESTIGATIVE ACTIVITIES)
Technical framework and specifications for lawful interception in Russia that requires telecom operators and ISPs to install equipment enabling authorized agencies (e.g. FSB) to intercept and obtain communications and related data.

SPYWARE
Malicious software designed to obtain and exfiltrate information from a system (e.g., data, communications, credentials, or location) and/or monitor user activity without the user's consent and operates covertly.

SS7 (SIGNALING SYSTEM N.º 7)
A set of signaling protocols used in telecommunication networks to establish and manage calls and services (roaming, SMS, and routing), exchanging control information among network nodes.

TACTICAL INFECTION
An infection vector that operates in close physical proximity to the target (e.g., malicious Wi-Fi networks or fake base stations).

TLS (TRANSPORT LAYER SECURITY)
A transport-layer cryptographic protocol that provides confidentiality, integrity, and authentication through a handshake process and symmetric encryption, securing client–server communications.

UPSTREAM	An acquisition modality in which the NSA collects communications in transit as they traverse the Internet backbone, with the compelled assistance of the companies operating that infrastructure, applying filtering based on selectors associated with authorized targets.
URL (UNIFORM RESOURCE LOCATOR)	The address of a resource on the internet; a string of text that specifies where something is located (and usually how to access it), such as a webpage, image, or file.
VENDORS	Companies that develop, manufacture, or supply technological products and services.
VPN (VIRTUAL PRIVATE NETWORK)	A method for securely connecting networks over public infrastructure and/or concealing a user's identity.
VOIP (VOICE-OVER-IP)	A technology that enables real-time voice transmission over IP networks by digitizing, encoding, and encapsulating audio into packets, using signaling and transport protocols (e.g., SIP / RTP) to establish and maintain calls.
XKEYSCORE	Codename for an NSA system used to index, process, and query large volumes of data collected from various intelligence sources, enabling searches by selectors (e.g., email, IP addresses, cookies) and network activity analysis.

About SocialTIC

SocialTIC is a Mexican non-profit organization that, since 2012, has been dedicated to research, training, support, and the promotion of digital technology for social purposes.
socialtic.org /@socialtic / contacto@socialtic.org

Author

Lucas Dominguez Rubio

Acknowledgements

To CeDInCI, where I developed as a researcher and continue to work. To my colleagues at Social TIC and to Paul Aguilar, with whom I carried out this research. To the Open Technology Fund and to those who support its essential mission. To the civil society organizations and experts across South America who have sustained debates on these issues for decades.
To Iván Arce, Gary Miller, Beatriz Busaniche, Margarita Trovato, Patricia Diaz Charquero, Gaspar Pisanu, and 0xche, for generously sharing their knowledge and perspectives.
I also benefited from decisive readings and support: this entire work would not have been possible without T. I owe this journey to her; I learned everything from her, and much more.

SOCIALTIC

OPEN TECHNOLOGY FUND


OPEN
TECHNOLOGY
FUND


SOCIALTIC